SAFER SKIES ACT · INTERIM FINAL RULE · Q&A

COUNTER-DRONE AUTHORITY: QUESTIONS & ANSWERS

ISSUED JOINTLY BY

U.S. DEPARTMENT OF JUSTICE | U.S. DEPARTMENT OF HOMELAND SECURITY

Effective July 2026

Q&A · v1.0

Fifty plain-language answers on the SAFER SKIES interim final rule — for chiefs, sheriffs, wardens, and agency counsel weighing whether, and how far, to opt in.

START HERE — THE BASICS

Q01 What is this rule?

An interim final rule issued on July 1, 2026, jointly by the **Departments of Justice and Homeland Security**, implementing the SAFER SKIES Act (signed December 18, 2025). It sets the conditions under which state, local, tribal, and territorial (SLTT) agencies may lawfully counter drone threats. It is in force now, with a 60-day public comment period.

6 & 28 CFR Part 124

Q02 Does it apply to my agency?

If you are an SLTT **law enforcement or correctional agency**, yes — you are eligible. The authority may be exercised only by your own officers and employees, never by contractors or private security. § 124.4

Q03 Are we required to do anything?

No. The rule is entirely opt-in. An agency that conducts no counter-UAS (C-UAS) operations has no new obligations. However, confirm that your current equipment does not rely on the Act's legal relief — some detection gear you may already use does, and comes into scope. See **Q14**.

Q04 What actually changes?

Until now your certified operators could act only as part of a **federal task force**, under federal sponsorship and deputation. The rule lets an accredited agency act **on its own authority, in its own jurisdiction** — coordinated through the Federal C-UAS Coordination Portal, but no longer dependent on a federal operation.

Q05 What can a certified agency do?

At the **Detection & Warning** tier: detect, identify, monitor, and track drones — including intercepting the radio link that controls them — warn the operator, and seize a drone. At the **Mitigation** tier: disrupt, disable, take control of, or, using reasonable force, damage or destroy a threatening drone. § 124.3

Q06 What can we never do, even certified?

Act against **any aircraft with a pilot, crew, or passengers aboard**; use the authority as a general investigative or surveillance tool; let uncertified personnel operate; or use equipment that is not on the authorized lists. The authority exists to protect against drone threats — nothing more. §§ 124.3, 124.20

Q07 What are we allowed to protect?

The four interests the statute names: **people, facilities, and assets**; venues for **large-scale public gatherings or events**; **critical infrastructure**; and **correctional facilities** — against a credible drone threat.

Q08 How long does this authority last?

The statutory authority **terminates December 31, 2031** unless Congress extends it; obligations arising before then survive. The rule itself is effective immediately, and the Departments are taking comment on nearly every design choice — see page 6. § 124.21

Q09 Drones aren't a daily problem here. Why act now?

Because the threat is growing faster than most jurisdictions expect: contraband drops over prison walls are now a **routine smuggling method**, incursions over stadiums, airports, and mass gatherings are documented and recurring, and weaponized-payload plots have been federally charged. The question is less *whether* than *which tier*.

Q10 What does this actually cost?

The paperwork is the small part — roughly **33 hours/year** for a detection-tier agency, ~150 for a mitigation-tier agency, 15 minutes for the annual attestation, ~45 minutes per post-operation report. The real cost is **staffing and sustainment**: operators pulled from other duties, equipment acquisition and maintenance, legal review, and recurring proficiency training.

Q11 Is there federal funding?

Yes. The **FEMA C-UAS Grant Program** totals $500M across FY26–27: $250M already awarded to FIFA World Cup and America 250 jurisdictions, and $250M expected to open to all 56 states and territories this fall through your State Administrative Agency. Detection is broadly eligible; mitigation funding requires personnel trained or scheduled at the FBI's **National Counter-UAS Training Center (NCUTC)**. Byrne JAG and COPS funds may also purchase authorized systems with prior BJA approval.

Q12 We're a small or rural agency. Is this realistic for us?

You don't need your own program. Under **mutual aid**, an accredited agency — a regional, county, or state partner — can provide C-UAS coverage to non-accredited neighbors by written arrangement. Nothing in the rule requires a resource-limited agency to buy equipment or seek accreditation. § 124.4(c) SEEKING COMMENT

Q13 Can a contractor run it for us?

No. Only your officers and employees may operate mitigation systems or make threat determinations — "turnkey" and managed C-UAS services are expressly barred. You also can't route around that by having an accredited agency lend its name while another party actually runs the system. Contractors may still design, install, maintain, and train on systems, and provide detection services that don't need the Act's authority. § 124.4

Q14 We already operate drone detection gear. Are we affected?

