

Photo: United States Capitol · Noclip · Public domain · Wikimedia Commons

OSINT · POLICY ASSESSMENT

ALLOWED TO LISTEN, NOT TO SHOOT

For years, almost no one in the United States outside four federal departments could lawfully interfere with a drone, and even detecting one could raise questions under surveillance law. That changed in December 2025, when Congress extended counter-drone authority to trained state and local police. This report sets out the new rules in plain terms: who may detect, who may stop, and why the choice of sensor still matters. It is analysis, not legal advice.

REPORT DETAILS

PUBLISHED	SUBJECT	SOURCE BASE
October 2026	Who may detect and who may mitigate drones under U.S. law	Federal interagency advisory (2020), SAFER SKIES Act implementing rule (2026), legal and trade analysis
METHOD	**VERDICT**	**NOTE**
Read the primary guidance; separate detection from mitigation; flag what remains unsettled	The law now has two tiers; sensors that don't intercept communications sit on the firmest ground	Analysis, not legal advice
CONFIDENCE	**AUTHOR**	
Moderate	Ghulam Mujtaba, Ph.D.	

BOTTOM LINE

In the United States, the right to stop a drone is now shared with trained local police, but not with the people who own the places drones threaten, and the legal position of detection depends on how the sensor works. Until December 2025, Congress had authorised only four federal departments to counter drones, and even detection systems could fall foul of federal wiretap and pen-register laws. The SAFER SKIES Act, passed in the FY2026 defence bill, lets certified state, local, tribal and territorial agencies detect drones and, with further training, disable them. Private utilities, venues and companies still have no mitigation authority. For them, and for the agencies, the federal government's 2020 guidance points to sensors that detect the drone itself (radar, optical and acoustic) as less likely to raise surveillance-law concerns than systems that intercept drone communications.

4

FEDERAL DEPARTMENTS WITH COUNTER-DRONE AUTHORITY BEFORE 2025

◆ DEFENSE, ENERGY, JUSTICE, HOMELAND SECURITY

1 July 2026

STATE AND LOCAL POLICE GAIN CERTIFIED C-UAS AUTHORITY

◆ SAFER SKIES ACT IMPLEMENTING RULE

2 tiers

DETECTION AND WARNING, THEN MITIGATION

◆ SEPARATE FBI CERTIFICATION FOR EACH

0

MITIGATION POWERS GRANTED TO PRIVATE OPERATORS

◆ UTILITIES, VENUES, COMPANIES

KEY QUESTIONS

Who can legally stop a drone in the United States?

Federal agencies with express authority from Congress (Defense, Energy, Justice and Homeland Security) and, since July 2026 under the SAFER SKIES Act, state, local, tribal and territorial law enforcement and correctional agencies that complete FBI certification. Private companies and property owners are not given mitigation authority.

Is it legal to detect drones in the United States?

Detection is far less restricted than mitigation, but it depends on how a system works. A 2020 federal advisory says sensors such as radar, EO/IR and acoustic systems, which sense the drone itself rather than intercepting its communications, are less likely to raise concerns under federal surveillance laws. Radar also needs an FCC licence. Operators should take legal advice.

