-9F; 4410-02

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 124

RIN 1601-AB25

DEPARTMENT OF JUSTICE

28 CFR Part 124

[Docket No. FBI-2026-0001]

RIN 1110-AA39

Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies

AGENCIES: Department of Homeland Security; Department of Justice.

ACTION: Interim final rule; request for comment.

SUMMARY: In this interim final rule ("IFR"), the Department of Justice ("DOJ") and the Department of Homeland Security ("DHS") (collectively, "the Departments") codify the framework for implementing the SAFER SKIES Act, which authorizes State, local, Tribal, and territorial law enforcement or correctional ("SLTT") agencies to conduct counter-unmanned aircraft system ("C-UAS") operations. This framework governs training and certification (including a two-tiered structure for detection and warning operations and for mitigation operations), authorized technologies, spectrum coordination, airspace approval, real-time air traffic control notification, mitigation reporting, privacy protections, and compliance requirements for SLTT agencies in relation to the exercise of C-UAS authority.

DATES: *Effective date:* This interim final rule is effective July 1, 2026.

Comment due date: Comments must be received on or before [**INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**].

The electronic Federal Docket Management System ("FDMS") at

https://www.regulations.gov will accept electronic comments until 11:59 p.m. Eastern Time on that date.

ADDRESSES: You may submit comments on the entirety of this IFR, identified by FDMS Docket No. FBI-2026-0001, through the Federal eRulemaking Portal: https://www.regulations.gov. Follow the website instructions for submitting comments. The Departments are not accepting mailed, couriered, or hand-delivered comments at this time. If you cannot submit your comment by using https://www.regulations.gov, please use the contact information in the FOR FURTHER INFORMATION CONTACT section for alternate instructions.

FOR FURTHER INFORMATION CONTACT:

For DHS: Steven A. Willoughby, Acting Executive Director, Program Executive Office for Drones and Counter-Unmanned Aircraft Systems, U.S. Department of Homeland Security, drones@dhs.gov.

For DOJ: Micheal J. Torphy, Assistant Section Chief, Unmanned Aviation Section, Critical Incident Response Group, Federal Bureau of Investigation, ncutc@fbi.gov.

SUPPLEMENTARY INFORMATION:

I. Public Participation

The Departments invite all interested parties to participate in this rulemaking by submitting written data, views, comments, and arguments on all aspects of this rule. The Departments also invite comments that relate to the economic, environmental, or federalism effects that might result from this rule. Comments must be submitted in English, or an English translation must be provided. Comments that will provide the most assistance to the Departments in implementing these changes will reference a specific portion of the rule, explain the reason for any recommended change, and include data, information, or authority that supports such recommended change. Comments

submitted in a manner other than the one listed above, including e-mails or letters sent to Department officials, will not be considered comments on the rule and may not receive a response from the Departments.

Instructions: If you submit a comment, you must include the agency name (Federal Bureau of Investigation) and the FDMS Docket No. FBI-2026-0001 for this rulemaking. All submissions will be posted, without change, to the Federal eRulemaking Portal at https://www.regulations.gov, and will include any personal information you provide. Therefore, submitting this information makes it public. You may wish to consider limiting the amount of personal information that you provide in any voluntary public comment submission you make to the Departments. The Departments may withhold information provided in comments from public viewing that they determine may impact the privacy of an individual or is offensive. For additional information, please read the Privacy and Security Notice available at https://www.regulations.gov.

Docket: For access to the docket and to read background documents or comments received, go to https://www.regulations.gov, referencing FDMS Docket No. FBI-2026-0001. You may also sign up for email alerts on the online docket to be notified when comments are posted or a final rule is published.

II. Executive Summary

In 2018, Congress recognized the growing threat of drones (unmanned aircraft) and unmanned aircraft systems ("UAS") to public safety and national security, including their use by extremists, terrorists, and criminals. *See* S. Rep. No. 115-332, at 2–3 (2018). Congress recognized that "[t]errorist organizations promote the use of UAS to conduct attacks in the U.S. and surveillance on potential targets." *Id.* at 2. In one notable instance, "Al-Qaeda in the Arabian Peninsula used their Inspire magazine in May 2016 to encourage individuals to use UAS to collect information about potential assassination attempts and killings." *Id.* And "[i]n September 2011, Rezwan Ferdaus, a U.S. citizen,

was arrested for planning to attach explosives to a UAS and attack the Pentagon and U.S. Capitol." *Id.* "Another potentially dangerous incident occurred in 2017 when a UAS flew over the San Francisco 49ers and Oakland Raiders National Football League stadiums dropping leaflets and causing panic." *Id.*

Congress also recognized that Federal law hampered the ability of law enforcement to respond to these threats. Congress noted that Federal law enforcement agencies were "prohibited from taking actions against UAS due to decades-old statutes," such as "the Wiretap Act of 1968 and the Computer Fraud and Abuse Act of 1986," that "were enacted long before UAS were widely available." *Id.* Such laws make "it illegal to intercept any wire, oral, or electronic communication, or to access a computer without authorization, respectively, making it imposing to use the electronic transmission to track down the operator of the drone." *Id.* Congress also noted that "DHS and DOJ are prevented from taking action against a rogue UAS due to the FAA Modernization and Reform Act of 2012 that define[d] UAS as aircraft" and as a result subjected UAS to "aircraft piracy laws [that] ma[de] it illegal to seize or exercise control of an aircraft." *Id*. (citing 49 U.S.C. 331).

In order to remedy this problem, as part of the FAA Reauthorization Act of 2018, Congress passed the Preventing Emerging Threats Act of 2018, which authorized the Secretary of Homeland Security and the Attorney General to designate certain facilities or assets as "covered facilities or assets" and take certain measures necessary to mitigate a credible threat that an unmanned aircraft or UAS poses to the safety or security of a covered facility or asset, notwithstanding certain provisions of Federal criminal law, including prohibitions against aircraft piracy, destruction of an aircraft, computer fraud, interference with the operation of a satellite, the Wiretap Act, and the prohibition on pen register and trap and trace device use. Pub. L. No. 115–254, sec. 1602(a), 132 Stat. 3186, 3522–29 (codified at 6 U.S.C. 124n). Generally, the authorized protective measures

included, and still include, detection, disruption, seizure, confiscation, and destruction of UAS using reasonable force (if necessary). 6 U.S.C. 124n(b)(1)(F). However, the Act did not authorize SLTT agencies to take such measures.

In testimony before the Senate Judiciary Committee in July 2025, DOJ recommended that all SLTT agencies be authorized to address the continuing threat of UAS (for example, smuggling contraband into prisons, or threatening public safety at sporting events or other outdoor gatherings), again notwithstanding these same Federal criminal laws. Dep't of Justice, *Securing the Skies: Law Enforcement, Drones, and Public Safety: Hearing Before the S. Comm. on the Judiciary*, 119th Cong. 8–9 (2025), https://www.judiciary.senate.gov/imo/media/doc/94f53245-d172-92ba-152b-06bc9ee00a50/2025-07-22%20-%20Testimony%20-%20Torphy%20&%20Hardee1.pdf [https://perma.cc/F3J7-NWDG] (statement of Christopher Hardee, Chief, Office of Law & Policy, Nat'l Sec. Div., DOJ, and Micheal Torphy, Unit Chief, Critical Incident Response Grp., FBI). DOJ suggested that State and local law enforcement be authorized to use pre-approved, detection-only equipment, and that certain State and local law enforcement be trained to use all C-UAS capabilities (including mitigation measures such as exercising control of a UAS or destroying a UAS). *Id*.

In recognition of this continued challenge, Congress passed the SAFER SKIES Act, signed into law by the President on December 18, 2025. National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119–60, div. H, tit. LXXXVI, §§ 8601–07, 139 Stat. 718, 1938–45 (2025) ("SAFER SKIES Act" or "the Act") (codified in large part in 6 U.S.C. 124n). The SAFER SKIES Act authorizes SLTT agencies to take certain measures to detect and mitigate credible threats that unmanned aircraft and UAS pose to the safety or security of people, facilities, and assets, a venue or set of venues used for large-scale public gatherings or events, critical infrastructure, or

correctional facilities,[1] notwithstanding the same provisions of Federal criminal law (prohibitions against aircraft piracy, destruction of an aircraft, computer fraud, interference with the operation of a satellite, the Wiretap Act, and the prohibition on pen register and trap and trace device use), and notwithstanding the laws of any particular State, local, Tribal, or territorial jurisdiction, but only under certain conditions. 6 U.S.C. 124n(a)(2).

Specifically, the SAFER SKIES Act authorizes SLTT agencies to take the mitigation measures identified in 6 U.S.C. 124n(b)(1)(C), (D), and (F) if they: (1) are trained and certified by the Attorney General, or the Attorney General's designee, through a national schoolhouse, 6 U.S.C. 124n(d)(2)(A)(i); (2) use technologies on authorized technologies and systems lists maintained jointly by DOJ, DHS, the Department of Defense,[2] the Department of Transportation, the Federal Communications Commission ("FCC"), and the National Telecommunications and Information Administration ("NTIA"), 6 U.S.C. 124n(d)(2)(A)(iii); (3) comply with specific compliance, coordination, and audit requirements, 6 U.S.C. 124n(d)(2)(B) (Oversight), (e) (Privacy protection); and (4) report mitigation actions to DOJ and DHS, 6 U.S.C. 124n(d)(2)(C). At the same time, the SAFER SKIES Act authorized SLTT agencies to take measures identified under 6 U.S.C. 124n(b)(1)(A), (B), and (E)—that is to detect, monitor, identify, track, and confiscate UAS, as well as warn the operator of a UAS, including by passive or active, direct or indirect physical, electronic, radio, or electromagnetic means, and through the use of a remote identification broadcast, or by other means—subject to satisfying training and certification procedures; but the training

[1] Note that the SAFER SKIES Act also amended the definition of "personnel" under section 124n, thus facilitating the use of detailed and deputized personnel. 6 U.S.C. 124n(l)(6)(A). The FBI is currently using SLTT agencies as federally deputized task force officers in operations to mitigate UAS. This IFR does not address federally deputized or detailed SLTT agency personnel. Note as well that the Act provided two new bases for DOJ and DHS protective measures: that is, to enforce the law, and to protect the public. 6 U.S.C. 124n(a)(1). However, the Act did not make these two new bases available to SLTT agencies.

[2] The Department of Defense is also known as the Department of War. E.O. 14347, 90 FR 43893 (Sept. 5, 2025). This rule refers to the "Department of Defense" to be consistent with the SAFER SKIES Act.

and certification procedures required to take these specific protective measures need not occur at a national schoolhouse. 6 U.S.C. 124n(a)(2) (allowing SLTT agencies to take measures in subsection (b)(1), but only subject to subsection (d)(2)); *see also* 6 U.S.C. 124n(d)(2)(A)(ii) (providing that SLTT agencies must satisfy the training and certification procedures before taking any action in all of subsection (b)(1)).

Finally, the Act directs the Secretary of Homeland Security and the Attorney General, in coordination with the Secretary of Defense, the Secretary of Transportation, and the Administrator of the Federal Aviation Administration ("FAA"), to develop and publish regulations governing C-UAS authority—that is, the authority to conduct protective measures to detect, identify, monitor, track, and, if necessary, mitigate the threat of UAS—for SLTT agencies under section 124n. This IFR implements this statutory authority, to include compliance requirements and procedures for coordination.

III. Background and Purpose

A. Background and Legal Authority

As noted in Section II of this preamble above, the Preventing Emerging Threats Act of 2018 permits the Attorney General and the Secretary of Homeland Security to authorize certain personnel to take certain protective measures (generally, detection, disruption, seizure, confiscation, and disablement, damage, or destruction using reasonable force) necessary to mitigate a credible threat that an unmanned aircraft or UAS poses to the safety or security of a covered facility or asset, notwithstanding certain provisions of Federal criminal law. *See* 6 U.S.C. 124n(b)(1). Specifically, the Attorney General and the Secretary of Homeland Security are authorized to take such measures notwithstanding Federal criminal prohibitions in 49 U.S.C. 46502 (aircraft piracy), 18 U.S.C. 32 (destruction of aircraft), 18 U.S.C. 1030 (computer fraud), and 18 U.S.C. 1367 (interference with the operation of a satellite), as well as chapters 119 (interception of communications) and 206 (pen registers and trap and trace devices) of Title 18. 6 U.S.C.

124n(a)(1). Generally, a "covered facility or asset" must be identified as high risk and a potential target for unlawful unmanned aircraft activity by the Secretary or the Attorney General, in coordination with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment. 6 U.S.C. 124n(l)(3)(A).

The SAFER SKIES Act amended section 124n in several ways, notably by authorizing SLTT agencies to take certain protective measures to mitigate a credible threat that unmanned aircraft and UAS pose to the safety or security of people, facilities, and assets, a venue or set of venues used for large-scale public gatherings or events, critical infrastructure, or correctional facilities, notwithstanding certain provisions of Federal criminal law, and notwithstanding the laws of any particular State, local, Tribal, or territorial ("SLTT") jurisdiction, 6 U.S.C. 124n(a)(2), but subject to additional requirements.

Notwithstanding the foregoing statutory changes, the SAFER SKIES Act did not amend or waive the applicability of other Federal statutory provisions that may govern or proscribe SLTT agencies' otherwise authorized activity, including those in the Communications Act or other regulations governing access to spectrum. *See, e.g.*, 47 U.S.C. 301 (licensing and authorization), 47 U.S.C. 302 (interfering devices), 47 U.S.C. 333 (jamming), 47 U.S.C. 605 (unauthorized transmissions). As a result, this regulation requires SLTT agencies to obtain approvals from the FCC before deploying any C-UAS system (whether detection only or mitigation) that involves the emission of radio waves.

1. Detecting, identifying, monitoring, tracking, and warning

First, the Act authorizes SLTT agencies to "detect, identify, monitor, and track" UAS or unmanned aircraft, without prior consent, including by means of interception of or other access to a wire communication, an oral communication, or an electronic communication used to control the UAS or unmanned aircraft. 6 U.S.C. 124n(b)(1)(A). The Act also authorizes SLTT agencies to warn the operator of a UAS, including by

"passive or active, and direct or indirect physical, electronic, radio, electromagnetic means, and through the use of remote identification broadcast or other means." 6 U.S.C. 124n(b)(1)(B). The Act also allows SLTT agencies to seize or otherwise confiscate a UAS or unmanned aircraft. 6 U.S.C. 124n(b)(1)(E). This rule covers confiscation under section 124n(b)(1)(E) through the Detection and Warning Certification process alongside the detection and warning activities in section 124n(b)(1)(A) and (B) because, like those activities, confiscation does not involve the use of a mitigation technology. The Act authorizes SLTT agencies to take measures under section 124n(b)(1)(A), (B), and (E) subject to the training and certification requirement described in section 124n(d)(2)(A)(ii), which applies to all actions in section 124n(b)(1), only if they:

(1) use "systems or technologies that are included on a list of authorized technologies maintained jointly by the Department of Justice, the Department of Homeland Security, the Department of Defense, the Department of Transportation, the Federal Communications Commission, and the National Telecommunications and Information Administration," 6 U.S.C. 124n(d)(2)(A)(iii);

(2) comply with specific privacy protections identified in section 124n(e), which include compliance with the First and Fourth Amendments to the Constitution of the United States, data retention limitations, and limits on collecting certain data; and

(3) comply with Federal oversight, audits, coordination, and compliance requirements, including by the Secretary of Homeland Security and Attorney General, in coordination with the Secretary of Transportation and the Administrator of the FAA, over SLTT agencies' compliance with the privacy protections identified in section 124n(e) and the requirements outlined in this regulation consistent with sections 8602, 8605, and 8606 of the SAFER SKIES

Act.

2. Disrupting, disabling, interfering, seizing control, or using reasonable force under the totality of the circumstances to disable, damage, or destroy

Regarding the protective measures identified in section 124n(b)(1)(C), (D), and (F)— that is, mitigation measures generally involving disruption, seizure and control, and destruction using reasonable force—SLTT agencies are only authorized to use these protective measures under a more restrictive set of conditions. Specifically, in order to use the protective measures identified in section 124n(b)(1)(C), (D), and (F), SLTT agencies must:

(1) be trained and certified by the Attorney General, or the Attorney General's designee, in coordination with the Secretary of Homeland Security, through a national schoolhouse, 6 U.S.C. 124n(d)(2)(A)(i);

(2) use technologies that are included on a list of authorized technologies and systems maintained jointly by DOJ, DHS, the Department of Defense, the Department of Transportation, the FCC, and the NTIA, 6 U.S.C. 124n(d)(2)(A)(iii);

(3) comply with specific privacy protections identified in section 124n(e), which include compliance with the First and Fourth Amendments of the Constitution of the United States, data retention limitations, and limits on collecting certain data, and with Federal oversight, audits, coordination, and compliance requirements, including by the Secretary of Homeland Security and the Attorney General, in coordination with the Secretary of Transportation and the Administrator of the FAA, as concerning compliance with the privacy protections identified in section 124n(e), 6 U.S.C. 124n(d)(2)(B); and

(4) notify DHS and DOJ within 48 hours of any mitigation action taken, 6 U.S.C. 124n(d)(2)(C).