Depends on the gear. **Cameras, radar, acoustic sensors, passive RF energy detection, and Remote ID receivers** are outside the rule — unchanged. Systems that **intercept the drone's control link** likely rely on the Act's legal relief, so they require the online Detection & Warning Certification, a short policy, and an Operations Plan. An agency can come into compliance in days, at about an hour of operator time. § 124.12

Q15 Our officers are already on a federal C-UAS task force.

Keep it. Task force and deputization arrangements continue **unchanged and without accreditation** — they run on separate federal authority. Accreditation is an add-on that lets your agency also act independently; the two coexist, and holding both is a **strong SLTT–federal partnership posture for high-risk or high-threat events**. § 124.19

Q16 We only care about our jail or prison.

The rule is built for you: correctional facilities are a named protected interest, an abbreviated **Correctional Mitigation Certification** covers personnel operating only at correctional facilities, and a fixed site can hold a **365-day standing** Operations Plan instead of monthly renewals. §§ 124.5(e), 124.8

CERTIFICATION & ACCREDITATION

Q17 What are the two certification tiers?

Detection & Warning — find, track, identify, warn, and seize; no interference with the aircraft. **Mitigation** — the authority to stop a drone: disrupt, take control, or bring it down. Every action under the Act requires the matching tier; personnel holding only the detection tier may never mitigate. § 124.5

Q18 What does Detection & Warning certification take?

An online curriculum with a required assessment — about a **90-minute module** — delivered at **no cost** through the NCUTC Training Portal, with no application or waitlist. It is designed for broad certification across a workforce.

Q19 What does Mitigation certification take?

Resident training at the FBI's NCUTC (Redstone Arsenal, AL) — a two-week course with hands-on system stations and a live capstone exercise. Congress made the national schoolhouse the **sole certifying authority** for mitigation; there is no equivalency or online path. Every candidate must already hold the online **Detection & Warning Certification** — it is a prerequisite to enroll. Enrollment is expanding through late 2026.

Q20 Is there a shorter path for correctional officers?

Yes. An abbreviated **Correctional Mitigation Certification** with a correctional-specific curriculum covers personnel who operate only at correctional facilities — narrower authority, proportionately lighter training. § 124.5(e)

Q21 How many certified operators do we need?

Fewer than you might think. **Only a Mitigation-certified operator may execute a mitigation command.** But a single graduate can lead a team whose other members hold the online Detection & Warning Certification — and those D&W operators are an important force multiplier in the Counter-UAS Tactical Operations Center (CUTOC). Scale residency slots to your operational tempo, not your roster.

Q22 What does the agency itself have to do?

Adopt an **implementation policy** (command responsibility, operator rostering, equipment control, privacy procedures, recordkeeping), have **agency counsel review it**, and **attest through the Federal C-UAS Coordination Portal** — that attestation is your accreditation gate. Detection-only agencies use the abbreviated model policy already published there. § 124.6

Q23 Does the federal government pre-approve our policy?

No — you self-certify. The Departments chose attestation over pre-approval to avoid a federal bottleneck across thousands of agencies. The accountability is on the back end: audits, and suspension exposure for an agency that attests falsely or maintains a deficient policy. Treat the attestation as a real representation. §§ 124.6, 124.16

Q24 Do certifications expire?

Not under the current rule. The Departments are considering an expiration period — 36 or 48 months, tied to refresher training — and have specifically invited comment on whether certifications should expire, for how long, and what renewal should require.

SEEKING COMMENT

Q25 Who signs off on operations inside the agency?

A designated **Agency Approving Official** at senior-executive rank (or the agency head where no equivalent exists). The rule deliberately places authorization of any C-UAS operation — detection or mitigation — with **an accountable command official**, above line-supervisor level.

§ 124.2

Q26 Can a certification be taken away?

Yes — **suspended**, in writing, with the basis and any remedial steps stated; immediately in exigent circumstances. There is no separate revocation: an uncured suspension simply stands, and reinstating a Mitigation Certification requires the full course again. The review process is on page 6 (**Q46**). § 124.5

Q27 What equipment may we use?

Only what the two federal lists allow. The **Authorized Technologies List (ATL)** approves categories of technology; the **Authorized Systems List (ASL)** names specific make/model systems within them. Until the ASL is populated for a category you may use any system in that category; once populated, you must use a **listed system**. § 124.7

Q28 What's authorized today?

The initial ATL covers three RF categories: **RF detection with control-signal interception**, **RF disruption** (broadband and protocol-specific jamming), and **RF protocol manipulation** (command injection / cyber takeover). The initial ASL lists 21 systems, drawn first from equipment with federal operational history, and populates in phases; the Departments expect to consider additional systems in fall 2026.

