

AUTHORIZED TECHNOLOGIES LIST

The interagency list of authorized technology categories for SLTT counter-UAS operations.

AUTHORIZED & MAINTAINED JOINTLY BY

DOJ

Department of Justice

DHS

Department of
Homeland Security

DOW

Department of War

DOT/FAA

Federal Aviation
Administration

FCC

Federal Communications
Commission

NTIA

Telecommunications
& Information Admin.

This is the initial list of authorized technology categories for Counter-Unmanned Aircraft System (C-UAS) operations by State, local, Tribal, and territorial (SLTT) law enforcement or correctional agencies to take the actions described in 6 U.S.C. § 124n(b)(1).

CONSISTENT WITH

§ 8606(a)(4), SAFER SKIES Act

6 U.S.C. § 124n(d)(2)(A)(iii)

6 C.F.R. § 124.7

28 C.F.R. § 124.7

APPLICABILITY

This list applies only to technology categories whose operation requires the legal authorities and relief from certain laws provided by 6 U.S.C. § 124n(a)(2).

COMPANION LIST - ASL

Specific systems authorized within these categories (make and model) are published in the Authorized Systems List (ASL), 28 C.F.R. § 124.7(b).

AUTHORIZED TECHNOLOGY CATEGORIES

ATL-1 RF detection with command-and-control signal interception

Systems that detect, intercept, and analyze radio frequency (RF) signals used for command-and-control between a ground control station (GCS) and an unmanned aircraft system (UAS), using detailed knowledge of UAS communication protocols to demodulate, decode, or decrypt data packets in real time. This can provide access to signal information and content such as:

- UAS identification — make and model, serial number, registration, media access control (MAC) address, or other unique identifier, including a device or subscriber identifier used by a cellular- or satellite-controlled UAS
- Packet details, such as source and destination addresses
- RF parameters, such as channel frequency and signal strength
- UAS telemetry, such as location, altitude, speed, trajectory, battery level, and flight mode
- The estimated position of the operator or control station
- Video data necessary to the command and control of the UAS

ATL-2 RF protocol manipulation

Systems that exploit weaknesses in the RF communication protocol between a GCS and a UAS in order to disrupt, redirect, or assume control of the UAS.

ATL-3 RF disruption (broadband and protocol-specific jamming)

Systems that interfere with the RF communications used to control a UAS by transmitting high-power signals on the same frequencies as the UAS command-and-control link, telemetry, and/or video links, in order to disrupt the UAS RF link(s). This category is limited to communications used to control the UAS within the meaning of 6 U.S.C. § 124n(b)(1)(A) and does not by itself authorize disruption of Global Navigation Satellite System (GNSS) signals or general cellular network services that are not part of the UAS command-and-control link. Authorization under this category does not extend to system configurations that employ GNSS or cellular disruption capabilities; any potential future use of such capabilities by SLTT law enforcement and correctional agencies requires separate evaluation and the updating of this list through the interagency process.

Due to the rapidly evolving nature of the technology and commercial solutions landscape, this initial list is expected to change in the future to allow SLTT law enforcement or correctional agencies other technology solutions. Interagency stakeholders are expected to establish processes for further revisions to the ATL.

PUBLISHED & MAINTAINED ON THE

Interim Federal C-UAS Coordination Portal

Operated by the Federal Bureau of Investigation, Critical Incident Response Group.

justiceconnect.cjis.gov/communities/community/cuas

Access to the portal is limited to authorized users.

The United States does not endorse, recommend, or certify any vendor, system, or manufacturer.

The SAFER SKIES Act is Pub. L. 119–60, div. H, title LXXXVI, 139 Stat. 1944 (2025).

The Department of Defense is also known as the Department of War (E.O. 14347, 90 FR 43893 (Sept. 5, 2025)).