The Act also provides for suspension of C-UAS authority and civil fines for SLTT agencies, as well as their personnel, authorized to take C-UAS protective measures who knowingly engage in such action without Federal coordination as required by the Act. Pub. L. No. 119–60, sec. 8605(f), 139 Stat. at 1944 (codified at 6 U.S.C. 124n-1(f)) ("Penalties for Unauthorized Counter-UAS Actions"); *id.* sec. 8605(g) (codified at 6 U.S.C. 124n-1(g)) ("Civil Enforcement").

The Act also requires the "Attorney General, in coordination with the Secretary of Homeland Security, the Secretary of Defense, and the Secretary of Transportation," to develop training and certification procedures that SLTT law enforcement and correctional officers must satisfy before engaging in those protective measures requiring training and certification. 6 U.S.C. 124n(d)(2)(A)(ii) (training and certification procedures).

Finally, the Act directs the "Secretary of Homeland Security and the Attorney General, in coordination with the Secretary of Defense and Secretary of Transportation," and the Administrator of the FAA to publish regulations governing C-UAS authority for SLTT agencies under section 124n. *See* Pub. L. No. 119–60, sec. 8606, 139 Stat. 1944–45. This IFR implements the statutory directive to promulgate regulations, to include additional compliance requirements and procedures based on such coordination.

B. Discussion of Interim Rule

This IFR identifies the requirements and procedures for SLTT agencies to become authorized to take C-UAS measures under section 124n. Specifically, for the full range of C-UAS protective measures identified under section 124n(b)(1)(A) and (B) (involving detecting, identifying, monitoring, and tracking UAS, and warning the operator), the mitigation measures under section 124n(b)(1)(C), (D), and (F), and (E) (involving seizure and confiscation of UAS or unmanned aircraft), the IFR identifies how SLTT agencies must (1) use only systems or technologies that are included on a list of authorized technologies, and how to obtain the list; and (2) comply with specific privacy protections

identified in section 124n(e) and how they must comply with Federal oversight, audits, coordination, and compliance requirements by the Secretary of Homeland Security and Attorney General as outlined in this rule, consistent with sections 8602, 8605, and 8606 of the SAFER SKIES Act.

Concerning C-UAS protective measures identified under section 124n(b)(1)(C), (D), and (F) (generally involving mitigation—that is, disrupting, disabling, interfering with, seizing control of, or using reasonable force, if necessary, to disable, damage or destroy a UAS), the IFR sets forth the requirements for the use of such measures. Specifically, the IFR explains how SLTT agencies: (1) receive training and certification through the Federal Bureau of Investigation's ("FBI") national schoolhouse; (2) obtain the list of authorized technologies they may use; (3) comply with the specific privacy protections identified in section 124n(e); and (4) comply with Federal oversight, audits, and compliance requirements established by the Secretary of Homeland Security and the Attorney General, in coordination with the Administrator of the FAA, as outlined in this regulation and as provided in 6 U.S.C. 124n(d)(2)(B), with suspension of authority under sections 8605 and 8606(f) of the SAFER SKIES Act available to the Attorney General or the Secretary.

The rule is organized as follows in parts 124 of titles 6 and 28 of the Code of Federal Regulations: purpose and scope (§ 124.1); definitions (§ 124.2); scope of authority and mitigation standards (§ 124.3); authorized personnel, contractors, and mutual aid (§ 124.4); training and certification (§ 124.5); the agency implementation policy (§ 124.6); authorized technologies (§ 124.7); the C-UAS Operations Plan (§ 124.8); advance coordination, notification, and authorization (§ 124.9); interagency and lead-agency coordination (§ 124.10); real-time air traffic control notification (§ 124.11); detection and warning operations (§ 124.12); post-operation reporting (§ 124.13); privacy and civil liberties (§ 124.14); protection of sensitive operational

information (§ 124.15); compliance and enforcement (§ 124.16); confiscation and forfeiture (§ 124.17); activities for evaluation, testing, training, and pre-operational validation (§ 124.18); task force arrangements and Federal support (§ 124.19); rules of construction (§ 124.20); termination (§ 124.21); and severability (§ 124.22).

This rule establishes the framework governing SLTT agency C-UAS operations under 6 U.S.C. 124n(a)(2). This rule provides requirements for training and certification of SLTT agency personnel, the agency implementation policy, the C-UAS Operations Plan, advance coordination, interagency and lead-agency coordination, notification and reporting requirements, and privacy and data handling protections. The Secretary of Transportation and the Administrator of the FAA have coordinated in the development of this rule as required by 6 U.S.C. 124n(d)(3), and the rule was developed in coordination with the Secretary of Defense as required by 6 U.S.C. 124n(d)(2)(A)(ii) and section 8606(a)(1) of the SAFER SKIES Act.

Consistent with the SAFER SKIES Act, the rule does not change the applicability of the Communications Act, *see* 47 U.S.C. 301 *et seq.*, or implementing rules administered by the FCC that relate to spectrum licensing, equipment authorization, and harmful interference to authorized services, among other things. SLTT agencies thus remain subject to applicable provisions that may govern or proscribe activities otherwise authorized by this rule.

The following discussion describes each provision of the regulatory text added by this rule to new parts 124 in both titles 6 and 28 of the Code of Federal Regulations. The two parts are identical.

Section 124.1—Purpose and scope. This section states the purpose and scope of the new part 124 and its relationship to other laws, including the statutory provisions displaced by the notwithstanding clause of 6 U.S.C. 124n(a)(2), provides that this part is the comprehensive framework for SLTT agency C-UAS operations, and identifies for

SLTT agencies that conduct only detection and warning operations the provisions of the part principally applicable to them. As used in this rule, the term "notwithstanding clause of 6 U.S.C. 124n(a)(2)" means the provision that permits a certified agency to take the actions described in 6 U.S.C. 124n(b)(1) without violating the Federal criminal laws the clause displaces—49 U.S.C. 46502 (aircraft piracy), 18 U.S.C. 32 (destruction of aircraft), 18 U.S.C. 1030 (computer fraud), 18 U.S.C. 1367 (interference with the operation of a satellite), and chapters 119 (interception of communications) and 206 (pen registers and trap and trace devices) of title 18—as well as "the laws of any particular State, local, Tribal, or territorial jurisdiction." In plain terms, protective measures described in 124n, such as intercepting the radio link that controls a drone or taking control of a drone away from its operator, are lawful—notwithstanding the laws mentioned above—when a certified SLTT agency performs them in compliance with the Act and the regulations this IFR adopts.

For an agency that conducts only detection and warning operations, the provisions principally applicable are those identified in § 124.1(b): the Detection and Warning Certification requirement of § 124.5(c), the detection and warning policy provisions of § 124.6(g), the authorized technology requirements of § 124.7, the C-UAS Operations Plan requirement of § 124.8, the operational conditions of § 124.12, and the privacy and data handling requirements of § 124.14. The authority to regulate detection and monitoring activity conducted in reliance on the Act rests on the statute itself: the opening text of 6 U.S.C. 124n(a)(2) conditions any action on completion of the training detailed in subsection (d)(2); 6 U.S.C. 124n(d)(2)(A)(ii) requires training and certification before personnel take any action described in subsection (b)(1), including detection; 6 U.S.C. 124n(d)(2)(A)(iii) limits the technologies used for any such action to listed technologies; 6 U.S.C. 124n(e) imposes privacy requirements; and section 8606(a)(1) of the SAFER SKIES Act directs publication of regulations governing the

authority.

This section also clarifies that the Departments maintain parallel regulations for ease of use, and that each Department administers and interprets its own regulations with respect to its programs and authorities.

Section 124.2—Definitions. This section defines the terms used in the part, including the two-list technology framework (the Authorized Technologies List and the Authorized Systems List), the two certification tiers (Detection and Warning Certification and Mitigation Certification), the data categories the part regulates (control communications, raw sensor data, and pattern data), the credible threat standard, the Agency Approving Official, and the designated Federal C-UAS coordination portal.

Two definitions reflect policy choices that warrant explanation. First, the Agency Approving Official must hold a rank not below a Senior Executive or Senior Official, or its equivalent. The Departments set the threshold at this level because approving a mitigation operation, which may involve the use of force against an aircraft, is a command decision that in most agencies rests above the line-supervisor level. The same senior official also approves the agency's detection and warning operations, so that authorization of all C-UAS operations under this part rests with one accountable command official. The reference is to the agency's senior command or executive ranks, not to any particular title, and where no equivalent rank exists the agency head or the agency head's designee may serve. Second, the credible threat standard governs agency action on a credible threat to the protected interests the statute enumerates, but the statute does not define the term. The rule's definition adapts the objective, totality-of-the-circumstances standard applied in Federal C-UAS operations under 6 U.S.C. 124n(a)(1) since 2018, reflected in the Attorney General's April 2020 Guidance[3] and the DOJ

[3] Memorandum from the Attorney General, *Guidance Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems* (Apr. 13, 2020), https://www.justice.gov/archives/ag/page/file/1268401/dl?inline.

objective standards for C-UAS operations,[4] and is framed on the reasonable-officer model familiar from use-of-force doctrine, with enumerated indicators drawn from Federal operational experience.

Section 124.3—Scope of authority and mitigation standards. This section states the scope of authority, the credible threat determination, proportionality in the reasonableness of the use of force, the protective purpose limitation, the mitigation operator execution requirement, the independent professional judgment of the certified operator under the totality of the circumstances, and the airspace awareness function.

The credible threat determination requirement implements the statutory condition of 6 U.S.C. 124n(a)(2) and requires that the determination be made and documented before mitigation. The proportionality standard requires that a mitigation action taken be reasonable in relation to the threat presented; it reflects the statute's authorization of actions that are necessary to mitigate the threat and the reasonable force limitation of 6 U.S.C. 124n(b)(1)(F). The protective purpose limitation confines the exercise of the authority to protective ends and forecloses use of the authority as a general investigative tool, consistent with the structure of 6 U.S.C. 124n(e). The mitigation operator execution requirement provides that only personnel holding Mitigation Certification may execute mitigation actions, implementing 6 U.S.C. 124n(d)(2)(A)(i). The independent professional judgment provision preserves the certified operator's discretion to decline an action the operator assesses to be unsafe, a safeguard the Departments adopted from Federal C-UAS practice because the operator of the system has the best real-time awareness of airspace and spectrum conditions. The airspace awareness function requires the operating agency to maintain awareness of manned aircraft in the vicinity of an operation, implementing the aviation safety coordination obligations of 6 U.S.C. 124n(b)(4) and (d)(3).

---

[4] *See id.* at 5.

Section 124.4—Authorized personnel, contractors, and mutual aid. This section limits the exercise of authority to officers and employees of the SLTT agency, prohibits contractor operation of systems requiring the authority of the Act, establishes the conditions for mutual aid, and contains an anti-circumvention provision.

The limitation of operational authority to officers and employees implements the Act rather than a discretionary policy choice. Congress defined the personnel who may exercise SLTT agency authority as the officers and employees of the SLTT agency, 6 U.S.C. 124n(l)(6)(B), in contrast to the broader personnel definition applicable to Federal operations under 6 U.S.C. 124n(l)(6)(A), which extends to certain contractors, detailed personnel, and deputized personnel. The prohibition on contractor operation of mitigation systems, including arrangements described as turnkey or managed C-UAS services, follows from that statutory structure. The rule preserves substantial roles for the private sector: contractors and vendors may design, manufacture, sell, install, and maintain C-UAS systems; provide technical support and system-level operator training; receive operational data for diagnostics under the conditions of § 124.14(j); and provide detection services using systems that do not require the authority of the Act or the relief it provides from certain laws.

Section 124.4 also permits accredited SLTT agencies to provide C-UAS support to non-accredited SLTT agencies through mutual aid or other written arrangement. This approach reflects the Departments' judgment that public safety is better served by strong regional, county, statewide, and multi-jurisdictional C-UAS programs than by requiring every small or resource-limited agency to establish a separate, rarely used capability. The rule therefore allows a non-accredited agency to request and receive C-UAS support, while ensuring that the accredited agency remains the C-UAS operating agency and that all actions requiring 6 U.S.C. 124n authority are performed by properly certified personnel under the requirements of this part. The Departments invite comment on these

provisions, including the conditions governing mutual aid.

Section 124.5—Training and certification. This section establishes the training and certification structure required by 6 U.S.C. 124n(d)(2)(A). It implements the statute's two distinct requirements. The national-schoolhouse sole-certifying-authority requirement of 6 U.S.C. 124n(d)(2)(A)(i) applies to mitigation under 6 U.S.C. 124n(b)(1)(C), (D), and (F), and the FBI's National Counter-UAS Training Center ("NCUTC") is designated as that schoolhouse. The Act separately requires training and certification before personnel take any of the actions it authorizes, including detection. The opening text of 6 U.S.C. 124n(a)(2) permits an agency to act only after completing the training detailed in subsection (d)(2), and 6 U.S.C. 124n(d)(2)(A)(ii) requires the Attorney General to develop training and certification procedures that officers must satisfy before taking any action described in subsection (b)(1). Detection and warning under 6 U.S.C. 124n(b)(1)(A), (B), and (E) are among the actions described in subsection (b)(1), so the training and certification requirement reaches them as well as mitigation. The Departments have accordingly provided for a Detection and Warning Certification requirement for detection and warning operations conducted with systems that require the authority of the Act or the relief it provides from certain laws, but the requirement that training and certification take place "through a national schoolhouse" in clause (i) does not extend to those actions. Thus, the NCUTC delivers the detection and warning curriculum through an online portal that issues the certification automatically on completion, rather than at an in-person resident instruction at the national schoolhouse. Detection activities conducted with systems that do not require the authority of the Act or the relief it provides from certain laws are outside this requirement. Examples of such activities include electro-optical and infrared cameras, acoustic sensors, and radar operated under FCC authorization. Operating those systems does not implicate the prohibitions the Act displaces, because they intercept no communications, so the Act's

training requirement does not attach.

Online delivery for the detection tier does not create the public safety risks that warrant resident instruction for mitigation. Detection and warning do not involve disrupting, taking control of, or otherwise affecting an aircraft in flight. Although some detection systems (such as radar) transmit radio frequency energy to sense an aircraft, such systems cannot interfere with an aircraft's operation, and the associated risks are legal and privacy compliance risks, which are knowledge-based and are effectively taught and tested through structured online instruction with a required detection assessment. Resident instruction for the detection tier would impose travel and backfill costs on thousands of agencies without a corresponding safety benefit and would consume schoolhouse capacity needed for mitigation training.

This section also establishes the correctional-specific curriculum and the decertification, suspension, administrative-review, and reinstatement process. Two choices in this section warrant further explanation.

First, training and certification for mitigation occur through a national schoolhouse because Congress required it: 6 U.S.C. 124n(d)(2)(A)(i) conditions the exercise of the mitigation authorities—that is, authorities at 6 U.S.C. 124n(b)(1)(C), (D), and (F)—on certification through a national schoolhouse serving as the sole certifying authority. *See* 6 U.S.C. 124n(d)(2)(A)(i).

Second, the section provides for suspension of certifications and agency accreditations. Suspension is the measure section 8605(f)(2) of the SAFER SKIES Act provides, and the suspension and administrative review process is described in the discussion of the administrative review provisions below. Because the rule provides for suspension of certifications and agency accreditations, the Departments describe the process and its basis here. A suspension decision is communicated in writing and specifies the basis for the action and any available remedial steps. In exigent

circumstances that pose a risk to aviation safety, public safety, or national security, the Director or the Director's designee may immediately suspend a certification or accreditation pending administrative review. An individual or agency that receives a suspension notice may request administrative review within 30 calendar days. The Attorney General, acting through the Director, designates a reviewing official from DOJ who did not participate in or supervise the initial decision; that official considers the written submissions of both parties, may hold an informal hearing, and issues a written determination within 60 calendar days stating the factual findings and the basis for the determination. The reviewing official may affirm, modify, condition, or reverse the action, and the determination is final agency action for purposes of this part. The rule contains no separate revocation action. A suspension that is affirmed and not cured remains in effect until reinstatement, and reinstatement of a Mitigation Certification requires completion of the full course. This process affords affected individuals and agencies notice and an opportunity to respond before a neutral reviewing official, while preserving the ability to act immediately when continued exercise of C-UAS authority would pose a safety or security risk.

