Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Regulating State, Local, Tribal, and Territorial Law Enforcement Actions to Counter Unmanned Aircraft Systems (C-UAS)

July 29, 2026

The use of unmanned aircraft systems (UAS, or drones) has increased for commercial and recreational purposes; so too have concerns about their potential public safety and security risks. Since 2018, federal law enforcement agencies within the U.S. Department of Justice (DOJ) and U.S. Department of Homeland Security (DHS) have had counter-unmanned aircraft systems (C-UAS) authorities to respond to threats from malicious drones. More recently, through the SAFER SKIES Act, included in the National Defense Authorization Act for Fiscal Year 2026 (FY2026 NDAA; P.L. 119-60), Congress extended similar authorities to state, local, tribal, and territorial (SLTT) law enforcement and correctional agencies. These authorities are conditioned on compliance with training and certification requirements, outlined in a recently released July 2026 Interim Final Rule (IFR) issued jointly by DOJ and DHS: *Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies* (hereinafter, "July 2026 IFR"). This In Focus provides an overview of potential threats from malicious drones; authorities granted to federal and SLTT agencies; training and certification requirements included in the July 2026 IFR, and issues that Congress may consider regarding the regulation of SLTT agencies' C-UAS activities.

Concerns about Malicious Drones

UAS may pose unique public safety or security risks. Some have warned, for instance, that drones can be used as reconnaissance tools for malicious actors "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.

Various federal criminal laws have historically limited law enforcement's C-UAS options. For instance, criminal surveillance laws, like the Wiretap Act and Pen/Trap Statute, may be implicated when law enforcement intercepts signals or communications 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 run up against laws concerning communication lines, stations, or systems; 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 seizing an aircraft.

Expanding Law Enforcement's Toolkit

In response to concerns about malicious drones, policymakers have taken steps to expand law enforcement's ability to engage in C-UAS activities—including detecting, identifying, monitoring, tracking, communicating with, and disrupting or disabling suspicious or malicious drones.

Federal Law Enforcement

The Preventing Emerging Threats Act of 2018 (Division H of P.L. 115-254; 6 U.S.C. §124n) granted DOJ and DHS certain C-UAS authorities to protect covered facilities and assets from malicious drones. In doing so, it provided them with relief from possible violations of certain federal criminal laws when engaging in specified counter-UAS activities, such as detecting, identifying, and tracking drones and disabling, seizing, or destroying them. The SAFER SKIES Act amended 6 U.S.C. §124n to authorize these agencies to take such actions, not just for covered facilities and assets, but 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."

SLTT Law Enforcement

Through the SAFER SKIES Act, Congress also granted SLTT law enforcement and correctional agencies authority to engage in actions to counter potential UAS threats. This authority is contingent on these entities undergoing DOJ training and certification. DOJ, in coordination with DHS, the U.S. Department of Defense (DOD) and U.S. Department of Transportation (DOT), is required to develop regulations for this training and report to Congress on SLTT agencies' C-UAS use. DOJ—along with DHS, DOD, DOT, the Federal Communications Commission, and the National Telecommunications and Information Administration—is also required to maintain a list of authorized C-UAS systems and technologies that may be used by SLTT agencies. The SAFER SKIES Act 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 SLTT law enforcement recipients to use funds to purchase and operate approved C-UAS technology.

National Schoolhouse for C-UAS

The Federal Bureau of Investigation (FBI) runs DOJ's C-UAS training and certification program through the National C-UAS Training Center (NCUTC), a national schoolhouse established

at the FBI's campus at Redstone Arsenal, AL. Before enactment of the SAFER SKIES Act and final DOJ training and certification, the NCUTC trained SLTT officers deputized to serve on FBI C-UAS task forces. DOJ and DHS recently issued the July 2026 IFR, outlining the training and certification to be carried out at the NCUTC.

Training, Certification, and Implementation

Among other provisions, the July 2026 IFR outlines two types of certification for SLTT agencies engaged in C-UAS activities: (1) Detection and Warning and (2) Mitigation. It specifies that officers and employees (but not contractors) may receive certification to conduct C-UAS activities and may engage in mutual aid and regional C-UAS support of other agencies. The NCUTC maintains a certification database, and only certified personnel may exercise the C-UAS authorities.