Q29 Are cameras, radar, and Remote ID receivers on the lists?

No — they don't need to be. The list requirement reaches only technology whose operation needs the Act's legal relief. Sensors you could lawfully operate before — cameras, radar, acoustic, Remote ID — stay available exactly as before. Any system that **emits RF**, though, still needs **FAA spectrum authorization** before it operates (see **Q30**).

Q30 Do we need FCC and FAA approval?

If the system **emits radio waves** — jammers, most radars — yes. ASL-listed systems now carry an **FCC standing authorization**, so a per-operation FCC filing is no longer the norm — but **FAA spectrum authorization is still required** before an RF emitter operates. § 124.9

Q31 If a system is on the ASL, is it endorsed and safe to buy?

No. The United States does not endorse, recommend, or certify any vendor, system, or manufacturer, and listing does not guarantee performance. Your agency remains responsible for its own procurement diligence and **cybersecurity assessment** — listed systems have completed federal technical review, not vendor vetting for you.

Q32 Can we get a system added, or flag a bad one?

Yes. Accredited agencies may **nominate systems** for the ASL and submit **feedback on listed systems** through the C-UAS-ASLN form on the Federal C-UAS Coordination Portal. § 124.7(f)

Q33 What if a system we own gets suspended?

On an interagency **emergency suspension notice**, you must cease use of that system or category immediately — even mid-deployment posture. Build the possibility into procurement risk: avoid single-system dependence for a mission-critical site. § 124.7(g)

Q34 Can we test and train with the equipment?

Yes, but **not under the Act's authority** — testing lacks the credible-threat predicate. Testing, proficiency training, and pre-operational validation run under a written activities plan with FCC authorization and FAA coordination, the same mechanisms federal programs use. § 124.18

BEFORE & DURING AN OPERATION

Q35 What has to happen before we operate?

A **C-UAS Operations Plan (OPLAN)** on the standard form, signed by your Approving Official with a counsel certification, plus **one portal submission** that routes automatically: to the FBI and DHS for deconfliction, the FAA for airspace and spectrum. You file once — no separate federal filings. Passive, non-emitting detection needs no per-operation coordination. §§ 124.8–124.9

Q36 How long does an authorization last?

30 days per operational window, renewable by updated submission — or a **365-day standing window** for fixed-site persistent protection (a prison, a utility plant), so an unchanged plan isn't resubmitted monthly. § 124.8

Q37 What about major events with multiple agencies?

For a nationally significant event, each participating agency files a **Notice of Intent**, engages in early coordination, and operates under a designated **lead C-UAS agency** running one tactical picture. An agency that declines the lead agency's tactical coordination **may not operate** within the covered area and period — because simultaneous RF systems interfere and two agencies may act on the same aircraft. § 124.10 SEEKING COMMENT

Q38 What happens at the moment of mitigation?

A documented **credible-threat determination** (an objective, reasonable-officer standard), an action **proportionate** to the threat, executed only by a Mitigation-certified operator — who retains discretion to decline an action they judge unsafe. Air traffic control is notified **within five minutes** or as soon as practicable, with a follow-up when the action ends. §§ 124.3, 124.11

Q39 Is there an emergency exception?

Yes, narrow: where a drone poses an **imminent risk to human life**, action may precede the usual coordination — with prompt notification and full reporting after the fact. It is an exception for genuine emergencies, not a workaround for skipped paperwork. § 124.9(g)

Q40 A drone lands carrying a suspected explosive. Is this a C-UAS problem?

No — it's a bomb squad problem. A suspected hazardous or destructive device delivered by drone must be handled by a bomb squad accredited through the FBI's Hazardous Devices School, under the national render-safe framework. Your C-UAS team hands off. § 124.17

AFTER THE OPERATION — REPORTING, RECORDS & PRIVACY

Q41 What do we report after a mitigation?

A report to DOJ and DHS **within 48 hours** — one portal filing covers both: date, time, and location; the credible threat; the capability used; and any known operational effects. Budget about 45 minutes. § 124.13

Q42 We protect the same site every week. Report every time?

For **detection** operations, no — the rule provides **consolidated, recurring-venue, and persistent-protection formats** that keep every statutory data element without duplicative per-event filings, and a semiannual operational summary supports the Departments' report to Congress. Each **mitigation** action still requires its own 48-hour report (see **Q41**). § 124.13

Q43 What privacy rules bind us?