The Departments are considering whether certifications should expire after a given period of time—such as 36 or 48 months—conditioned upon additional training requirements to ensure continuing proficiency and welcome comment on whether certifications should expire, the length of their validity period, and the requirements for renewal.

Section 124.6—Agency implementation policy. This section establishes the agency implementation policy, the legal counsel review, the portal attestation, and the detection and warning policy for SLTT agencies conducting only detection and warning operations. An agency's implementation policy is not subject to pre-approval by the NCUTC; the agency self-certifies through a portal attestation, and the NCUTC retains

audit and suspension authority. The implementation policy is the agency-level governing document for the agency's C-UAS program; it must address command responsibility, integration with the agency's use-of-force policy, operator rostering and certification verification, equipment control and maintenance, the privacy procedures required by § 124.14, and recordkeeping. The legal counsel review requires the agency's counsel to review the policy for compliance with this part and with applicable SLTT law before adoption. The portal attestation is the agency's certification, submitted through the Federal C-UAS coordination portal, that the policy has been adopted and reviewed. The detection and warning policy is an abbreviated policy, based on a model the Departments will publish, for agencies that conduct only detection and warning operations. The Departments chose self-certification with audit, rather than Federal pre-approval of each agency policy, for two reasons. Pre-approval of policies from the thousands of agencies expected to participate would create a Federal bottleneck, which would be inconsistent with the independent authority Congress conferred on certified SLTT agencies, and would add months of delay without a corresponding compliance benefit. Audit with suspension exposure, by contrast, preserves accountability: an agency that attests falsely or maintains a deficient policy is subject to the compliance audit program of § 124.16 and to suspension under § 124.5.

The rule neither directly requires an SLTT agency to notify its State government of the agency's adoption of C-UAS capability or of individual operations, nor prohibits such notification, and nothing in the rule conditions the exercise of authority under 6 U.S.C. 124n(a)(2) on State-level notification, endorsement, or approval; Congress conferred that authority directly on SLTT agencies. The Departments recognize, however, that Governors, State homeland security advisors, and State law enforcement agencies have a legitimate interest in awareness of C-UAS capability within their States, including for purposes of intrastate and interstate deconfliction, mutual aid planning, and

security planning for major events, and that the visibility provided through existing channels, such as the State Administrative Agency structure of DHS's C-UAS grant program, does not extend to agencies that participate without grant support through that program. The Departments have therefore included one reference to State notification requirements under § 124.9(b), if otherwise required by State law or policy, and invite comment on whether the rule should provide an additional State-level awareness mechanism and, if so, on its appropriate form, including whether the Federal Government should make available to a State-designated point of contact the roster of attested and accredited agencies within the State, or whether the agency implementation policy should address notification to a State-designated point of contact upon adoption of C-UAS capability, and on how any such mechanism should be structured so that notification does not operate as a condition on, or approval requirement for, the exercise of statutory authority.

Section 124.7—Authorized technologies. This section establishes the two-list technology authorization framework and limits SLTT agency C-UAS operations to listed technology categories and, where the Authorized Systems List is populated, listed systems. It clarifies that the list requirement applies only to technologies the operation of which requires the legal relief provided by the notwithstanding clause of 6 U.S.C. 124n(a)(2). Under the two-list framework, the Authorized Technologies List identifies the categories of technology authorized for SLTT agency use, and the Authorized Systems List identifies specific systems within those categories. The Authorized Systems List is populated for a category when the interagency process has assessed and listed specific systems in that category. Until the Authorized Systems List is populated for a category, an agency is limited to the listed technology categories of the Authorized Technologies List, which is the limit 6 U.S.C. 124n(d)(2)(A)(iii) itself imposes; once the Authorized Systems List is populated for a category, the agency must use a listed system.

SLTT agencies are therefore never free of the list requirement: category-level limits apply at all times, and system-level limits attach as listings are completed.

The Departments adopted the two-list structure so that category-level policy is set through a deliberate interagency process while system-level additions can keep pace with a rapidly developing market. It clarifies that the list requirement applies only to technologies the operation of which requires the legal relief provided by the notwithstanding clause of 6 U.S.C. 124n(a)(2); technologies an agency may use lawfully without that relief, such as cameras, radar, and acoustic sensors, are not subject to the list requirement and remain available on the same basis as before the Act. Such technologies remain subject to existing laws and regulations, including FCC and equipment authorization requirements, FAA requirements, and SLTT law; the Act neither expands nor restricts their availability.

This section also requires an agency to cease use of a system or technology category upon an emergency suspension issued through the interagency process. The detailed mechanics of evaluating, listing, and maintaining technologies are established through the interagency process required by 6 U.S.C. 124n(d)(2)(A)(iii) and section 8606(a)(4) of the SAFER SKIES Act, in which agencies other than the Departments share responsibility, and are therefore not codified in this part. The Departments expect the initial Authorized Technologies List to include radio frequency ("RF") detection with command-and-control signal interception, RF disruption (broadband and protocol-specific jamming), and RF protocol manipulation (command injection and cyber takeover), and expect the Authorized Systems List to be populated on a phased basis, drawing first on systems with existing Federal operational deployment and interagency coordination history under 10 U.S.C. 130i, 6 U.S.C. 124n, 10 U.S.C. 6227 (or its predecessor, 50 U.S.C. 2661), or 50 U.S.C. 3515a, that have been assessed and authorized for operational use by Federal agencies, and for which the FAA has completed

an assessment of aviation safety risks and for which any necessary aviation safety mitigations the using agency or the FAA would need to implement have been identified as operational constraints. Each RF-emitting system listed on the Authorized Systems List will have completed a system-level spectrum evaluation through the interagency process before listing. Accredited agencies would submit nominations for the Authorized Systems List, and feedback regarding systems on the list, via an internal process announced via the Federal C-UAS coordination portal, which houses the list. The Departments expect to coordinate a 60-day sprint to consider any necessary revisions to the list following publication of this rule.

Section 124.8—C-UAS Operations Plan. This section establishes the C-UAS Operations Plan, signed by the Agency Approving Official and supported by a legal counsel certification, as the instrument authorizing each detection or mitigation operation, or each combined detection and mitigation operation, on behalf of the SLTT agency. The plan must be prepared on a standardized form prescribed by the Attorney General, appropriately coordinated and deconflicted in accordance with §§ 124.9, 124.10, and 124.11, and establishes the 30-day operational window, the 365-day standing window for fixed-site persistent protection, and the renewal process. The Departments chose these requirements based on the experience of the FBI and the DHS C-UAS programs since 2018.

The C-UAS Operations Plan serves three functions: it documents the Agency Approving Official's authorization of mitigation for a defined location and period, it records the legal counsel certification that the planned operation complies with this part and applicable law, and it supplies, in a standardized format, the data elements the Federal coordination process requires. The form is standardized and prescribed by the Attorney General so that every plan carries the same data elements, which permits automated routing through the coordination portal and consistent FAA airspace review;

the Federal C-UAS programs' experience since 2018 is that nonstandard submissions are the principal source of coordination delay. The 30-day operational window keeps the threat assessment, airspace picture, and coordination data underlying a plan current, while the 365-day standing window for fixed-site persistent protection, paired with the recurring reviews required elsewhere in this part, avoids requiring a correctional facility or other fixed site to resubmit an unchanged plan every month. Renewal is by updated submission rather than automatic extension so that each operational period rests on a current authorization.

Section 124.9—Advance coordination, notification, and authorization. This section establishes the advance coordination and notification process, conducted through a single submission to the designated Federal C-UAS coordination portal, operated by the FBI, that routes the relevant data elements to the FBI and DHS for deconfliction, to the FAA for airspace safety coordination, and to the FCC for spectrum coordination. Consistent with 6 U.S.C. 124n, the airspace process is one of coordination, not approval; however, an SLTT agency may only conduct C-UAS operations once the C-UAS Operations Plan is approved under § 124.8. As to the FCC, however, the process is one of coordination and authorization not mere coordination. Because 6 U.S.C. 124n does not displace 47 U.S.C. 301, an SLTT law enforcement or correctional agency must obtain the authorization it needs from the FCC before operating a C-UAS system that emits radio waves (such as certain radar systems), and FCC coordination alone does not suffice. The Departments and the FCC will work to establish standing or categorical authorizations and a vendor equipment authorization pathway that reduce the need for per-operation FCC approval, and the Departments intend to pursue these mechanisms as a priority following publication of this rule. In the interim, an SLTT law enforcement or correctional agency may operate equipment on the Authorized Technologies List under existing FCC authorizations and waivers, and the FCC may issue expedited waivers

under its Part 2 authority, including 47 CFR 2.1204, for equipment already in use and for equipment needed to address a newly identified or evolving threat. The Departments chose these requirements based on the experience of the FBI and the DHS C-UAS programs since 2018.

Advance coordination is the process by which an agency, before commencing a mitigation operation or an operation employing an RF-emitting system, submits the operation's data elements for Federal deconfliction. Notification is the corresponding transmission of those elements to the affected Federal entities. The single-submission design is the central policy choice: the SLTT agency files once, through the Federal C-UAS coordination portal, and the portal routes the relevant elements to the FBI for operational deconfliction, to the FAA for airspace safety coordination, and to the FCC for spectrum coordination. The alternative, separate filings with each Federal entity, would multiply the burden on SLTT agencies, produce inconsistent records, and recreate the sequential processing delays the Federal programs experienced before consolidated coordination mechanisms were adopted.

This section also requires the SLTT agency to submit a comparable advance notification to the State if required by State law or policy. This notification does not operate as a condition on, or approval requirement for, the exercise of statutory authority. The Departments welcome comment on this provision, including whether it is more appropriately included as part of the State implementation policy.

Section 124.10—Interagency and lead-agency coordination. This section establishes interagency and lead-agency coordination, including early coordination and the notice of intent for nationally significant events, tactical coordination under a designated lead C-UAS agency, the requirement that an agency that does not accept tactical coordination cannot conduct C-UAS operations within the area and period covered by the lead-agency designation, coordination of overlapping SLTT operations,

and deconfliction direction when a conflict with a Federal operation cannot otherwise be resolved. Early coordination is advance engagement with the FBI and the designated lead C-UAS agency for an event significant enough to draw multiple C-UAS operators, and the notice of intent is the submission through which an agency states its intent to operate at a nationally significant event so that protective planning can integrate it. Tactical coordination under a designated lead C-UAS SLTT agency places participating SLTT agencies' C-UAS activity under a single, integrated operational picture for the event; the requirement that an agency declining tactical coordination refrain from operating within the covered area and period, and the reasons that requirement is consistent with the independent statutory authority Congress conferred on certified SLTT agencies, are discussed in the following paragraph. Coordination of overlapping SLTT operations addresses adjacent or concurrent operations by multiple agencies outside designated events, and deconfliction direction is the limited mechanism for resolving a conflict between an SLTT agency operation and a Federal operation when coordination fails. Each element responds to the same operational fact, demonstrated repeatedly in Federal C-UAS operations since 2018: simultaneous uncoordinated C-UAS activity is mutually interfering, because RF systems interact and multiple operators may act against the same aircraft.

Paragraph (d) of § 124.10 requires an SLTT agency that does not accept tactical coordination by a designated lead C-UAS agency to refrain from conducting C-UAS operations within the geographic area and time period covered by the designation. The Departments considered whether that requirement is consistent with the independent character of the authority Congress provided to certified SLTT agencies in 6 U.S.C. 124n(a)(2) and have concluded that it is. The Act assigns the Secretary of Homeland Security and Attorney General responsibility for developing regulations and guidance governing SLTT agency C-UAS operations, 6 U.S.C. 124n(d)(1); section 8606(a)(1) of

the Act, and the Attorney General for oversight of the exercise of the authority, 6 U.S.C. 124n(d)(2)(B). The Act also requires coordination with the Administrator of the FAA on matters that might affect aviation safety, civil aviation and aerospace operations, aircraft airworthiness, or the use of airspace. 6 U.S.C. 124n(b)(4) and (d)(3). Uncoordinated simultaneous C-UAS operations, even at a single event, present unacceptable risks: RF mitigation systems can interfere with one another and with protective communications, multiple agencies may attempt conflicting mitigation actions against the same aircraft, and aviation safety coordination assumes a single integrated operational picture. The requirement is limited in three respects: it applies only within the geographic area and time period of a designated lead-agency event; it does not transfer the SLTT agency's statutory authority, including the authority to make credible threat determinations; and it preserves the emergency exception for an imminent risk to human life. Outside designated events, an SLTT agency's C-UAS operations are subject only to the coordination processes of §§ 124.9, 124.10(e). The Departments invite comment on this approach.

Section 124.11—Real-time air traffic control notification. This section establishes the requirement of real-time notification to air traffic control upon activation of any C-UAS system for mitigation action. The requirement protects aviation safety. Activation of an RF-emitting mitigation system can affect aircraft operating near the protected area, by interfering with their communications systems, so real-time notification allows the FAA and air traffic control to account for the mitigation action, issue advisories, and deconflict other aircraft while the system is active. A mitigation action that does not emit radio frequency energy can likewise affect the airspace near the protected area, for example by bringing an unmanned aircraft down or creating falling debris, so the same real-time air traffic awareness is warranted whether or not the system emits radio frequency energy. The Departments set the timing at five minutes or as soon

as operationally practicable, rather than a fixed advance-notice requirement, because mitigation against a credible threat is time-sensitive and often cannot be predicted far enough in advance to permit prior notice; the standard requires notification at the earliest point that does not compromise the protective action. Notification is routed through a single FAA notification point and follows procedures jointly established by DHS, DOJ, and the FAA, rather than procedures fixed in this part, so that the operational mechanics can be adjusted as the air traffic procedures develop without amending this rule. The SLTT agency must also provide a follow-up notification confirming the time the mitigation action terminates. Real-time notification under this section is distinct from the advance airspace and spectrum coordination required for a planned operation under §§ 124.8 and 124.9; this section addresses the air traffic awareness that a mitigation action requires in real time. Paragraph (d) accordingly confirms that mitigation actions that do not employ RF-emitting systems also require notification under this section, unless the applicable Department of Transportation or FAA notification procedures provide otherwise.

Section 124.12—Detection and warning operations. This section establishes the conditions for detection and warning operations using systems that require the authority of the Act or the relief it provides from certain laws, which do not require per-operation coordination when no RF-emitting system is employed, and prohibits any mitigation action by personnel holding only a Detection and Warning Certification.

The Departments recognize that some SLTT agencies have, before the effective date of this rule, deployed UAS detection systems, including systems that do not require the authority and relief provided by the SAFER SKIES Act. This rule governs operations conducted under 6 U.S.C. 124n(a)(2) on and after the rule's effective date; it does not adjudicate the lawfulness of detection activity conducted before the effective date or under legal authorities other than the Act, and nothing in this rule should be read as a

determination that any particular past deployment was or was not lawful. Prospectively, an SLTT agency that intends to operate a detection system, the operation of which requires the authority of the Act or the relief it provides from certain laws must satisfy the conditions of § 124.12, including the Detection and Warning Certification, Operations Plan, and the detection-and-warning policy or implementation policy.

The Departments have structured these requirements to minimize disruption to existing protective postures: the detection and warning curriculum is delivered online at no cost through the NCUTC training portal, and certification issues automatically upon completion, the detection-and-warning policy is adopted on the SLTT agency's own attestation without pre-approval, and no per-operation coordination is required for passive non-emitting systems (systems that do not actively transmit RF energy). However, systems that involve radio frequency emissions must be evaluated for compliance with the laws and regulations administered by the FCC.

These choices balance the competing concerns directly. Safety is preserved because every operator of a system requiring the Act's authority or relief from criminal liability completes the required curriculum and assessment before operating, and because the certification database gives the Federal Government visibility into who is operating. Privacy is preserved because the privacy protections of § 124.14, including minimization and the retention limit, apply in full to detection operations after the effective date of this rule. Efficiency and cost are addressed by online delivery at no tuition cost, automatic certification, attestation without pre-approval, and the absence of per-operation coordination for passive systems, which together allow an SLTT agency already operating detection equipment to come into compliance in days at the cost of approximately one hour of operator time.

