



September 4, 2026

Steve Willoughby
Acting Executive Director
Program Executive Office for Drones
and Counter-Unmanned Aircraft
Systems
U.S. Department of Homeland Security
Washington, D.C. 20024

Micheal J. Torphy
Assistant Section Chief
Unmanned Aviation Section,
Critical Incident Response Group
Federal Bureau of Investigation
U.S. Department of Justice
Washington, D.C. 20535

**Re: Comments on the Department of Homeland Security and Department of Justice;
Interim Final Rule; Counter-UAS Authority for State, Local, Tribal, and Territorial Law
Enforcement and Correctional Agencies (Docket No. FBI-2026-0001)**

Dear Mr. Willoughby and Mr. Torphy:

The U.S. Chamber of Commerce (the “Chamber”) welcomes this opportunity to comment on the Department of Homeland Security’s (“DHS”) and Department of Justice’s (“DOJ”) interim final rule (“IFR”) on *Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies*.¹

The Chamber respectfully submits the following comments in response to the IFR published jointly by DOJ and DHS implementing the SAFER SKIES Act's framework for State, Local, Tribal, and Territorial (“SLTT”) law enforcement and correctional agencies to conduct Counter-UAS (“CUAS”) operations.

Implementation of the SAFER SKIES Act is an important step toward strengthening the nation's ability to address the growing threat posed by malicious or unauthorized unmanned aircraft systems (“UAS”). We support the Departments' efforts to establish a framework that enables SLTT agencies to conduct safe, accountable, and effective CUAS operations while ensuring there are guardrails in place to prevent harmful interference to lawful communications as SLTT agencies and correctional facilities begin to deploy radiofrequency (“RF”) C-UAS measures nationwide. At the same time, the Chamber recommends two aspects of the interim final rule be revised to strengthen protections for critical infrastructure and help ensure homeland security.

¹ Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies, Interim Final Rule, 91 Fed. Reg. 41466, Docket No. FBI-2026-0001 (rel. July 6, 2026) (“IFR”).

I. The Importance of Critical Infrastructure

The IFR defines critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”.

Critical infrastructure, including energy facilities, transportation systems, communications networks, defense industrial base facilities, and large public venues faces an increasingly significant threat from malicious and unauthorized drone activity. Congress appropriately recognized this risk by including "critical infrastructure" among the protected interests for which SLTT agencies may exercise C-UAS authority under 6 U.S.C. § 124n(a)(2).

II. The Final Rule Should Expand Mitigation Training Capacity

The IFR designates the FBI's National Counter-UAS Training Center ("NCUTC") in Huntsville, Alabama as the national schoolhouse and sole certifying authority for personnel exercising mitigation authorities under 6 U.S.C. 124n(b)(1)(C), (D), and (F). However, demand for qualified personnel to exercise the authorities under the SAFER SKIES Act will far exceed the current training capacity. As of July 2026, personnel at only 46 agencies received mitigation training from the NCUTC. This pace of training of SLTT authorities at NCUTC is insufficient to adequately protect strategically important critical infrastructure sites across the country.

While the Chamber supports the use of a standardized curriculum and centralized oversight to ensure safe, lawful, and consistent use of mitigation authorities and technology and supports the IFR's recognition of the potential for interference with communications systems, limiting instruction to a single training location creates an unnecessary bottleneck. Section 124.5(d)(3) of the IFR states the Attorney General may authorize the training to be given at additional sites, so long as the NCUTC retains control over the curriculum, with such authorization at the sole direction of the Attorney General.

The Chamber strongly supports this provision and urges the Attorney General to exercise this authority to increase the availability of this training at additional sites across the country. We recommend the Final Rule require the establishment of additional training sites, or, at a minimum, require the Attorney General to develop, report on, and implement a plan for expanding mitigation training to meet state and local demand while ensuring that there are guardrails in place to manage any potential harmful interference to communications systems from mitigation technologies.

III. Concern about Implicit Curtailment of Certain Detection Technologies

The second issue concerns the treatment of certain detection technologies. The Chamber urges DOJ and DHS to use this rulemaking to clarify that the Pen Trap/Trace and Wiretap Acts do not apply to detection activities that are being carried out for core security purposes and do not involve capture of any sensitive information. Absent clarification, the Final Rule risks unintentionally discouraging or limiting the use of passive detection technologies by critical infrastructure owners and operators.

The IFR distinguishes between technologies that require authority under 6 USC 124n, given otherwise applicable criminal law prohibitions, and those that do not trigger these prohibitions. Under the definition of detection and warning operations, the IFR describes “systems that do not require the authority of 6 U.S.C. 124n (including, for example, electro-optical, infrared, acoustic sensors, and radar).” This list notably excludes RF systems, creating ambiguity regarding a range of RF systems that have long been used for CUAS detection.

Separate guidance seems to suggest that any system that can “detect, intercept, and analyze” RF signals is prohibited, even if it is used simply to gather non-sensitive data, such as UAS telemetry, location, altitude, speed, trajectory, battery level, and flight mode. This technology is of critical importance to critical infrastructure owners and operators that rely on RF technology to identify the location and trajectory of drones over their facilities, in ways that do not involve the collection of communications or other sensitive data.

Notably, the Federal Aviation Administration’s recently issued Notice of Proposed Rulemaking, *Designation-Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility*, pursuant to which critical infrastructure owners and operators would be able to apply for flight restrictions over their fixed-site facilities, asks applicants to “describ[e] unmanned aircraft operations in close proximity to the facility during the previous 24 months” and to continue to monitor flight patterns, something that most applicants will be unable to do without the aid of key RF technologies.

This concern is not speculative. FAA’s proposed Section 2209 rule would itself require fixed-site facility operators seeking an unmanned aircraft flight restriction to maintain the capability, directly or through a contracted service, to receive broadcast Remote ID from unmanned aircraft operating within or near the facility. Proposed 14 C.F.R. § 74.56(d), 91 Fed. Reg. 24650, 24687 (May 6, 2026). Remote ID reception is itself a form of RF-based detection. But as commenters in that docket have observed, Remote ID reception alone is an inadequate security measure precisely because operators engaged in intentional malicious, disruptive, or criminal activity are the least likely to broadcast compliant Remote ID—meaning that facilities seeking to meet FAA’s own risk-based

showing under proposed 14 C.F.R. § 74.100 will, in practice, need broader RF detection capability beyond bare Remote ID reception to identify and respond to genuine threats. Any DOJ/DHS interpretation that casts ambiguity over RF-based detection generally would therefore not only affect passive security monitoring in the abstract but would directly undermine a detection capability that a companion federal rulemaking is contemporaneously asking these same facilities to build.

There is a risk that the rule, as written, could meaningfully curtail private-sector entities' ability to conduct basic drone detection. This would undermine critical infrastructure security and runs counter to FAA guidance under the proposed Section 2209 rule.

IV. Conclusion

The SAFER SKIES Act provides an important opportunity to strengthen the nation's ability to respond to evolving drone threats and ensure homeland security. The Chamber appreciates the opportunity to provide these comments, and we look forward to continued engagement with the Departments on this critical issue.

Sincerely,



Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce



Chris Roberti
Senior Vice President
Cyber, Space, and National Security Policy
U.S. Chamber of Commerce