The authority may never be used solely to monitor First Amendment–protected activity. Intercepted communications are minimized, used only for protective purposes, and **deleted within 180 days** absent a narrow, documented exception. Shared "pattern data" must meet written anonymization standards, and an audit trail backs it all. Quarterly minimization reviews apply to standing deployments. § 124.14 SEEKING COMMENT

Q44 Are our plans and coverage maps public records?

The rule requires you to protect operations plans, system locations, coverage patterns, and tactics under access controls — **to the extent your public-records law permits**. Capability-revealing detail is handled as law enforcement sensitive; general coordination information as CUI. Have counsel map your state's exemptions before you build the program. § 124.15

QUESTIONS YOUR COUNSEL WILL ASK

Q45 Which laws does certified action displace?

For authorized actions only: aircraft piracy (49 U.S.C. 46502), destruction of aircraft (18 U.S.C. 32), computer fraud (18 U.S.C. 1030), satellite interference (18 U.S.C. 1367), the Wiretap Act, and pen-register/trap-and-trace prohibitions — plus contrary SLTT law. **Not displaced:** the Communications Act, which is why FCC authorization still applies (**Q30**).

Q46 What's our exposure if we get it wrong?

Knowingly acting without required federal coordination risks a civil fine of up to **$100,000 per violation** and/or suspension, enforceable in federal court. Penalties are graduated by severity, with compliance history and corrective action weighed — and a **first procedural violation, self-reported in good faith, draws no penalty**. If suspended: written notice, 30 days to request administrative review, an independent DOJ reviewing official, and a written determination within 60 days.

§§ 124.5, 124.16 SEEKING COMMENT

Q47 Does the state have a veto? Do we owe the state notice?

Congress conferred the authority **directly on SLTT agencies** — nothing in the rule conditions it on state-level notification, endorsement, or approval. But if your **state law or policy** requires advance notification, the rule expects you to give it, and the Departments are weighing a formal state-awareness mechanism. § 124.9(b) SEEKING COMMENT

Q48 Does this create new liability for our officers? And who keeps a seized drone?

The rule creates **no enforceable right** in others and no new basis of liability for officers protecting identified mass gatherings — compliance with the framework is the shield. A confiscated drone is forfeited under **your jurisdiction's law**; a drone on the ground can be seized under ordinary authority, and FBI technical exploitation may be available through your field office. §§ 124.17, 124.20

Q49 What counts as a "credible threat"?

The trigger for every action. A credible threat is one that — on the **totality of circumstances** known to the operator at the time — would lead a **reasonable person in the operator's position**, given their training and experience, to conclude a drone poses an **articulable risk** to the people, place, or asset being protected. For detection and warning, a reasonable basis to *anticipate* such a risk can suffice. First Amendment–protected activity may never be a factor, and Fourth Amendment reasonableness still governs any search or seizure. §§ 124.2, 124.3

Q50 Can evidence from an operation be used in a prosecution?

Yes, within limits. The authority may never be used *solely* to gather evidence, and it is never a substitute for a wiretap or pen/trap order. But evidence obtained **incidental** to a lawful protective operation may be used in later criminal proceedings, consistent with applicable law — and counsel should coordinate with the prosecutor to limit disclosure of operationally sensitive detail. §§ 124.3, 124.15

STILL BEING DECIDED – THE DEPARTMENTS ASKED FOR YOUR VIEW

- Whether certifications should **expire** and what renewal requires
- A **state-awareness mechanism** — rosters or notification on adoption
- Privacy calibration — **retention exceptions**, anonymization standards, real-time feeds
- The **mutual aid** conditions for covering non-accredited agencies
- The **lead-agency** stand-down requirement at designated events
- The **penalty framework**, including first-violation treatment

Comments shape the final rule. Read the rule — including its **preamble**, which explains why each provision was crafted as it is — in the Federal Register, then submit by **September 4, 2026** at regulations.gov, Docket No. **FBI-2026-0001** — reference the specific section, explain the change you want, and attach supporting data.

GET STARTED

INTERIM FEDERAL C-UAS COORDINATION PORTAL

justiceconnect.cjis.gov/communities/community/cuas

PROGRAM QUESTIONS

cuas@fbi.gov

Both the Federal C-UAS Coordination Portal and the NCUTC Training Portal are operating in interim status - a streamlined, interactive portal is in development to make coordination even easier.

JOINTLY ISSUED BY

The **U.S. Departments of Justice and Homeland Security**, under the SAFER SKIES Act.

PORTAL OPERATED BY

The **Federal Bureau of Investigation**, Critical Incident Response Group.

This Q&A is a plain-language summary; the interim final rule (**6 & 28 CFR Part 124**) is the controlling text. The United States does not endorse, recommend, or certify any vendor, system, or manufacturer.