Section 124.13—Post-operation reporting. This section establishes a reporting requirement within 48 hours after a mitigation action is taken; the content of the report;

consolidated, recurring-venue, and persistent-protection reporting; a semiannual operational summary; and the elements compiled to support the biannual congressional report required by 6 U.S.C. 124n(d)(2)(D), including critical-infrastructure protection requests and the requests an agency was unable to support.

The 48-hour reporting requirements and the content elements of the report implement 6 U.S.C. 124n(d)(2)(C)(i), which requires a notification to the Attorney General and the Secretary of Homeland Security "within 48 hours of any mitigation action described in [6 U.S.C. 124n](b)(1)" containing the date, time, and geographic location of the action, a description of the credible threat or safety concern, the type of mitigation capability employed, and any known operational effects. The submission mechanism implements 6 U.S.C. 124n(d)(2)(C)(ii), which directs the Attorney General and the Secretary of Homeland Security to establish a streamlined and secure mechanism for those notifications. Consolidated, recurring-venue, and persistent-protection reporting are burden-reduction formats the Departments adopted for agencies that conduct repeated operations at the same venue or maintain standing fixed-site protection; they preserve every statutory data element while avoiding duplicative per-event filings. The semiannual operational summary and the compiled reporting elements support the report the Attorney General must submit to Congress under 6 U.S.C. 124n(d)(2)(D), including the deployment frequency, location, and circumstance data and the critical-infrastructure protection determination that subparagraph requires.

Section 124.14—Privacy and civil liberties. This section implements the privacy protections of 6 U.S.C. 124n(e), addressing the First Amendment limitation, the scope of interception and incidental capture, data collection minimization and periodic review, the 180-day retention limit for records of communications and its statutory exceptions, the treatment of State and local retention requirements, the bases for dissemination of control communications, the dissemination of pattern data, the protective purpose limitation, the

prohibition on acquiring unlawfully intercepted control communications from third parties, and the audit trail.

Each element implements 6 U.S.C. 124n(e). The First Amendment limitation restates the statutory prohibition on exercising the authority solely to monitor protected activity. The interception and incidental capture provisions define the scope of permissible acquisition of control communications and the handling of communications acquired incidentally. Minimization and periodic review require procedures limiting acquisition, retention, and use to what the protective purpose requires. The 180-day retention limit and its exceptions implement the statutory limit on retaining intercepted communications, and the SLTT agency retention provision addresses the interaction of that Federal limit with SLTT records laws. The dissemination provisions implement the statutory bases on which intercepted communications may be shared, and the pattern data provisions govern derived products. The protective purpose limitation confines use of acquired communications to the protective, law enforcement, and aviation safety purposes related to the UAS activity. The third-party acquisition prohibition forecloses obtaining from a vendor or other third party what the agency could not lawfully intercept itself, and the audit trail creates the record on which the compliance audit program and the Attorney General's oversight under 6 U.S.C. 124n(d)(2)(B) operate.

In calibrating these protections, the Departments made several judgments on which they specifically invite comment. First, the rule construes the statutory retention exceptions narrowly: an ongoing security operation justifies continued retention only where a specific, identified threat supports a discrete protective objective, and a standing operational window does not by itself qualify. Second, for standing detection deployments, the rule pairs the narrowest-technical-configuration requirement with a recurring minimization review, conducted not less than quarterly, to address the heightened incidental capture risk of persistent collection. Third, the rule requires that

pattern data satisfy written anonymization standards adopted in the agency's implementation policy and verified before dissemination outside the agency, rather than prescribing a single national anonymization standard, because aggregation thresholds and re-identification risks vary substantially with jurisdiction size, population density, and event frequency; the adequacy of agency standards is subject to the compliance audit program of § 124.16. The Departments invite comment on the operation of the retention exceptions and their documentation requirements, on whether the rule should prescribe minimum Federal anonymization standards for pattern data, on the conditions governing real-time detection feeds, and on whether additional safeguards are warranted for incidental capture during standing deployments.

Section 124.15—Protection of sensitive operational information. This section requires the protection of sensitive operational information associated with planned or completed operations as well as protection of sensitive Federal and operational information. The protected information includes C-UAS Operations Plans, advance coordination submissions, system capabilities, locations, and coverage patterns, and the tactical procedures associated with planned or completed operations. The section requires agencies to handle that information under access controls and to protect it from public disclosure to the extent permitted by applicable Federal, State, local, Tribal, and territorial law. The section uses a two-tier approach. Information that ties specific system capabilities, vulnerabilities, or countermeasure effectiveness to a planned or completed operation is handled as law enforcement sensitive and evaluated for classification where it reveals a capability gap of national security concern; general operational coordination information, such as the existence, general timing, or general coverage area of a deployment, is handled as Controlled Unclassified Information so that it can be shared with covered partners, including a State-designated aviation point of contact, without the added handling a law enforcement sensitive caveat would impose.

The Departments chose these protections because disclosure of coverage patterns, system locations, or capability details enables a hostile operator to circumvent protection, and the operational record of the Federal C-UAS programs shows that adversaries probe for exactly that information.

Section 124.16—Compliance and enforcement. This section establishes the compliance audit program contemplated by section 8606(b)(2) of the SAFER SKIES Act and addresses the civil penalties and civil enforcement that sections 8605(f) and (g) of the Act establish, including their relationship to suspension. The civil penalties are established by the statute, not by this section; § 124.16 implements the statutory penalty scheme, as discussed together with the graduated penalty levels and assessment factors in the following paragraph. The compliance audit program gives an agency the means to demonstrate, and the Departments the means to verify, compliance with the requirements of this part before a violation occurs.

With respect to civil penalties, section 8605(f) of the SAFER SKIES Act authorizes a civil fine of up to $100,000 per violation or suspension of C-UAS authority pending review by the Attorney General or the Secretary of Homeland Security. If a fine is not paid, section 8605(g) authorizes the Attorney General to bring a civil action in a United States district court to collect such fines and enforce civil penalties. The rule provides for graduated penalty levels proportionate to the severity of the violation and enumerates the factors that inform assessment, including the agency's compliance history, the availability and quality of compliance assistance from Federal partners, whether the violation resulted in actual harm, and whether the agency took prompt corrective action, and it provides that a first violation of a procedural reporting or notification requirement will not draw a penalty where the agency demonstrates a good-faith effort to comply and voluntarily self-reports. The Departments invite comment on the penalty framework, including the graduated structure, the enumerated factors, and the

treatment of first-time procedural violations.

Section 124.17—Confiscation and forfeiture. This section implements the confiscation authority of 6 U.S.C. 124n(b)(1)(E) and the forfeiture provision of 6 U.S.C. 124n(c)(2), addresses in-flight physical interception, and requires that the response to a suspected hazardous device delivered by an unmanned aircraft be conducted by a bomb squad accredited through the Hazardous Devices School. Confiscation under 6 U.S.C. 124n(b)(1)(E) is the seizure or other taking of possession of an unmanned aircraft or UAS consistent with the Act. Forfeiture under 6 U.S.C. 124n(c)(2) follows the law of the seizing agency's jurisdiction, as the statute directs, so the section does not create a Federal forfeiture process. The section also notes that an aircraft on the ground may be seized under traditional law enforcement authority—that is, ordinary seizure authority such as seizure incident to arrest or pursuant to a warrant or a recognized exception to the warrant requirement, without reliance on the Act. In-flight physical interception is addressed because catching or netting an aircraft in flight can implicate several of the statutory authorities at once and carries distinct safety risks; the section therefore directs that personnel conducting such actions hold Mitigation Certification. The bomb squad requirement reflects a deliberate policy choice: an unmanned aircraft that is a potential hazardous or destructive device is the domain of certified public safety bomb technicians, not a C-UAS problem, and render-safe response is a separate discipline with its own national certification structure. Requiring response by a bomb squad accredited through the Hazardous Devices School, consistent with the National Guidelines for Bomb Technicians, keeps that response within the established national framework rather than creating a parallel one.

Section 124.18—Activities for evaluation, testing, training, and pre-operational validation. This section establishes the conditions for operational testing, pre-operational function checks, on-the-job proficiency training, and pre-operational validation, which

are conducted under FCC coordination and authorization and FAA coordination and notification. Testing is the evaluation of a system's function and effects before operational use; proficiency training is recurring operator practice; and pre-operational validation is the verification, before a planned operation, that a system performs as expected at the operating location. These activities are conducted under FCC coordination and authorization and FAA coordination and notification, rather than under the authority of the Act, because the Act's authority is conditioned on a credible threat and these activities, by definition, lack one. The Departments considered permitting testing under the Act's authority and rejected that approach as inconsistent with the statutory predicate; the established Federal mechanisms for experimental spectrum use and airspace safety coordination are the lawful and proven path, and they are the same mechanisms the Federal C-UAS programs use for their own testing.

Section 124.19—Task force arrangements and Federal support. This section preserves existing task force and deputization arrangements under 6 U.S.C. 124n(a)(1), provides that the availability of C-UAS authority through such task force and deputization arrangements neither requires accreditation under this part nor affects those arrangements, and establishes the framework for Federal C-UAS support upon SLTT agency request. The section preserves task force arrangements because 6 U.S.C. 124n(a)(1) authority and 6 U.S.C. 124n(a)(2) authority are separate authorities: an agency with officers who serve as deputized task force officers under Federal sponsorship may continue those arrangements without seeking accreditation under this part, and an accredited agency may still participate in Federal task forces. The Federal support framework establishes how an SLTT agency may request Federal C-UAS support, such as coverage of a threat beyond the agency's certified capabilities. The Departments adopted these provisions to avoid forcing a transition: agencies operating effectively under existing task force models, including those supporting major public events in 2026,

should not lose that posture because a separate path now exists. An agency may also request FBI technical exploitation support for a seized UAS through its local FBI field office.

Section 124.20—Construction. This section sets out rules of construction, including that this part creates no enforceable right, does not authorize action against any aircraft operated with a human pilot, crew, or passengers onboard, and does not create a new basis of liability for officers participating in the protection of identified mass gatherings.

Section 124.21—Termination. This section implements the December 31, 2031, termination date of 6 U.S.C. 124n(j)(2) and provides that obligations and proceedings arising before termination survive it.

Section 124.22—Severability. This section is a severability provision. The provisions in this rule are not necessarily interrelated and can function independent of one another. As such, the Departments believe that most of the provisions of this IFR can function sensibly and independently of other provisions. Therefore, in the event that any provisions in this rule are invalidated by a reviewing court, the Departments intend the remaining provisions to remain in effect to the fullest extent possible.

IV. Regulatory Certifications

A. Administrative Procedure Act

For the reasons described below, there is good cause for the Departments to forgo the APA's notice-and-comment procedures for this rule because following such procedures is impracticable. Additionally, the rule is not subject to the delayed-effective date requirement because it recognizes an exemption or relieves a restriction and because there is good cause for the rule to be immediately effective. Notwithstanding the explanation below, the Departments nonetheless welcome post-promulgation comment on all aspects of this IFR.

1. Good cause to forgo notice and comment

The Administrative Procedure Act ("APA") allows an agency to issue a rule without notice and comment "when the agency for good cause finds . . . that notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest." 5 U.S.C. 553(b)(B). "[T]he good cause exception is to be narrowly construed and only reluctantly countenanced." *Mack Trucks, Inc. v. EPA*, 682 F.3d 87, 93 (D.C. Cir. 2012) (citation and quotation marks omitted). Courts apply "the good cause exception to excuse notice and comment in emergency situations, where delay could result in serious harm, or when the very announcement of a proposed rule itself could be expected to precipitate activity by affected parties that would harm the public welfare." *Am. Pub. Gas Ass'n v. Dep't of Energy* ("*APGA*"), 72 F.4th 1324, 1340 (D.C. Cir. 2023) (cleaned up); *see also California v. Azar*, 911 F.3d 558, 575 (9th Cir. 2018) ("[T]he good cause exception is usually invoked in emergencies . . . .").

Following the notice-and-comment procedures for this rule is impracticable. Impracticability "is generally confined to emergency situations in which a rule would respond to an immediate threat to safety, such as to air travel, or when immediate implementation of a rule might directly impact public safety." *NRDC v. NHTSA*, 894 F.3d 95, 114 (2d Cir. 2018). For instance, it applies when "air travel security agencies would be unable to address threats posing a possible imminent hazard to aircraft, persons, and property within the United States," *Mack Trucks*, 682 F.3d at 93 (internal quotation marks omitted), "if a safety investigation shows that a new safety rule must be put in place immediately," *id.* (internal quotation marks omitted), or when some other "similarly serious threats" exist, *Mid Continent Nail Corp. v. United States*, 846 F.3d 1364, 1380 (Fed. Cir. 2017).

Those circumstances are present here. Recognizing the imminent threat that unmanned aircraft and UAS pose to public safety, Congress passed the SAFER SKIES

Act to provide a framework for SLTT agencies to exercise C-UAS authority independently of Federal task forces and deputization, which limit SLTT agencies to C-UAS activities as part of Federal actions. *See* 6 U.S.C. 124n(a)(2). Congress set a timetable for the Departments to promulgate regulations to govern that authority, with section 8606(a)(1) of the SAFER SKIES Act directing the Secretary of Homeland Security and the Attorney General to do so not later than 180 days after the date of enactment, and 6 U.S.C. 124n(d)(2)(A)(ii) separately requiring the Attorney General to develop the training and certification procedures within the same 180-day period. The Act was signed into law on December 18, 2025, placing the statutory deadline in mid-June 2026. Congress's compressed timetable reflects its own judgment about the urgency of the threat this authority addresses, and that deadline, coupled with the exigency that motivated it, supports the finding here. As explained below in this section, this rule is not only necessary to fulfill Congress's requirement that the Departments develop regulations and guidance, but it responds to immediate threats related to several high-profile events that are or may be the target of nefarious actors.

This rule responds to an immediate threat to safety because a growing number of irresponsible operators ignore flight restrictions and endanger the safety of the airspace and commercial aircraft as they approach airports. In addition, UAS pose an immediate and growing threat to public safety, security at prisons, and national security. For example, they can be used to conduct kinetic attacks using payloads of explosives. *See, e.g.*, *Belfair, Washington, man arrested by FBI in connection to planned attack on government officials at White House UFC event*, DOJ (June 22, 2026), https://www.justice.gov/usao-wdwa/pr/belfair-washington-man-arrested-fbi-connection-planned-attack-government-officials [https://perma.cc/L557-X9MS] (conspirators planned to load explosives onto drones and attack the White House UFC event on one side in order to force attendees to exit where they could be shot with rifles and other

weapons). UAS can also be weaponized with chemical, biological, or nuclear material, used to conduct espionage, and used to traffic in controlled substances and contraband cellphones in prisons. Dep't of Justice, *Securing the Skies: Law Enforcement, Drones, and Public Safety: Hearing Before the S. Comm. on the Judiciary*, 119th Cong. 5 (2025). Furthermore, without this rule, and specifically the rule's requirement and mechanism to coordinate with the FAA, air travel security agencies will become "unable to address threats posing 'a possible imminent hazard to aircraft.'" *Mack Trucks*, 682 F.3d at 93 (quoting *Jifry v. FAA*, 370 F.3d 1174, 1179 (D.C. Cir. 2004)).

The protective need is concrete and increasingly urgent, and this rule provides necessary mechanisms to address that growing need. Prior to this IFR, deputized SLTT agency C-UAS personnel that were fully trained and certified could only be used in connection with a Federal operation or with Federal assistance—they could not engage in C-UAS actions on their own, including to protect their own jurisdictions, without Federal partnership. *See* 6 U.S.C. 124n(a)(1). This rule allows the deputized C-UAS Task Force operators to conduct C-UAS operations to support the missions of their own SLTT agencies and protect their own "large-scale public gatherings or events, critical infrastructure, or correctional facilities." 6 U.S.C. 124n(a)(2). Furthermore, each trained and certified C-UAS operator is a force multiplier: one Mitigation trained and certified SLTT C-UAS operator can activate an entire SLTT C-UAS team, with the remaining members completing the online requirements. And, critically, the rule provides a mechanism for SLTT agencies to both coordinate and to deconflict with the FAA, other agencies in the Federal Government, and with other SLTT agencies.