Detection and Warning Certification. This certification course involves training on activities to detect, identify, monitor, or track a UAS, or to warn the operator. It does *not* involve mitigation efforts to disrupt, seize control of, disable, damage, or destroy a UAS. This certification is obtained after a law enforcement or correctional officer completes an online curriculum and passes a post-course assessment through the NCUTC training portal.

Mitigation Certification. This certification includes a two-week residential training course for SLTT officers on activities to disrupt, seize control of, disable, damage, or destroy a UAS. An abbreviated program is available for those operating only at correctional facilities. The July 2026 IFR indicates that the mitigation course includes "instruction on the legal, operational, and technological aspects of C-UAS operations…including [Federal Aviation Administration] coordination and airspace procedures, spectrum coordination requirements, real-time air traffic control notification procedures, FBI and DHS notification requirements, and the operational use of authorized mitigation technologies." Personnel engaging in mitigation actions must determine (using a totality of the circumstances standard) that a credible threat exists before taking any action, and any action taken must be proportionate to the threat.

Agency Implementation Policy. Any SLTT agency conducting C-UAS activities under the July 2026 IFR must adopt an agency implementation policy that, among other provisions, designates an Agency Approving Official and authorized personnel to engage in C-UAS activities, details tactical procedures for C-UAS operations, contains public notification provisions, and outlines procedures for data handling, retention, and dissemination. Agencies engaging only in detection and warning activities need not include details of tactical C-UAS procedures. Each agency must annually attest to their implementation policy through the NCUTC portal.

Authorized Technologies Lists. There are two lists to which agencies exercising C-UAS authorities under the July 2026 IFR must adhere. The IFR notes that "the Authorized Technologies List identifies the technology categories authorized for SLTT law enforcement and correctional agency C-UAS operations. The Authorized Systems List identifies specific systems, at the make and model level, that have completed interagency evaluation within those technology categories and stated operating restrictions."

C-UAS Operations Plan and Coordination. Each mitigation operation or detection and warning operation conducted under the July 2026 IFR must be authorized by a C-UAS Operations Plan signed by an Agency Approving Official. This is an event/operation-specific document. However, facilities with ongoing operations, such as correctional facilities and critical infrastructure sites, may receive a standing approved plan for up to 365 days. Each plan must contain specified information on the operation and a risk-based assessment of engaging in the C-UAS activities. Additionally, before conducting any mitigation operation, an SLTT agency must submit an advance notification document through the NCUTC portal, identifying certain details about the operation. Any SLTT agency activating a C-UAS system for mitigation must notify the Federal Aviation Administration (FAA) within five minutes for real-time coordination.

Privacy and Civil Liberties. The July 2026 IFR requires SLTT agencies and personnel to comply with certain privacy and civil liberties protections when exercising the C-UAS authorities. For example, the IFR specifies that no C-UAS authority may be used "solely to seize, monitor, deter, interfere with, or disrupt individuals exercising rights protected by the First Amendment."

C-UAS Reporting. Within 48 hours after taking a mitigation action or confiscating a UAS under the authority of 6 U.S.C. §124n, an agency must report relevant information, including operational effects, statistics, and unintended consequences, through the NCUTC portal. Each SLTT agency engaging in C-UAS actions under the July 2026 IFR must also provide a semi-annual report covering data on all C-UAS operations, not just mitigation actions.

Policy Considerations

DOJ and DHS opened the July 2026 IFR to public comment on several aspects, including on data retention requirements and "whether [C-UAS] certifications should expire, the length of their validity period, and the requirements for renewal." In addition to examining how the IFR may be amended for the final rule, Congress may look to relevant issues not addressed in the IFR. For instance, Congress may examine the FBI's capacity to train SLTT agencies applying for the two certification programs. As of July 1, 2026, the NCUTC had trained 61 officers across 46 agencies. The NCUTC had previously prioritized training officers in cities hosting FIFA World Cup events, and Congress may examine future training priorities. They may also look at potential barriers to SLTT agency participation in the training and certification programs. For example, the online NCUTC detection and warning certification is offered at no cost to participating law enforcement and correctional officers. However, Congress may examine whether cost adversely affects SLTT agencies' ability to attend the two-week residential mitigation training and certification program and explore paths (in addition to DHS's C-UAS Grant Program) to financially support agencies' participation.

Kristin Finklea, Specialist in Domestic Security

IF13279

Disclaimer