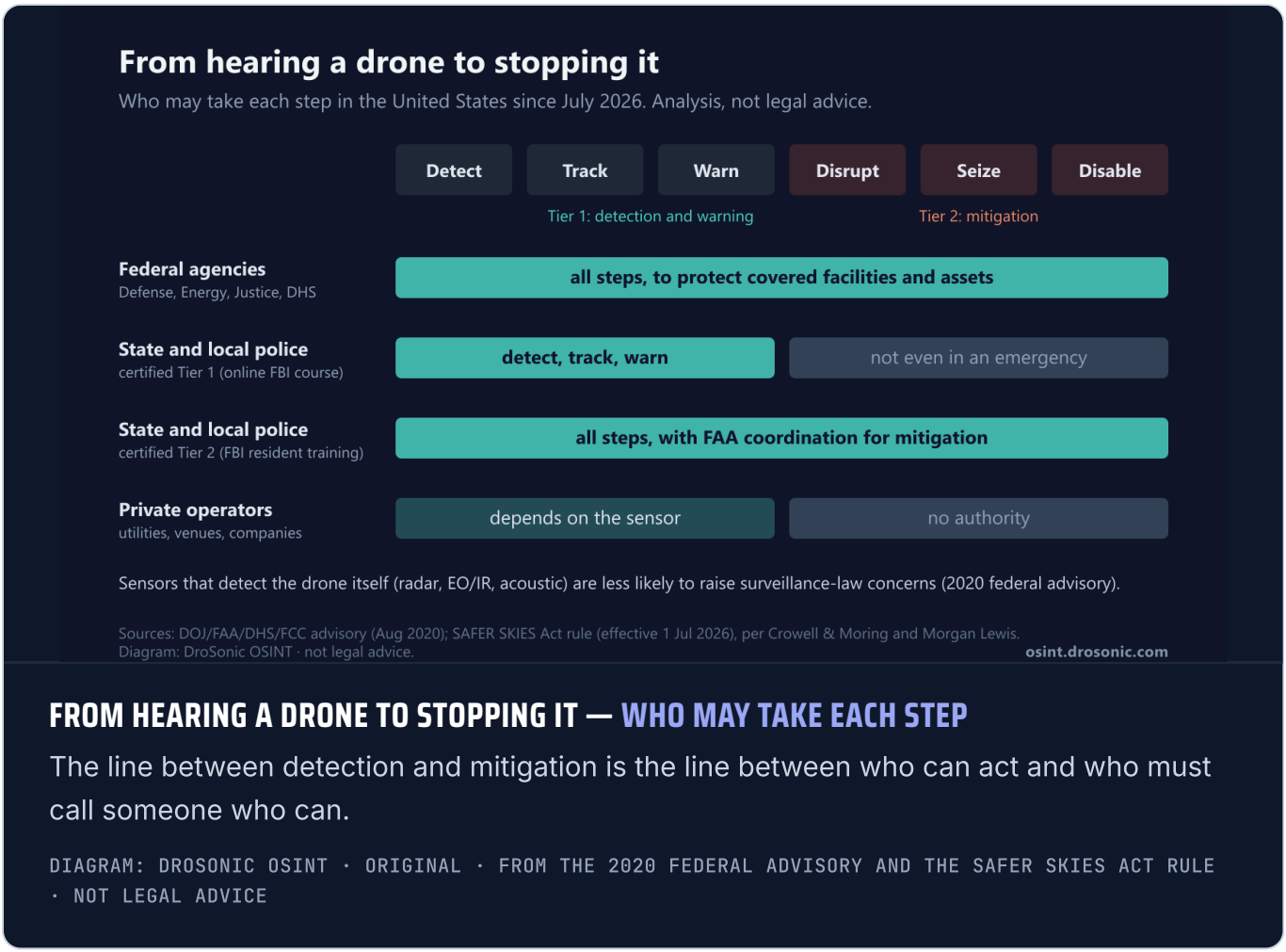
Can local police use drone detection without federal certification?

For some sensors, yes. SAFER SKIES certification covers the systems on its approved lists, which were RF-only in late summer 2026. In September 2026 the Police Executive Research Forum advised police chiefs that Remote ID reception, cameras, acoustic sensors and radar need no federal certification and can be deployed today, subject to FCC and FAA rules.