The authority Congress provided in 6 U.S.C. 124n(a)(2) is conditioned on the training, technology, and oversight requirements in the statute. This rule implements those requirements by establishing a binding framework under which personnel must complete required training and certification, SLTT agencies must adopt implementation

policies, and operators must employ authorized technologies and follow notification and coordination procedures. Without the rule's binding framework, certification of SLTT agency personnel to exercise authority under section 124n(a)(2) would at a minimum be substantially more challenging to monitor and regulate. Specifically, SLTT agencies were able to participate in C-UAS mitigation operations only through Federal task force arrangements under 6 U.S.C. 124n(a)(1), which require Federal sponsorship and individual deputization. Such arrangements could not scale to the public safety need or the volume of SLTT agency operations required to address the current threat level. Current task force arrangements permit SLTT agencies to operate alongside Federal agencies. Section 124n(a)(2) authority, however, would allow SLTT agencies to operate independently, which would drastically increase their capacity in all relevant jurisdictions.

The framework this rule establishes can scale in a way the task force model cannot. At the detection tier, the NCUTC online curriculum and automatic certification can train and certify operators nationwide without resident throughput limits; the Departments expect approximately 1,500 agencies to certify at that tier within two years.[5]

At the mitigation tier, the NCUTC has trained and certified the operators of approximately 46 agencies through its resident courses to date, is conducting additional classes on a continuing schedule, and is expanding the instructor cadre and course frequency to support broader SLTT agency enrollment beginning later in 2026. Although

[5] The Departments note that DOJ has issued a charging policy to encourage certain SLTT agencies with assigned duties that include the security or protection of people, facilities, or assets to engage in C-UAS detection operations (6 U.S.C. 124n(b)(1)(A)) while the Departments developed this rule in part to address the threat posed by unauthorized unmanned aircraft and UAS activity at the Fédération Internationale de Football Association ("FIFA") World Cup™. Acting Attorney General Blanche, *Memorandum to all Federal Prosecutors, Charging Policy Concerning Defensive Actions Against Unmanned Aircraft Systems* (June 12, 2026), https://www.justice.gov/olp/media/1450041/dl?inline. Although the charging policy shields SLTT agencies from chapters 119 and 206 of Title 18 (the Wiretap Act and the prohibition on pen register and trap and trace device use), it does not shield them from State, local, Tribal, or territorial law. In contrast, 6 U.S.C. 124n(a)(2) does shield SLTT agencies from State, local, Tribal, or territorial law, so long as they complete the training detailed in subsection (d)(2). 6 U.S.C. 124n(a)(2) ("notwithstanding the laws of any particular State, local, Tribal, or territorial jurisdiction, and after completing the training detailed in subsection (d)(2)"). As a result, this rule is necessary for SLTT agency detection operations.

deputized SLTT agencies are critical to Federal operations, deputization is insufficient to address the public safety need, which necessarily increases as UAS technologies improve and become more widely accessible. Unmanned aircraft incursions over stadiums, mass gatherings, airports, critical infrastructure, and correctional facilities are documented and recurring, and they present a threat to public safety, and to the safety-of-flight of manned aircraft and lawfully operating UAS in the national airspace system; moreover, the prospect of weaponized drones also presents a threat to national security.[6]

In addition, Federal C-UAS resources cannot be present at every site. Congress extended this authority to SLTT agencies precisely because Federal protective capacity is finite. The record is concrete. The National Football League's chief security officer told Congress in December 2024 that unauthorized drone incursions into the restricted airspace over NFL games grew from roughly a dozen in the 2017 season to 2,537 in 2022 and 2,845 in 2023.[7] Two of those incursions resulted in Federal felony charges announced by the United States Attorney for the District of Maryland: the January 28, 2024, drone flight over M&T Bank Stadium that forced a temporary suspension of the American Football Conference Championship game, and a second flight over the same stadium during a January 11, 2025, playoff game. In December 2024, the United States Attorney for the Central District of California charged a Chinese national who flew a drone over Vandenberg Space Force Base for nearly an hour and photographed the installation after base detection systems tracked the flight. Drone delivery of contraband into correctional facilities is the subject of recurring Federal prosecutions,[8] including the

---

[6] *See, e.g.*, Jordy Fee-Platt, *Man charged with allegedly flying drone above Levi's Stadium during NFL game*, The Athletic (Feb. 3, 2026), https://www.nytimes.com/athletic/7018723/2026/02/03/drone-operator-charged-levis-stadium/.

[7] Statement of Cathy L. Lanier, Chief Security Officer, National Football League, before the House Committee on Homeland Security (Dec. 10, 2024), https://www.congress.gov/118/meeting/house/117754/witnesses/HHRG-118-HM05-Wstate-LanierC-20241210.pdf [https://perma.cc/V8VQ-KN4J].

[8] *See, e.g.*, *Twelve Indicted in Alleged Drone Smuggling Conspiracy at Ten Prisons*, DOJ (June 24, 2026), https://www.justice.gov/usao-mdga/pr/twelve-indicted-alleged-drone-smuggling-conspiracy-ten-prisons [https://perma.cc/U824-36YY].

August 2024 indictments of 23 defendants in the Southern District of Georgia for conspiracies that used drones to deliver methamphetamine, marijuana, and contraband cell phones into State prisons, and earlier prosecutions in the District of Kansas, the Eastern District of California, and the District of New Jersey involving drone deliveries of drugs, cell phones, and tobacco into Federal and State facilities.

The exposure is increasing rapidly: the Fédération Internationale de Football Association ("FIFA") World Cup™, the largest sporting event ever held in the United States, began June 11, 2026, and runs through July 19, 2026, across 11 United States host cities; and the Nation's semiquincentennial celebrations culminate on July 4, 2026, in mass gatherings nationwide.[9]

These events proceed under the same stadium and special-event flight restrictions that the documented incursions repeatedly violated. Since the 2026 FIFA World Cup began, as of June 20, 2026, DHS and the FBI have recorded over 600 drone incursions into restricted airspace across host-city venues, and Federal C-UAS teams seized hundreds of unauthorized drones in multiple host cities.[10] And the highest-attendance matches, including the knockout rounds and the final, remain ahead.

The Nation's 250th anniversary observances bring large public events to multiple major cities on the same days, beginning the first week of July 2026 and continuing through mid-July, including tall-ship naval reviews, aircraft fly-overs, and major municipal fireworks displays. A number of these are federally designated special security events, including a National Special Security Event. Several involve planned manned-aircraft operations in the same airspace as the public gathering, which makes airspace deconfliction of any C-UAS response especially important. SLTT agencies are

---

[9] *See* Holmes Lybrand, *Drones and lone wolf attacks are key concerns as FBI works to secure 11 World Cup cities*, CNN (Jun. 13, 2026), https://www.cnn.com/2026/06/13/politics/drones-lone-wolf-attacks-fbi-world-cup.

[10] *See* David Shepardson, *US agencies have seized more than 300 drones near World Cup sites, TSA says*, Reuters (June 23, 2026), https://www.reuters.com/sports/soccer/us-agencies-have-seized-more-than-300-drones-near-world-cup-sites-tsa-says-2026-06-23/.

already supporting C-UAS protection at these events and will continue to do so through their conclusion, but without this rule's framework, they would not be able to act independently to fully protect their jurisdictions.

The reason these agencies cannot yet operate fully is the nature of the only mechanism now available to them. Most of the personnel the NCUTC has trained are already federally deputized, so the constraint is not the pace of deputization. It is that deputized personnel act under Federal authority and can exercise the C-UAS authorities that depend on the Act's legal protections, including mitigation and the use of RF-emitting systems, only when acting in connection with a Federal operation or with Federal assistance.[11] *See* 6 U.S.C. 124n(a)(1). Federal resources cannot be present at every one of the simultaneous events in July 2026, leaving SLTT agencies unable to nimbly protect their own communities and events under their own authority. This rule supplies the direct pathway that 6 U.S.C. 124n(a)(2) provides. After training and certification through the NCUTC and adoption of an implementation policy, SLTT agencies may exercise these authorities under their own authority, without case-by-case Federal deputization and without a Federal operation on scene. Making that pathway effective on public inspection is what allows these agencies to provide lawful, coordinated, and full C-UAS coverage during the events described above. Any delay for notice and comment would therefore frustrate critical safety and security activities authorized by the Act.

As noted above, approximately 46 SLTT agencies have already completed training and certification through the NCUTC and stand ready to operate, reflecting 61

[11] Specifically, deputized personnel must be operating pursuant to a Federal action or else risk being subject to State, local, Tribal, or territorial law. Section 124n(a)(1) only provides relief from certain Federal laws, which makes sense because it allows deputization of SLTT agency personnel for Federal operations—thus, relief from State, local, Tribal, and territorial laws is unnecessary. Section 124n(a)(2), on the other hand, provides relief from State, local, Tribal, and territorial law, thus providing relief to SLTT agencies engaged in C-UAS activity outside Federal operations so long as they are trained and certified. In other words, the framework in this rule is the key that unlocks SLTT agencies' ability to fully operate independently under the authority Congress provided.

individually certified officers per NCUTC certification records; the framework this rule establishes is one of the remaining requirements, in addition to the establishment of the list of authorized technologies required by 6 U.S.C. 124n(d)(2)(A)(iii). Delaying this rule's framework for pre-promulgation notice and comment would leave trained State and local protective capacity sidelined during the greatest period of need experienced so far. This rule responds to an increasing pattern of imminent threats to public safety, and its immediate implementation directly impacts public safety. *See NRDC*, 894 F.3d at 114.

Finally, the Departments note that they have been diligently working to expand Federal and SLTT agency C-UAS capacity via a range of efforts, of which this rulemaking effort is only one. For instance:

- DOJ has prioritized the full enforcement of applicable civil and criminal laws when drone operators endanger the public, violate established airspace restrictions, or operate a drone in furtherance of an element of another crime[12];
- DOJ, through the FBI, established and continues to expand the NCUTC through a resident mitigation course and an online detection and warning curriculum, which has certified 61 officers across approximately 46 SLTT agencies to date, and is expanding the NCUTC's instructor cadre and course frequency to meet anticipated nationwide demand;
- DHS, through the Federal Emergency Management Agency ("FEMA"), noticed and awarded $250 million in Federal funding in FY 2026 to enhance SLTT agency capabilities to detect, identify, track, or monitor UAS in

[12] *See* E.O. 14305, Restoring American Airspace Sovereignty, 90 FR 24719 (June 6, 2025).

anticipation of the FIFA World Cup™[13];

- The Departments planned, coordinated, and led C-UAS protection across all 11 U.S. host cities for the FIFA World Cup™, ensuring that trained State and local officers embedded in FBI-led task forces are able to support C-UAS operations at tournament venues and associated sites as needed[14]; and
- DHS provided ongoing assistance to Federal coordination teams and SLTT agencies acquiring and implementing C-UAS technologies in the U.S. host cities by optimizing C-UAS sensor placement, coordinating memoranda of understanding, conducting site surveys and RF analyses, enhancing operational strategies, and developing guidance on C-UAS procurement and field placement.[15]

The Departments also note that work on C-UAS matters—including this rule—was necessarily complicated by the lingering effects of a 43-day Federal Government shutdown that lasted from October 1, 2025, through November 12, 2025,[16] and which were compounded by a 75-day DHS-specific government shutdown that followed the

---

[13] *See* Counter Unmanned Aircraft Systems Grant Program, *FEMA* (June 9, 2026), https://www.fema.gov/grants/preparedness/counter-unmanned-aircraft-systems-grant-program [https://perma.cc/CRC2-9MW5].

[14] *See* FBI, *Philadelphia is a 'No Drone Zone' Around FIFA World Cup and Other Special Events This Summer* (June 2, 2026), https://www.fbi.gov/contact-us/field-offices/philadelphia/news/philadelphia-is-a-no-drone-zone-around-fifa-world-cup-and-other-special-events-this-summer.

[15] *See, e.g.*, DHS, *Counter-Unmanned Aircraft Systems (C-UAS) Equipment Placement Field Guidance for State and Local First Responders* (Mar. 9, 2026), https://www.dhs.gov/science-and-technology/publication/c-uas-equipment-placement-field-guidance-responders; DHS, *Purchasing Tool for Counter Unmanned Aircraft Systems (C-UAS)* (Dec. 15, 2025), https://www.dhs.gov/science-and-technology/publication/c-uas-purchasing-tool; DHS, *S&T Lab is Working with State and Local Agencies to Counter Drones at the World Cup* (May 7, 2026), https://www.dhs.gov/science-and-technology/news/2026/05/07/st-lab-working-state-and-local-agencies-counter-drones-world-cup.

[16] *See* Marc Labonte & Lida R. Weinstock, Cong. Rsch. Serv., R48832, *The 2025 (FY2026) Government Shutdown: Economic Effects* (Jan. 29, 2026), https://www.congress.gov/crs-product/R48832 ("The federal government experienced a funding gap beginning on October 1, 2025—the start of FY2026—and ending when the Continuing Appropriations, Agriculture, Legislative Branch, Military Construction and Veterans Affairs, and Extensions Act, 2026 (P.L. 119-37), was signed into law on November 12, 2025"); *see also* Joe Walsh et al., CBS News, *The 2025 U.S. Government Shutdown, by the Numbers* (Nov. 13, 2025), https://www.cbsnews.com/news/2025-government-shutdown-by-numbers/ ("The longest government shutdown in modern U.S. history came to a close Wednesday night when President Trump signed a bill to fund the government through Jan. 30—ending a 43-day-long impasse that had imperiled air travel and left thousands without paychecks.").

Act's enactment and lasted from February 14, 2026, to April 30, 2026.[17] Despite the challenges caused by funding disruptions and workforce shutdowns, the Departments have diligently worked to address UAS-related risks across a range of domains.

2. Immediate effective date

Additionally, the Departments are making this rule immediately effective. This rule recognizes an exemption or relieves a restriction and is thus not subject to the APA's delayed-effective-date requirement. *See* 5 U.S.C. 553(d)(1).

Additionally, there is good cause to forgo a delayed effective date, *see* 5 U.S.C. 553(d)(3), for the reasons provided for forgoing notice and comment explained in Section IV.A.1 of this preamble, but also because no one requires time to comply with the rule's requirements before it becomes effective. The primary purpose of the delayed-effective-date requirement is to give people a reasonable time to prepare to comply with the rule. *See* U.S. Dep't of Just., *Attorney General's Manual on the Administrative Procedure Act* 36 (1947); *Riverbend Farms, Inc. v. Madigan*, 958 F.2d 1479, 1485 (9th Cir. 1992) (holding that the purpose of 5 U.S.C. 553(d) is "to give affected parties time to adjust their behavior before the final rule takes effect"). This rule does not compel SLTT agencies to take any actions discussed in this rulemaking. Indeed, the requirements this rule sets forth reflect the procedures taught at the NCUTC, the resident mitigation courses of which have trained the operators of the SLTT agencies active to date, and participation remains voluntary at every step. Upon publication, the NCUTC will transmit this rule to every agency it has trained. The online detection and warning curriculum, updated to reflect the rule's data handling, dissemination, and retention requirements, will be available through the NCUTC training portal on the effective date; it requires

---

[17] *See* Scott Wong et al., *Record-long Department of Homeland Security Shutdown Ends*, NBC News (Apr. 30, 2026), https://www.nbcnews.com/politics/congress/congress-expected-end-record-75-day-partial-government-shutdown-rcna342903 ("The House on Thursday approved a Senate-passed bill that would fund much of the Department of Homeland Security, ending the record 75-day shutdown of the sprawling federal agency.").

approximately one hour to complete, and certification issues automatically upon completion. Section 124.5(n) preserves existing Mitigation Certifications while previously trained personnel complete that curriculum, so no SLTT agency loses capability on the effective date and no agency requires additional lead time to come into compliance. Additionally, some of the requirements this rule sets forth are already known to the SLTT agencies who acquired C-UAS technologies using FEMA grant dollars earlier in FY 2026. Specifically, the FEMA Notice of Funding Opportunity stipulated that deputized SLTT agency members must enroll and complete the training course at FBI's NCUTC to employ mitigation capabilities funded by Federal grant dollars.[18] Thus, SLTT agency personnel and their agencies do not require additional time to prepare to comply.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act's ("RFA") regulatory flexibility analysis requirements apply only to those rules for which an agency is required to publish a general notice of proposed rulemaking pursuant to 5 U.S.C. 553 or any other law. *See* 5 U.S.C. 604(a). As discussed previously, the Departments did not issue a notice of proposed rulemaking for this action as exempted by 5 U.S.C. 553(b)(B). Therefore, a regulatory flexibility analysis is not required for this rule.

C. Executive Orders 12866 and 13563—Regulatory Review

The Office of Management and Budget ("OMB") has determined that this rulemaking is a "significant regulatory action" under section 3(f) of Executive Order 12866, 58 FR 51735, 51738 (Sept. 30, 1993), but that it is not a section 3(f)(1) significant action. Accordingly, this rule has been submitted to OMB for review. This rule has been drafted and reviewed in accordance with section 1(b) of Executive Order 12866 and

[18] FEMA, *Counter-Unmanned Aircraft Systems Grant Program Fact Sheet* (Nov. 10, 2025), https://www.fema.gov/fact-sheet/counter-unmanned-aircraft-systems-grant-program-fact-sheet [https://perma.cc/6HKW-APHN].

section 1(b) Executive Order 13563, 76 FR 3821 (Jan. 18, 2011).

The changes made by this rulemaking are deregulatory in character and impose no mandate on any SLTT agency. The rule does not require any agency to acquire C-UAS capability or to conduct C-UAS operations; it establishes the framework through which agencies may voluntarily obtain certification and exercise the authority Congress provided, and it removes, for participating agencies that satisfy its conditions, exposure to the criminal prohibitions displaced by the notwithstanding clause of 6 U.S.C. 124n(a)(2). In plain terms, an agency that chooses to participate and follows the rule's conditions can lawfully take protective actions against threatening drones that criminal law would otherwise prohibit; an agency that does not participate is left exactly where it was before. The principal benefits are the public safety, critical infrastructure, and correctional security protections that trained and certified SLTT agencies can provide against UAS threats, the reduced reliance on limited Federal C-UAS assets that SLTT participation makes possible, and the immediate availability of a qualified SLTT law enforcement C-UAS capability for major public events. The principal costs are the training, equipment, coordination, and reporting costs that participating agencies, each of which decides whether the benefits justify those costs in light of its own assessment of its needs and resources, voluntarily incur. Because participation is voluntary, and the rule imposes no mandate, the Departments expect the rule's net effect to be beneficial, with costs falling only on agencies that have determined the capability to be worth the expense.

D. Executive Order 14192—Unleashing Prosperity Through Deregulation

Executive Order 14192, 90 FR 9065 (Jan. 31, 2025), requires an agency, unless prohibited by law, to identify at least 10 existing regulations to be repealed or revised when the agency publicly proposes for notice and comment, or otherwise promulgates, a new regulation that qualifies as an Executive Order 14192 regulatory action (defined in OMB Memorandum M-25-20 as a significant regulatory action as defined in section 3(f)

of Executive Order 12866 that has been finalized and that imposes total costs greater than zero). In furtherance of this requirement, section 3(c) of Executive Order 14192 requires that the incremental costs associated with such new regulations must, to the extent permitted by law, also be offset by eliminating existing costs associated with at least 10 prior regulations. 90 FR 9065. This IFR is an Executive Order 14192 deregulatory action. *See* OMB Memorandum M-25-20, "Guidance Implementing Section 3 of Executive Order 14192, titled 'Unleashing Prosperity Through Deregulation'" (Mar. 26, 2025).

E. Executive Order 14294—Overcriminalization of Federal Regulations

Executive Order 14294, 90 FR 20363 (May 9, 2025), requires agencies promulgating regulations with criminal regulatory offenses potentially subject to criminal enforcement to explicitly describe the conduct subject to criminal enforcement, the authorizing statutes, and the mens rea standard applicable to each element of those offenses. 90 FR 20363. This rule does not create a criminal regulatory offense and is thus exempt from Executive Order 14294 requirements.

F. Executive Order 13132—Federalism

This IFR will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government, as outlined by Executive Order 13132, 64 FR 43255 (Aug. 4, 1999). The IFR implements only a voluntary process for SLTT agencies to obtain certification to use certain C-UAS capabilities consistent with the requirements of the SAFER SKIES Act. By virtue of its "notwithstanding" provision, the SAFER SKIES Act may preempt the conflicting laws of any particular SLTT jurisdiction when a duly qualified SLTT law enforcement or correctional officer takes actions authorized under 6 U.S.C. 124n(a)(2). This IFR does not materially expand the preemptive effect of that provision. In developing this rule, the Departments engaged

with SLTT agencies, including through the NCUTC and through outreach to SLTT agencies, and will continue that engagement through the comment period. The rule also accommodates State and local law where Congress did not displace it: § 124.14(h) addresses the interaction between the Federal retention limit and the SLTT records retention requirements, and § 124.6(b) requires review of the interplay of proposed operations and implementing policies with applicable SLTT law. The Departments specifically invite comment from SLTT officials on all aspects of this rule, including the coordination requirements of § 124.10.

G. Executive Order 12988—Civil Justice Reform

This rule meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988, 61 FR 4729, 4730–32 (Feb. 5, 1996), to specify provisions in clear language. Pursuant to section 3(b)(1)(I) of the Executive Order, nothing in this rule is intended to create any legal or procedural rights enforceable against the United States. *See* 61 FR 4731.

H. Unfunded Mandates Reform Act of 1995

Title II of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–38, UMRA) requires each Federal agency to prepare a written statement assessing the effects of any Federal mandate in a proposed rule or final rule for which the agency published a proposed rule, which includes any Federal mandate that may result in a $100 million or more expenditure (adjusted annually for inflation) in any one year by State, local, and Tribal governments, in the aggregate, or by the private sector.

A written statement under UMRA is not required unless an agency has published a notice of proposed rulemaking. *See* 2 U.S.C. 1532(a). In addition, an action is exempt from UMRA if it is necessary for the national security. *See* 2 U.S.C. 1503(5). As discussed in Section IV.A. of this preamble, this rule is exempt from notice and comment rulemaking procedures and is necessary for the national security. Accordingly, the

Departments have not prepared a written statement in connection with this rule.

I. Paperwork Reduction Act

This rule contains information collection requirements subject to review by the Office of Management and Budget under the Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq.* The information collections in this rule are the agency implementation policy, the detection-and-warning policy, and the portal attestations under § 124.6, feedback on the Authorized Technologies List and Authorized Systems List described in § 124.7, the C-UAS Operations Plan under § 124.8, the advance notification and notice of intent under §§ 124.9 and 124.10, the mutual aid documentation under § 124.4, the real-time air traffic control notification under § 124.11, the post-operation reports and semiannual operational summaries under § 124.13, the testing activities plan under § 124.18, and the recordkeeping, retention determination, and audit trail requirements under § 124.14.

The Departments estimate the burden of these collections as follows, based on an expectation of approximately 1,500 detection-tier and 150 mitigation-tier participating agencies within the first two years.

- Agency implementation policy: approximately 16 hours for a mitigation-tier agency to adapt and adopt the model policy the Departments will publish, including legal review.
- Detection-and-warning policy: approximately 4 hours.
- Portal attestation: approximately 15 minutes, renewed annually.
- Annual policy renewal: approximately 1 to 2 hours.
- Feedback on the lists: approximately 5 minutes for 50 agencies.
- C-UAS Operations Plan: for a mitigation operation, approximately 3 hours per plan on the standardized form, and approximately 1 hour for a renewal plan incorporating a prior plan by reference; for a detection and warning operation,

approximately 30 minutes per plan.

- Advance notification, including the data elements supporting FAA and FCC coordination: approximately 2 to 6 hours per mitigation operation, varying with the number and complexity of RF-emitting systems to be deployed, and expected to trend toward the lower bound as the Authorized Systems List is populated with systems that have completed system-level spectrum evaluation.
- Notice of intent: approximately 30 minutes.
- Mutual aid documentation: approximately 1 hour.
- Post-operation report: approximately 45 minutes per reportable event.
- Semiannual operational summary: approximately 1 hour for a detection-tier agency and 2 hours for a mitigation-tier agency.
- Testing activities plan: approximately 2 hours.
- Recordkeeping, retention determinations, and audit trail maintenance: approximately 2 hours per year for a detection-tier agency and, for a mitigation-tier agency, approximately 2 hours per year plus approximately 1 hour per mitigation operation, or approximately 17 hours per year at the assumed operational tempo.

On these assumptions, and assuming on average 15 mitigation operations per mitigation-tier agency per year and 50 detection and warning operations per detection-tier agency per year, the aggregate annual burden is approximately 65,000 to 80,000 hours across all participating agencies, with a central estimate of approximately 72,000 hours, an average of roughly 33 hours per year for a detection-tier agency and roughly 150 hours per year for a mitigation-tier agency. Monetized respondent costs will be presented in the supporting statement using loaded hourly compensation rates derived from Bureau of Labor Statistics data for law enforcement and correctional personnel. The

Departments invite comment on each of these estimates and assumptions.

The FBI and the Justice Management Division of the Department of Justice will coordinate to finalize the information collection analysis, prepare the supporting statement, and obtain an OMB control number for these collections. The Departments invite comment on the estimated burden of these collections and on ways to minimize that burden.

J. National Environmental Policy Act

The Departments have analyzed this rule under the National Environmental Policy Act of 1969 ("NEPA"), 42 U.S.C. 4321 *et seq*., as amended by the Fiscal Responsibility Act of 2023, and under their respective NEPA implementing procedures, including Department of Homeland Security Directive 023-01 and Instruction Manual 023-01-001-01 and the Department of Justice procedures at 28 CFR part 61. This rule establishes an administrative and procedural framework consisting of training and certification requirements, agency policy and attestation requirements, technology authorization by reference to interagency lists, coordination and notification procedures, reporting, and privacy protections. The rule does not authorize, fund, or direct the construction of facilities, the acquisition or deployment of any equipment, or any other physical activity, and it has no potential to result in environmental effects. The rule therefore qualifies for categorical exclusion under DHS categorical exclusion A3 (rules of a strictly administrative or procedural nature and rules implementing statutory requirements without substantive change), and the Departments have determined that no extraordinary circumstances are present that would warrant preparation of an environmental assessment or environmental impact statement.

List of Subjects

6 CFR Part 124

Aircraft, Aviation safety, Critical infrastructure, Intergovernmental relations,

Investigations, Law enforcement officers, Penalties, Privacy, Reporting and recordkeeping requirements, Security measures, Seizures and forfeitures, Wiretapping and electronic surveillance.

28 CFR Part 124

Aircraft, Aviation safety, Critical infrastructure, Intergovernmental relations, Investigations, Law enforcement officers, Penalties, Privacy, Reporting and recordkeeping requirements, Security measures, Seizures and forfeitures, Wiretapping and electronic surveillance.

Department of Homeland Security

Accordingly, for the reasons set forth in the preamble, title 6 of the Code of Federal Regulations is amended by adding part 124 to read as follows:

PART 124—COUNTER-UNMANNED AIRCRAFT SYSTEM AUTHORITY FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL LAW ENFORCEMENT AND CORRECTIONAL AGENCIES

Sec.

Authority: 5 U.S.C. 301; 6 U.S.C. 124n, as amended by the SAFER SKIES Act (Division H, Title LXXXVI of the National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, sec. 8601–8607, 139 Stat. 718, 1938-45 (2025)).

§ 124.1 Purpose and scope.

(a) *Purpose.* This part implements the authority of the Secretary of Homeland Security and the Attorney General to develop the governance framework for the exercise of all counter-unmanned aircraft system (C-UAS) actions by State, local, Tribal, and territorial (SLTT) law enforcement and correctional agencies and their personnel under 6 U.S.C. 124n(a)(2), as amended by the SAFER SKIES Act. The purpose of actions taken under this authority is to detect, identify, monitor, track, warn, and, if necessary, mitigate credible threats posed by unmanned aircraft or unmanned aircraft systems (UAS) to the safety or security of people, facilities, or assets; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; or a correctional facility.

(b) *Scope.* This part applies to all SLTT law enforcement and correctional agencies, and their personnel seeking to exercise or exercising authority under 6 U.S.C. 124n(a)(2). This part does not govern Federal agency operations under 6 U.S.C. 124n(a)(1), nor deputized SLTT personnel conducting C-UAS as part of an FBI C-UAS task force, which are subject to separate policies and guidance. An SLTT law enforcement or correctional agency that conducts only detection and warning operations using systems the operation of which requires the authority of the Act or the relief it provides from certain laws is subject principally to the Detection and Warning Certification requirement of § 124.5(c), the detection and warning policy provisions of § 124.6(g), the authorized technology requirements of § 124.7, the C-UAS Operations Plan requirement of § 124.8, the operational conditions of § 124.12, and the privacy and data handling requirements of § 124.14.

(c) *Relationship to other laws.* As provided in 6 U.S.C. 124n(a)(2), actions taken

by SLTT law enforcement and correctional agencies and their personnel in compliance with this part may be taken notwithstanding section 46502 of title 49, United States Code, and sections 32, 1030, and 1367 and chapters 119 and 206 of title 18, United States Code, and notwithstanding the laws of any particular State, local, Tribal, or territorial jurisdiction. Nothing in this part vests in the Secretary of Homeland Security or the Attorney General any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration.

(d) *Comprehensive framework.* This part establishes the complete framework governing the exercise of authority under 6 U.S.C. 124n(a)(2), including the training and certification procedures required by 6 U.S.C. 124n(d)(2)(A) and the guidance required by 6 U.S.C. 124n(d)(1) on the matters this part addresses. An SLTT law enforcement or correctional agency and its personnel exercising authority under 6 U.S.C. 124n(a)(2) must conduct operations in accordance with this part. The Attorney General, the Secretary of Homeland Security, the Secretary of Transportation, and the Administrator of the Federal Aviation Administration may issue forms, templates, curricula, and other implementing materials under this part to the extent consistent with law. Where any implementing material addresses a matter also addressed by this part, this part controls. Nothing in this part limits the authority of the Secretary of Homeland Security, the Attorney General, or the Secretary of Transportation to issue guidance under 6 U.S.C. 124n(d)(1) in their respective areas.

(e) *Parallel regulations.* Consistent with section 8606(a)(1) of the Act, identical implementing regulations appear at 6 CFR part 124 and 28 CFR part 124. The Department of Homeland Security and Department of Justice administer and interpret their respective regulations with respect to their own programs, activities, and solely held authorities. Any description in these regulations of the other Department's programs, activities, or solely held authorities is provided for context and does not itself govern the

other Department's exercise of its statutory authorities.

§ 124.2 Definitions.

As used in this part:

Agency accreditation means an agency's eligibility to exercise authority under this part, established when the agency has adopted the implementation policy and completed the portal attestation required by § 124.6(d), deploys only systems within categories on the Authorized Technologies List and, where populated, on the Authorized Systems List, and ensures that its personnel hold the certifications required for the authorities exercised.

Agency Approving Official means the senior official designated by an SLTT law enforcement or correctional agency in its implementation policy under § 124.6(a)(1), or in its detection and warning policy under § 124.6(g), authorized to approve C-UAS operations on behalf of the agency. The Agency Approving Official must not be below the rank of a Senior Executive or Senior Official or its equivalent, except that for an agency in which no equivalent rank exists, the agency head or the agency head's designee may serve as Agency Approving Official. The Agency Approving Official may not serve as a mitigation operator for an operation that official has approved.

Authorized Systems List means the subset of the Authorized Technologies List that identifies specific systems—including make, model, and hardware version—that have been authorized for operational use within one or more technology categories on the Authorized Technologies List. The Authorized Systems List is populated on a phased basis. As systems complete interagency assessment, systems may be added to the Authorized Systems List with appropriate operational limitations based on the approved capabilities, functions, and hardware version of the system.

Authorized Technologies List means the list of authorized technology categories for C-UAS operations by SLTT law enforcement and correctional agencies, maintained

jointly by the Department of Justice, the Department of Homeland Security, the Department of Defense, the Department of Transportation and Federal Aviation Administration, the Federal Communications Commission, and the National Telecommunications and Information Administration, consistent with 6 U.S.C. 124n(d)(2)(A)(iii) and section 8606(a)(4) of the SAFER SKIES Act.

Control communications means any wire, oral, or electronic communication used to navigate, command, or otherwise control a UAS or unmanned aircraft, including telemetry transmitted from the aircraft to its operator, command-and-control signals transmitted from the operator to the aircraft, and any video, audio, or other data stream used by the operator to navigate the aircraft when other navigation telemetry is unavailable or insufficient. The operational role of a communication, rather than its packet type or transmission frequency, determines whether it is a control communication. Whether a communication is a control communication is determined when captured material is processed under § 124.14 and does not require an operator to determine in real time whether a particular video, audio, or data stream is being used to navigate the aircraft. Control communications also include a UAS unique identifier (such as a manufacturer device identifier or serial-correlated number), the operator or take-off location of the UAS, and the location, velocity, and emergency status of the UAS when that information is acquired by intercepting a communication from an unmanned aircraft or unmanned aircraft system pursuant to the relief provided by 6 U.S.C. 124n. The same information is not a control communication when it is obtainable without that relief.