Who may do what

WHO	DETECT, TRACK, WARN	DISRUPT, SEIZE, DISABLE
FEDERAL: DEFENSE, ENERGY, JUSTICE, HOMELAND SECURITY EXPRESS AUTHORITY	Yes, under their statutes	Yes, to protect covered facilities and assets
STATE, LOCAL, TRIBAL AND TERRITORIAL POLICE SAFER SKIES ACT NEW	Yes, after FBI Tier 1 certification	Yes, after FBI Tier 2 resident training
PRIVATE OPERATORS UTILITIES, VENUES, COMPANIES, AIRPORTS' OWN STAFF	Depends on the sensor and applicable law	No
PASSIVE ACOUSTIC SENSORS E.G. DROSONIC'S	Listening only: no transmissions and no access to communications	No: they detect and cue; action stays with authorised agencies

SINCE 1 JULY 2026 · ANALYSIS, NOT LEGAL ADVICE; SOURCES BELOW



FROM HEARING A DRONE TO STOPPING IT — WHO MAY TAKE EACH STEP

The line between detection and mitigation is the line between who can act and who must call someone who can.

DIAGRAM: DROSONIC OSINT · ORIGINAL · FROM THE 2020 FEDERAL ADVISORY AND THE SAFER SKIES ACT RULE · NOT LEGAL ADVICE

FIELD 01 — BEFORE 2025

Four departments and a legal minefield

For most of the drone era, U.S. law treated counter-drone activity as something only a handful of federal agencies could do. A joint 2020 advisory from the Justice Department, FAA, Homeland Security and FCC put it directly: "Congress has exclusively authorized the Departments of Defense, Energy, Justice, and Homeland Security to engage in limited UAS detection and mitigation activities" against drones threatening covered facilities, notwithstanding federal criminal laws that might otherwise apply. U.S. DOJ, FAA, DHS & FCC↗

The advisory's central warning concerned **surveillance law**. Whether a detection system risks breaching the federal Wiretap Act or Pen/Trap Statute, it said, "depends on whether it captures, records, decodes, or intercepts, in whole or in part, electronic

communications transmitted to and from a UAS and/or controller." It added that the legal analysis turns on how each system actually works, "not ... broad classifications of systems (e.g., active versus passive, detection versus mitigation)". U.S. DOJ, FAA, DHS & FCC↗

FIELD 02 — THE SENSOR MATTERS

Sensing the drone versus reading its signals

The advisory then drew the distinction that matters most for detection technology:

> **Detection systems "such as radar, EO/IR, and acoustic systems" sense "the sound or electromagnetic waves produced by or reflected from the UAS" and "are less likely to pose concerns under federal criminal surveillance statutes."**

The reason is that such sensors "do not capture, record, decode, or intercept electronic communications." They detect the drone's physical presence, not the messages between drone and pilot. Systems that work by intercepting or decoding drone radio links are the ones that need the most careful legal analysis. U.S. DOJ, FAA, DHS & FCC↗

That does not make any sensor automatically lawful. The advisory stresses that every system must still comply with FCC and FAA rules, and that state and local laws may apply. Radar, for example, emits radio energy and requires an FCC Radiolocation Service licence. Passive sensors that emit nothing, such as microphones and cameras, avoid that particular requirement.

FIELD 03 — THE CHANGE

The SAFER SKIES Act

In December 2025 Congress passed the **SAFER SKIES Act** as part of the FY2026 National Defense Authorization Act. It extends counter-drone authority, under 6 U.S.C. § 124n, to properly trained state, local, tribal and territorial law enforcement and correctional agencies. Crowell & Moring↗ The Justice Department and Homeland Security issued an interim final rule, effective 1 July 2026, that sets up two tiers:

— **Tier 1, detection and warning:** detect, identify, monitor and track drones and warn operators, after online certification.

— **Tier 2, mitigation:** disrupt, seize control of, or disable a drone, after hands-on training at the FBI's National Counter-UAS Training Center. Tier 1 personnel cannot take Tier 2 action, "even in an emergency."



A HANDHELD DRONE JAMMER — TIER 2 TERRITORY

Jamming is mitigation. In the United States it is reserved for certified government agencies and raises aircraft-sabotage and spectrum-law issues for anyone else.