Correctional agency has the meaning given in section 8606(c)(2) of the SAFER SKIES Act.

Correctional facility has the meaning given in 6 U.S.C. 124n(l)(9).

Credible threat means a threat that, based on the totality of circumstances known to the operator at the time of the determination, would cause a reasonable person in the

operator's position, considering the operator's training and experience, to conclude that a UAS or unmanned aircraft poses an articulable risk to the safety or security of people, a facility, or an asset; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; or a correctional facility.

(1) A credible threat may be based on, but is not limited to:

(i) Specific intelligence, including information from law enforcement databases, threat assessments, or intelligence community products;

(ii) Behavioral indicators, including operation in airspace in which UAS operations have been restricted or prohibited by the Federal Aviation Administration, operation not in compliance with Federal Aviation Administration's flight requirements, approach toward a protected interest, failure to respond to warnings, or evasive maneuvering inconsistent with normal flight operations;

(iii) Payload or physical configuration indicators, including observed attachments, modifications, or configurations inconsistent with ordinary recreational or commercial UAS use that suggest capability to cause harm or to deliver prohibited items;

(iv) Unauthorized surveillance or reconnaissance of a protected interest that by law is protected from such activities, or interference with the operational mission of a protected interest;

(v) Indications that the UAS is being used to gain unauthorized access to, or to disclose, classified, law enforcement sensitive, or otherwise lawfully protected information; or

(vi) Pattern-based indicators, including repeated unauthorized UAS activity at a specific location (such as repeat incursions of national defense airspace in violation of 49 U.S.C. 46307), which may inform but do not independently satisfy the credible threat standard.

(2) A credible threat determination rests on the totality of the circumstances. A

single indicator may establish a credible threat where it is sufficiently probative. For mitigation actions under 6 U.S.C. 124n(b)(1)(C), (D), and (F), the determination must be supported by a contemporaneous indicator that the specific unmanned aircraft system or unmanned aircraft at issue poses a current, articulable risk if unabated. For detection and warning actions under 6 U.S.C. 124n(b)(1)(A) and (B), a credible threat determination may also be supported by a reasonable basis to anticipate that one or more unmanned aircraft systems or unmanned aircraft poses an articulable risk. Activity protected by the First Amendment to the Constitution of the United States may not be considered in making a credible threat determination.

Critical infrastructure has the meaning given in subsection (e) of the Critical Infrastructures Protection Act of 2001 (Pub. L. No. 107-56, sec. 1016, 115 Stat. 272, 400-02 (codified at 42 U.S.C. 5195c)), as referenced in 6 U.S.C. 124n(l)(10).

Data purge verification means documented confirmation that records subject to purge have been deleted from all systems on which they were stored. Verification may be performed through an automated system, supervisory review, or other documented confirmation process, and must be recorded in the audit trail required by § 124.14.

Designated Federal C-UAS coordination portal means the electronic submission system designated by the Attorney General and Secretary of Homeland Security for advance notifications, notices of intent, C-UAS Operations Plans, mitigation notifications, post-operation reports, and other submissions required by this part.

Detection and Warning Certification means certification that personnel have successfully completed the online detection and warning training curriculum developed and maintained through the National Counter-UAS Training Center (NCUTC) and passed the post-course assessment. A Detection and Warning Certification authorizes the holder to exercise the authorities described in 6 U.S.C. 124n(b)(1)(A), (B), and (E). The certification is issued automatically through the NCUTC training portal upon successful

completion of the curriculum and assessment and recorded in the NCUTC certification database.

Detection and warning operations means operations conducted using systems the operation of which requires the authority of, or relief from certain laws under, 6 U.S.C. 124n and involve only the actions described in 6 U.S.C. 124n(b)(1)(A) and (B). Detection and warning activity conducted using systems that do not require the authority of 6 U.S.C. 124n (including, for example, electro-optical, infrared, acoustic sensors, and radar) is not subject to this part. Operation of RF-emitting C-UAS systems remains subject to applicable Federal Communications Commission authorization requirements and Federal Aviation Administration coordination if such emission could impact the National Airspace System or other systems located at or near airports.

Detection system means a system or technology used to take an action described in 6 U.S.C. 124n(b)(1)(A) or (B)—that is, to detect, identify, monitor, or track a UAS or unmanned aircraft, or to warn its operator, and that has no capability enabled to disrupt or seize control of, or disable, damage, or destroy a UAS or unmanned aircraft.

FAA-designated coordination mechanism means the program, office, or process designated by the Administrator of the Federal Aviation Administration for the coordination of C-UAS operations that might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace.

Hazardous Devices School means the schoolhouse operated by the Federal Bureau of Investigation at which public safety bomb technicians are certified and recertified in accordance with the National Guidelines for Bomb Technicians, or any successor publication.

Mitigation action means an action described in 6 U.S.C. 124n(b)(1)(C), (D), or (F). Detection and warning, described in 6 U.S.C. 124n(b)(1)(A) and (B), are not mitigation actions.

Mitigation Certification means certification issued by the National Counter-UAS Training Center upon successful completion of the NCUTC mitigation training course or a successor course approved by the Attorney General acting through the Director of the Federal Bureau of Investigation, authorizing the holder to exercise the authorities described in 6 U.S.C. 124n(b)(1)(C), (D), and (F), to the extent consistent with this part and applicable laws, using authorized technologies within the mitigation technology categories covered by the approved mitigation courses the holder has completed. A current Detection and Warning Certification is a prerequisite for obtaining and maintaining a Mitigation Certification.

Mitigation operation means an operation in which a mitigation system is deployed for the purpose of taking an action described in 6 U.S.C. 124n(b)(1)(C), (D), or (F), including disrupting, seizing, or exercising control of, or using reasonable force, if necessary, to disable, damage, or destroy a UAS or unmanned aircraft, whether or not a mitigation action is taken during the operation. A mitigation operation may include elements of detection and warning operations.

Mitigation system means a system or technology used or capable of being employed to take an action described in 6 U.S.C. 124n(b)(1)(C), (D), or (F), including disrupting, seizing or exercising control of, or using force to disable, damage, or destroy a UAS or unmanned aircraft. A system with both detection and mitigation capability is a mitigation system while its mitigation capability is enabled.

National Counter-UAS Training Center (NCUTC) means the national schoolhouse operated by the Federal Bureau of Investigation and designated by the Attorney General, acting through the Director of the Federal Bureau of Investigation, as the national training center for purposes of 6 U.S.C. 124n and as the sole certifying authority for SLTT C-UAS mitigation operators under 6 U.S.C. 124n(d)(2)(A)(i).

Pattern data means a derived data product reflecting aggregated trends,

frequencies, or statistical observations of UAS activity across multiple C-UAS operations that has met the anonymization standards established by the agency's implementation policy and contains no information identifying any specific aircraft, operator, or natural person.

Personnel means officers and employees with assigned duties that include the security or protection of people, facilities, or assets of SLTT law enforcement and correctional agencies, as defined in 6 U.S.C. 124n(a)(2) and (l)(6)(B). This term does not include contractors of SLTT law enforcement and correctional agencies.

Raw sensor data means unprocessed or minimally processed data generated by C-UAS detection or mitigation systems, including radio frequency signal captures, waveform recordings, radar returns, optical and infrared imagery, acoustic signatures, full sensor logs, and system telemetry. Whether a particular item of raw sensor data constitutes a control communication, and is therefore a record of communications subject to the retention limit of § 124.14, is determined by its function.

RF-emitting C-UAS system means any C-UAS system that, when employed for detection or mitigation purposes, actively transmits radio frequency energy to detect, disrupt, disable, or seize control of a UAS or unmanned aircraft. This includes systems employing technologies for detection-only purposes, such as radars that transmit radio frequency signals, that may require a radiolocation service license to be issued from the Federal Communications Commission, and mitigation systems that employ radio frequency jamming (broadband or protocol-specific disruption of command-and-control links, video downlinks, or navigation signals) and radio frequency protocol manipulation (command injection or cyber takeover of control signals).

SLTT law enforcement agency has the meaning given in section 8606(c)(1) of the SAFER SKIES Act.

Special Event Assessment Rating means a rating assigned to an event under the

special event assessment process administered by the Department of Homeland Security, or the equivalent rating under any successor event rating system.

§ 124.3 Scope of authority and mitigation standards.

(a) *Scope of authority.* An SLTT law enforcement or correctional agency exercising authority under 6 U.S.C. 124n(a)(2) may take actions described in 6 U.S.C. 124n(b)(1), which generally include detection, warning, and mitigation, that are necessary to address or eliminate a credible threat that a UAS or unmanned aircraft poses to the safety or security of people, a facility, or an asset; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; or a correctional facility. These statutory categories are functional and are not a prescribed list of property types. The determination of whether a specific property falls within these categories is made by the agency's Agency Approving Official, consistent with this part and 6 U.S.C. 124n. No "covered facility or asset" designation under 6 U.S.C. 124n(l)(3) is required for SLTT law enforcement or correctional agency operations; however, a risk-based assessment is required as part of the Operations Plan, as outlined in § 124.8. Whether the property falls within a section 124n(a)(2) category is a separate question from the credible threat determination. The credible threat determination required by paragraph (b) of this section must be made before any mitigation action.

(b) *Credible threat determination for mitigation actions.* Before taking any mitigation action, personnel must reasonably determine, under the totality of the circumstances, that a credible threat exists, as defined in § 124.2. The determination must be made in real time by the certified and trained personnel closest to the operational situation and documented as part of the post-operation report required by § 124.13. An established pattern of unauthorized UAS activity at a specific location is relevant to the totality of the circumstances and may, in combination with a contemporaneous indicator—including, for example, a new detection event at the same location during a

period consistent with the established pattern—support a credible threat determination. A contemporaneous indicator need not independently establish a threat. Considered with the totality of the circumstances, which may include an established pattern of unauthorized UAS activity, an intelligence indicator, or other contextual information, the contemporaneous indicator must provide a present-tense basis for concluding that the specific aircraft at issue poses a current risk. This operational standard governs individual mitigation decisions by authorized personnel in the application of reasonable force under the totality of the circumstances and does not limit the information or analysis that may be considered at the approval level in determining whether to authorize a C-UAS operation for a specific event or facility.

(c) *Proportionality.* Mitigation actions must be proportionate to the credible threat identified. Personnel must employ the least disruptive effective means of mitigation available under the totality of the circumstances. If equipment is available and time permits, a warning to the remote pilot-in-command should precede any mitigation action. Before taking any mitigation action that may result in the disabling, damage, or destruction of an unmanned aircraft, personnel must consider whether the threat posed by the UAS outweighs the risk of collateral harm to public safety. A mitigation action that creates a greater risk to public safety than the threat it is intended to address is not proportionate and must not be taken. Where a non-mitigation measure is sufficient to eliminate the threat, seizure or destruction of the aircraft should be avoided when feasible. The risk of collateral harm to public safety includes the risk of falling debris, damage to persons or property on the ground, disruption to communications systems, and risks to aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace.

(d) *Protective purpose limitation.* The authority of 6 U.S.C. 124n(a)(2) is limited to the protection of people, facilities, and assets; a venue or set of venues used for large-

scale public gatherings or events; critical infrastructure; and correctional facilities from credible threats posed by unmanned aircraft and UAS. C-UAS authority under this part may not be exercised for the sole purpose of collecting evidence for criminal prosecution or as a substitute for the authority provided by chapter 119 or 206 of title 18, United States Code. Evidence obtained incidental to lawful protective C-UAS operations may be used in subsequent criminal proceedings consistent with applicable law.

(e) *Mitigation operator requirement.* (1) The person who takes a mitigation action, including activating an RF-emitting system, executing a cyber-based takeover, or otherwise causing a C-UAS system to affect or otherwise impact the flight, control, or communications of a UAS or unmanned aircraft, must hold a current Mitigation Certification covering the technology category being employed, and must possess a valid 14 CFR part 107 remote pilot certificate. This requirement is not satisfied by supervision of an uncertified person by a certified operator; the certified operator must be the individual who directly executes the mitigation command or function.

(2) Support functions that do not involve the initiation of mitigation actions, such as detection system monitoring, threat triage and prioritization, ground intercept team dispatch, communications, and administrative functions, do not require Mitigation Certification, but must be performed by personnel trained in accordance with the agency's implementation policy and, where the support function involves operation of systems requiring the authority of 6 U.S.C. 124n(a)(2) or the relief it provides from certain laws, by personnel holding a current Detection and Warning Certification.

(3) For operations involving multiple personnel performing distinct roles, the agency's implementation policy must define the roles and responsibilities of each position, identify which positions require Mitigation Certification, and which require Detection and Warning Certification only, and establish the communication and concurrence procedures between the mitigation operator and other personnel.

(f) *Independent professional judgment.* (1) The certified mitigation operator retains independent professional judgment on whether to initiate a mitigation action.

(2) A supervisor, commander, or other official, regardless of rank, may provide operational direction, tactical context, and coordination guidance to the operator, and may direct the operator to withhold or cease mitigation when broader operational considerations warrant.

(3) A supervisor, commander, or other official may not direct a certified operator to initiate a mitigation action when the operator has determined that the credible threat standard is not met or that the proportionality requirement of paragraph (c) of this section is not satisfied.

(4) The agency's implementation policy must address the chain of command for mitigation decisions and must make clear that non-certified personnel, regardless of rank, may not direct mitigation actions that override the certified operator's professional judgment on whether the conditions for mitigation are present.

(5) An operator who declines to initiate mitigation based on a good-faith professional determination that the conditions for mitigation are not met may not be subjected to adverse employment action for that decision.

(g) *Airspace awareness.* (1) For operations where known authorized manned or unmanned aviation is operating or anticipated in or near the area of operations, the agency's implementation policy or C-UAS Operations Plan must designate a person or position responsible for maintaining real-time awareness of known authorized aviation within the operational area and for ensuring that this information is communicated to personnel authorized to initiate mitigation actions before any mitigation is executed. For purposes of this paragraph, known authorized aviation means any manned or unmanned aircraft that has been identified in the C-UAS Operations Plan, communicated to the C-UAS team during the operation, or otherwise confirmed as lawfully operating in or near

the area of operations. The designated person, or the individual filling the designated position, must have the ability to communicate directly with the mitigation operator. No mitigation action may be initiated without reasonable efforts to confirm that the target is not a known authorized aircraft.

(2) The scope and formality of this role must be commensurate with the complexity of the aviation environment. For operations with minimal or no known authorized aviation, this role may be performed as an additional duty by the certified operator or other command post personnel; for operations with significant aviation activity, the agency must designate a dedicated individual with airspace awareness and coordination responsibilities. When a target cannot be correlated with any known, authorized aircraft and meets the credible threat standard, mitigation may proceed.

§ 124.4 Authorized personnel, contractors, and mutual aid.

(a) *Officers and employees.* The authority provided by 6 U.S.C. 124n(a)(2) may be exercised only by SLTT law enforcement or correctional agency personnel. No SLTT law enforcement or correctional agency may delegate or transfer the exercise of C-UAS mitigation authority to any person or entity that is not an officer or employee of the agency.

(b) *Prohibition on contractor exercise.* Contractors may provide technical support, system maintenance, and training assistance, but may not operate C-UAS mitigation systems, make credible threat determinations, or execute mitigation actions. An arrangement in which a contractor exercises de facto operational control of a C-UAS mitigation system during an operation, including an arrangement described as a turnkey, managed service, or operator-provided C-UAS service, constitutes an unauthorized delegation of authority and is grounds for suspension of accreditation or certification under § 124.5(i). Detection services that do not require the authority of the Act or the relief it provides from certain laws may be provided by contractors.

(c) *Mutual aid and regional C-UAS support.* (1) An SLTT law enforcement or correctional agency accredited under 6 U.S.C. 124n(d)(2) may provide C-UAS support to another SLTT law enforcement or correctional agency, including an agency that is not accredited under this part, under a mutual aid agreement, memorandum of understanding, request for assistance, task force arrangement, or other written arrangement authorized by applicable State, local, Tribal, or territorial law.