PHOTO: VOIDWANDERER · CC BY-SA 4.0 · WIKIMEDIA COMMONS

Agencies may deploy only technologies on federally maintained authorised lists, mitigation generally requires FAA coordination and real-time notice to air traffic control, and the FCC created a temporary nationwide authority for qualifying agencies to run approved RF-based systems. Morgan Lewis↗ Penalties for knowingly skipping required federal steps can reach $100,000 per violation. Crowell & Moring↗

The early lists are narrow. According to LE Drones, a law-enforcement drone supplier, radio-frequency systems were the only approved technology category as of late summer 2026, with 21 systems listed, and authority may be exercised only by an agency's own certified officers, never by contractors. LE Drones↗

FIELD 04 — WHAT'S STILL MISSING

The private operator's position

The new law helps the places drones threaten mostly through the police who protect them. Stadiums, utilities, prisons, airports and critical-infrastructure owners benefit, but the authority sits with government agencies. Trade coverage of the Act notes that other facilities could monitor their airspace continuously only "if given the authority to do so".[Facilities Dive↗] No private operator has gained the right to jam, seize or shoot down a drone.

That leaves three open questions:

1. **Private detection.** What a utility or venue may run on its own property is still governed mainly by the 2020 analysis: the less a sensor touches drone communications, the firmer its footing.
2. **Technology lists.** Lists that start with RF-only systems leave agencies without approved options against drones that transmit nothing, the fibre-optic and autonomous drones now common in Ukraine. Passive detection sits outside the rule: in September 2026 the Police Executive Research Forum advised police chiefs that "Remote ID reception, cameras, acoustic sensors, and radar require no federal certification and can be deployed today, subject to the FCC and FAA restrictions governing each."[PERF↗]
3. **Coordination.** The February 2026 airspace closure at El Paso (Thirty-Four Thousand Flights), which followed the uncoordinated use of a counter-drone laser, showed what happens when counter-drone action and aviation safety are not joined up.[Wikipedia↗]

CONFIDENCE

How sure we are, and what would change it

High confidence in the primary texts quoted: the 2020 interagency advisory and the existence, date and two-tier structure of the SAFER SKIES rule.

Moderate confidence in details of the implementing rule (approved-technology lists, FCC actions), which come from law-firm and trade analysis of a rule still open to revision after its comment period.

This is not legal advice. Anyone deploying detection or mitigation technology should consult counsel familiar with federal and state surveillance, aviation and communications law, as the 2020 advisory itself recommends.

DROSONIC — OUR APPROACH

Built for the side of the law that leaves room

DroSonic's sensors only listen. They detect, classify and locate drones by propeller sound using neural networks on low-cost edge hardware, and they transmit nothing and read none of a drone's signals.[DroSonic↗] That puts them on the detection side of the line this report draws, which is open to far more operators than mitigation.

Its U.S. provisional patent application covers detection, classification, localisation and tiered defeat cueing,[DroSonic↗] the cue being for whoever is legally authorised to act. A prototype was tested against live drones at DIRT Days 26.04 in September 2026.[DroSonic↗] This is our reading of the law, not legal advice.



DIRT DAYS 26.04 — SENSING, NOT INTERCEPTING

DroSonic's test position at the field exercise. Listening for a drone reads none of its signals.

PHOTO: DROSONIC · FIELD-TEST WRITE-UP

CLOSE — WHAT IT MEANS

Detection is where the law leaves room

The legal map of U.S. drone defence now has a clear shape. Stopping drones is for certified government agencies, under federal training and supervision. Detecting them is open more widely, and its legal footing depends on how the sensor works. Sensing the drone itself (its echo, image or sound) is on firmer ground than intercepting what it says.

That is one reason passive acoustic detection suits critical-infrastructure operators and the agencies that protect them. It emits nothing, needs no spectrum licence, and senses a drone's sound rather than its communications, including drones that send no radio signal at all. At DroSonic we expect approved-technology lists to widen beyond RF as fibre-optic and autonomous drones spread, and we are building for that. Our explainer What a Microphone Can Hear covers how the technology works.

ABOUT DROSONIC

DroSonic builds passive acoustic drone detection: networked sensors that listen for drones instead of their radio signals, using acoustic AI and edge computing. DroSonic OSINT is our open-source research into the threat that technology is built to meet.

THE RECORD SO FAR

OCT 2026	Joined the SOF RACER consortium, which connects USSOCOM with commercial technology companies
SEPT 2026	Prototype tested against live drones at DIRT Days 26.04, a field exercise supported by CMI2 with U.S. Central Command and U.S. Army DEVCOM
SEPT 2026	Technical presentation at NDIA's Emerging Technologies for Defense conference on detecting fibre-optic and radio-silent drones
SEPT 2026	Filed U.S. provisional patent 64/148,522 on passive acoustic detection, classification, localisation and defeat cueing
JUL 2026	Pitched to the U.S. Space Force at Space Systems Command's Reverse Industry Engagement Day, Colorado Springs

How DroSonic detection works → · Where it is used → · Talk to the team →

THIS REPORT ONLINE

https://osint.drosonic.com/assessments/us-counter-drone-law-detection.html

Cite as: Mujtaba, G. (2026, October 9). *Allowed to Listen, Not to Shoot: Law Enforcement Drone Detection and Mitigation: U.S. Law Explained*. DroSonic OSINT. https://osint.drosonic.com/assessments/us-counter-drone-law-detection.html

Reusing this report. Text and original diagrams © DroSonic. You may quote this report and share its link with credit to DroSonic OSINT; to republish it in full, reuse our diagrams or use it commercially, contact us first. Photos and third-party figures keep the licences shown in their credits.

DroSonic OSINT: open-source assessments on drones and counter-UAS from DroSonic, passive acoustic drone detection. drosonic.com · sudo@drosonic.com



ABOUT THE AUTHOR

Ghulam Mujtaba, Ph.D.

FOUNDER AND CEO, DROSONIC

Ghulam Mujtaba, Ph.D., is the founder and CEO of DroSonic and leads its work on passive acoustic drone detection. A computer engineer with 13 years of experience building machine-learning systems for edge hardware, he holds a Ph.D. in computer engineering from Gachon University in South Korea, was an NSF postdoctoral fellow at West Virginia University in the United States, and is an Assistant Professor of AI and Data Science at Regis University in Denver, Colorado. An IEEE Senior Member, he has published more than 20 papers on deep learning, computer vision and multimedia for edge devices.

PROFILE ↗ LINKEDIN ↗ ORCID ↗

ALL SOURCES (10)

1. U.S. DOJ, FAA, DHS & FCC — Advisory on the application of federal laws to UAS detection and mitigation, August 2020
2. Crowell & Moring — SAFER SKIES Act in FY2026 NDAA; IFR effective 1 July 2026; two tiers
3. Morgan Lewis — Authorised technology lists; FAA coordination; FCC special temporary authority for RF-based systems
4. LE Drones — RF the only approved category late summer 2026; 21 systems; never by contractors
5. Facilities Dive — Authority rests with certified government agencies; private facilities not granted it
6. PERF — Police Executive Research Forum, A Clear and Present Danger: The Rise of Malicious Drones and What Police Executives Can Do About It, September 2026, PDF pp. 15 and 49: two tiers of detection; acoustic sensors need no federal certification; methods outside the SAFER SKIES rule remain available
7. Wikipedia — El Paso closure, February 2026; laser use not coordinated with the FAA
8. DroSonic — Passive acoustic detection: neural networks on low-cost edge hardware, no emissions
9. DroSonic — U.S. provisional patent application 64/148,522, September 2026
10. DroSonic — DIRT Days 26.04 field test, September 2026