(2) When the requesting or host agency is not accredited under 6 U.S.C. 124n(d)(2), the accredited agency providing C-UAS support is the C-UAS operating agency for purposes of this part and is responsible for compliance with the applicable requirements of this part.

(3) Personnel of a non-accredited requesting or host agency may support the operation through ordinary law enforcement, correctional, public safety, evidence-handling, perimeter-security, ground-intercept, evacuation, traffic-control, or incident-command functions. Such personnel may not exercise C-UAS authority under 6 U.S.C. 124n(a)(2), operate systems whose operation requires the authority of or relief from certain laws under 6 U.S.C. 124n, make a credible-threat determination, or initiate any mitigation action, unless those personnel independently satisfy the requirements of this part, hold the applicable certification under § 124.5, and are expressly designated in the accredited C-UAS operating agency's C-UAS Operations Plan to perform that function. Personnel so designated operate under that agency's implementation policy, Agency Approving Official approval, supervision, and compliance responsibility. An individual certification does not, by itself, authorize personnel to exercise 6 U.S.C. 124n(a)(2) authority, and this designation must be established in advance through the C-UAS Operations Plan and the mutual-aid arrangement under paragraph (c)(4) of this section.

(4) The written mutual aid arrangement must identify the requesting or host agency, the accredited agency providing C-UAS support, the legal basis for the

accredited agency's personnel to operate in the host jurisdiction, the allocation of operational responsibilities, and the handling of C-UAS-derived information consistent with §§ 124.14 and 124.15.

(5) For multi-jurisdictional operations, the participating agencies must identify a lead C-UAS agency for tactical C-UAS coordination. The lead C-UAS agency must be an accredited agency unless the operation is conducted under Federal authority pursuant to § 124.19. A non-accredited requesting or host agency may serve as the lead public safety, law enforcement, correctional, or incident-command agency for the overall event or incident, but may not serve as the lead C-UAS agency unless accredited under this part.

(6) An accredited agency may enter into standing regional, county, statewide, or other multi-jurisdictional arrangements to provide recurring or on-call C-UAS support to non-accredited agencies. A standing arrangement does not itself authorize a mitigation operation; each mitigation operation remains subject to the applicable requirements of this part.

(7) Nothing in this part requires a small, rural, or otherwise resource-limited SLTT law enforcement or correctional agency to acquire C-UAS equipment, obtain accreditation, or establish an independent C-UAS program in order to receive C-UAS support from an accredited agency.

(d) *Anti-circumvention.* (1) No SLTT law enforcement or correctional agency, officer, employee, contractor, vendor, or other person may structure or use a mutual aid, regional support, managed-service, technical-support, or other arrangement to evade the requirements of this part.

(2) Prohibited circumvention includes using an accredited agency as a nominal sponsor while a non-accredited agency, contractor, vendor, or other entity exercises de facto operational control of C-UAS activity requiring the authority of or relief from

certain laws under 6 U.S.C. 124n; allowing personnel who lack the certifications required by § 124.5 to exercise C-UAS authority; using systems outside the requirements of § 124.7; avoiding the coordination, reporting, privacy, sensitive-information, or compliance requirements of this part; or acquiring third-party intercepted communications in a manner inconsistent with § 124.14(i).

(3) A mutual aid, regional support, statewide support, county support, or multi-jurisdictional C-UAS arrangement is not circumvention merely because the requesting or host agency is not accredited, provided that the C-UAS operating agency is accredited, the personnel exercising C-UAS authority hold the required certifications, and the operation is conducted in compliance with this part.

§ 124.5 Training and certification.

(a) *Training and certification structure.* This section establishes the training and certification structure implementing the requirements of 6 U.S.C. 124n(d)(2)(A). Detection and Warning Certification governs training for detection and warning operations under 6 U.S.C. 124n(b)(1)(A) and (B). Mitigation Certification governs training and certification for mitigation operations under 6 U.S.C. 124n(b)(1)(C), (D), and (F). A current Detection and Warning Certification is a prerequisite both for initial enrollment in the mitigation training course and for mitigation recertification.

(b) *Agency implementation policy.* Before conducting any operations under this part, an SLTT law enforcement or correctional agency must adopt an agency implementation policy or detection and warning policy and complete the portal attestation in accordance with § 124.6, and must authorize each operation by a C-UAS Operations Plan in accordance with § 124.8, consistent with the other requirements and obligations of this part and applicable laws and policies.

(c) *Detection and Warning Certification.* The Attorney General, acting through the Director of the Federal Bureau of Investigation, will develop and maintain through

the NCUTC an online training curriculum for detection and warning operations, accessible through a secure web-based training portal. The curriculum includes the confiscation authority of 6 U.S.C. 124n(b)(1)(E), evidence preservation, and chain of custody. Only those personnel who have completed the curriculum and passed the post-course assessment may exercise the authorities described in 6 U.S.C. 124n(b)(1)(A), (B), and (E). Upon successful completion, the NCUTC training portal automatically issues a Detection and Warning Certification. Detection and Warning Certification is issued only by the NCUTC, and detection and warning training or certification obtained from another agency or a private entity does not satisfy this requirement. Detection and warning activity conducted using systems that do not require the authority of 6 U.S.C. 124n is not subject to this requirement. Upon successful completion, the training portal records the individual's name, agency, date of completion, and certification status in the NCUTC certification database, which is the system of record for all certifications issued under this section. Each agency must maintain a roster of its certified personnel drawn from the NCUTC certification database and must verify the certification status of personnel assigned to C-UAS operations. Vendor-specific and system-level operator training is the responsibility of each agency through its own training procedures and is not part of the detection and warning curriculum.

(d) *Mitigation training and certification.* (1) The Attorney General, acting through the Director of the Federal Bureau of Investigation, designates the NCUTC 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), as required by 6 U.S.C. 124n(d)(2)(A)(i). Only personnel who hold a valid Mitigation Certification may exercise these authorities. The NCUTC mitigation training program consists of the mitigation training course and such advanced and supplemental courses as the Attorney General, acting through the Director of the Federal Bureau of Investigation, approves. Each

course is evaluated on a pass or fail basis and requires demonstrated proficiency in each mitigation technology category it covers; a person who does not demonstrate proficiency in each category does not pass that course. A person obtains Mitigation Certification by passing the mitigation training course and may extend the scope of that certification to additional mitigation technology categories by passing an advanced or supplemental course covering those additional categories. Failure to pass a particular advanced or supplemental course does not affect the scope of a certification already held.

(2) A person who holds a current Mitigation Certification under this paragraph (d) may conduct mitigation operations at a correctional facility. An abbreviated Correctional Mitigation Certification, limited to correctional-facility operations, is available for personnel who will operate only at correctional facilities.

(3) The mitigation training course under this paragraph is delivered at the NCUTC. The Attorney General, acting through the Director of the Federal Bureau of Investigation, may authorize the Federal Law Enforcement Training Centers or another qualified Federal training provider to deliver the mitigation training course at one or more additional sites, provided the NCUTC retains approval authority over curriculum and standards, exercises oversight of the delivery, and issues all certifications upon verified completion. Any such authorization is at the sole discretion of the Attorney General, acting through the Director, confers no entitlement on any agency or training provider, and may be modified or withdrawn at any time.

(e) *Correctional mitigation training and certification*. The NCUTC offers an abbreviated Correctional Mitigation Certification for personnel who will conduct mitigation operations only at correctional facilities. The correctional course of instruction is shorter than the mitigation training course under paragraph (d) of this section because the fixed perimeter and persistent-threat environment of a correctional facility reduce the operational setup and mission-planning instruction required. The

correctional course of instruction addresses the persistent-threat environment, perimeter operations, and the legal and safety considerations of correctional settings. A person who holds only the Correctional Mitigation Certification may conduct mitigation operations at a correctional facility but may not conduct other mitigation operations under this part. The NCUTC may arrange for the Federal Law Enforcement Training Centers or another qualified training provider to deliver the correctional curriculum, provided the NCUTC retains approval authority over curriculum and standards, exercises oversight of the delivery, and issues all certifications upon verified completion.

(f) *Training standards.* The mitigation training course, as administered by the NCUTC, will include instruction on the legal, operational, and technological aspects of C-UAS operations as required by section 8606(b)(1) of the SAFER SKIES Act, including FAA 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. The Attorney General, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Secretary of Transportation, and the Administrator of the Federal Aviation Administration, will approve training program standards and may approve additional courses of instruction for specialized C-UAS operations. The mitigation training course must include scenario-based instruction on the application of the credible threat standard.

(g) *Eligible personnel.* Personnel eligible for Mitigation Certification or Detection and Warning Certification must have assigned duties that include the security or protection of people, facilities, or assets, as specified in 6 U.S.C. 124n(a)(2), and must be officers or employees of an SLTT law enforcement or correctional agency accredited by the Attorney General acting through the Director of the Federal Bureau of Investigation. The NCUTC, under the authority of the Attorney General, may establish additional attendance prerequisites.

(h) *Sufficiency of certification.* Successful completion of the applicable training requirement, combined with the use of systems within technology categories on the Authorized Technologies List and specific systems on the Authorized Systems List where populated, and compliance with the requirements of this part, satisfies the training and certification prerequisites of 6 U.S.C. 124n(d)(2)(A) for the exercise of the corresponding authorities under 6 U.S.C. 124n(a)(2).

(i) *Suspension.* The Attorney General, acting through the Director of the Federal Bureau of Investigation or the Director's designee, may suspend the Mitigation Certification or Detection and Warning Certification of any individual, or the accreditation of any SLTT law enforcement or correctional agency, for failure to comply with the requirements of this part, violation of the conditions of certification, or for any conduct that demonstrates unfitness to exercise C-UAS authority. Suspension of a certification or accreditation under this section is distinct from suspension of C-UAS authority by the Attorney General or the Secretary of Homeland Security under section 8605(f) of the SAFER SKIES Act, which is addressed in § 124.16. Neither a suspension of certification under this section nor an enforcement action against an individual under section 8605(f) of the SAFER SKIES Act prevents or bars the responsible agency from taking any additional actions it deems necessary to address the circumstances that led to suspension or enforcement action by the Attorney General or designee.

(j) *Suspension notice.* A suspension will be communicated in writing and will specify the basis for the action and any available remedial steps. The suspension notice must include the factual basis for the action in sufficient detail to enable the affected individual or agency to respond. In exigent circumstances, the Director of the Federal Bureau of Investigation or the Director's designee may immediately suspend a certification or accreditation pending administrative review without the requisite written notice when continued exercise of C-UAS authority poses a risk to aviation safety, public

safety, or national security. In such cases, the Director or the Director's designee must provide the requisite notice within 3 days of the suspension.

(k) *Administrative review.* An individual or agency that receives a suspension notice may request administrative review within 30 calendar days of receipt. The Attorney General, acting through the Director of the Federal Bureau of Investigation, will designate a reviewing official of the Department of Justice who did not participate in or supervise the initial decision. The affected party may submit documentary evidence and written witness statements in support of its response. The reviewing official will consider the written submissions of both parties, may conduct an informal hearing at the reviewing official's discretion, and will issue a written determination within 60 calendar days of receipt of the request, stating the factual findings and the basis for the determination. The reviewing official may affirm the action, modify its terms, impose conditions for reinstatement, or reverse the action. A suspension that is affirmed remains in effect until reinstatement under paragraph (m) of this section or the expiration of the suspended certification or accreditation, whichever occurs first.

(l) *Conditions.* The Attorney General, acting through the Director of the Federal Bureau of Investigation, may issue a certification or accreditation subject to conditions, and may modify the conditions of a certification or accreditation, consistent with the standards and procedures applicable to suspension under this section.

(m) *Reinstatement.* An individual or agency whose certification or accreditation has been suspended may apply for reinstatement after completing the remedial steps specified in the suspension notice or the reviewing official's determination. An individual Mitigation Certification may alternatively be reinstated upon the successful recompletion of the full mitigation training course.

(n) *Transition for previously trained personnel.* Personnel holding a Mitigation Certification issued by the NCUTC before the effective date of this part must complete

the detection and warning curriculum under paragraph (c) of this section by September 29, 2026. During that period, the Mitigation Certification remains valid, and the Detection and Warning Certification prerequisite for Mitigation Certification is deemed satisfied. An agency's accreditation is not affected while its personnel complete the curriculum during the transition period.

§ 124.6 Agency implementation policy.

(a) *Requirement.* Before conducting any operations under this part, each SLTT law enforcement or correctional agency must adopt and maintain an agency implementation policy governing the exercise of authority under 6 U.S.C. 124n(a)(2). The agency implementation policy is comprehensive. It governs all operations the agency conducts under this part, including detection and warning operations, and it addresses the detection and warning matters listed in paragraph (g) of this section. An agency that adopts and maintains an agency implementation policy under this paragraph is not required to adopt a separate policy under paragraph (g) of this section. An agency that conducts only detection and warning operations may instead adopt the abbreviated policy under paragraph (g) of this section. The agency implementation policy must, at a minimum:

(1) Designate an Agency Approving Official meeting the requirements of § 124.2;

(2) Designate the personnel authorized to exercise C-UAS authority and describe the recurrent training requirements applicable to such personnel;

(3) Establish procedures consistent with § 124.14 for the handling, retention, and dissemination of data acquired during C-UAS operations, including written anonymization standards specifying the aggregation thresholds, identifier suppression, and re-identification risk assessment used to qualify a data product as pattern data;

(4) Include provisions for public notification regarding the potential use of C-UAS authority within the agency's jurisdiction;

(5) Ensure compliance with the requirements of this part; and

(6) Detail standing tactical procedures governing the execution of C-UAS operations, including engagement protocols that account for the risk to persons and property on the surface and in the air before engagement, escalation procedures, use of force considerations, ground intercept team procedures, render safe procedures, evidence collection and chain-of-custody procedures, communications procedures, system operating procedures, data handling and purge procedures consistent with the retention requirements of this part, operation plan requirements, and post-operation procedures that incorporate data purge verification.

(b) *Legal counsel review.* The implementation policy must be reviewed and concurred in by the agency's legal counsel before adoption and upon each annual renewal. The review must specifically address the privacy and civil liberties requirements of this part, including the data retention, minimization, and dissemination provisions, and the interplay of proposed C-UAS operations and implementing policies with applicable State, local, Tribal, or territorial law. For an agency that has a designated official responsible for the agency's privacy and civil liberties compliance, regardless of title, the implementation policy must also be reviewed by that official.

(c) *Alternative certification for agencies without in-house counsel.* For an agency without in-house counsel, the review required by paragraph (b) of this section may alternatively be satisfied by review and certification by a State, local, territorial, or Tribal attorney's office that the implementation policy addresses each element required by paragraph (a) of this section. An agency obtaining a certification under this paragraph (c) must document the basis for using this paragraph (c). Certification pursuant to this paragraph (c) does not relieve the agency of any compliance obligation under this part.

(d) *Portal attestation.* Upon adoption of the implementation policy, the agency head or designee must certify compliance through the Federal C-UAS coordination portal

by attesting that the agency has adopted an implementation policy addressing each element required by paragraph (a) of this section. The portal records the certifying official, agency, and date of attestation. The implementation policy is not subject to pre-approval by the NCUTC. The NCUTC retains authority to audit implementation policies and to suspend certification or accreditation under § 124.5. The attestation must be renewed annually.

(e) *Retention and availability.* The agency must retain the implementation policy and make it available to the Attorney General or the Secretary of Homeland Security, or their designee, upon request, including during compliance audits under § 124.16.

(f) *Operating without attestation.* An agency that conducts operations under this part without a current portal attestation is in violation of this part, and the absence of an attestation constitutes grounds for compliance action under § 124.16.

(g) *Detection and warning policy.* An SLTT law enforcement or correctional agency that conducts only detection and warning operations requiring the authority of, or the relief from certain laws provided by, 6 U.S.C. 124n may adopt a detection and warning policy in lieu of the implementation policy required by paragraph (a) of this section. A detection and warning policy must satisfy the requirements of this section, except that it need not include the standing tactical procedures of paragraph (a)(6) of this section. The agency must designate an Agency Approving Official under paragraph (a)(1) of this section and complete the portal attestation under paragraph (d) of this section, which must be renewed annually. For purposes of that attestation, a detection and warning policy need address only the elements of paragraph (a) of this section that apply to detection and warning operations.

§ 124.7 Authorized technologies.

(a) *Two-list authorization framework.* The technology authorization framework consists of two complementary lists. 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. Both lists are maintained jointly by the Department of Justice, the Department of Homeland Security, the Department of Defense, the Department of Transportation and Federal Aviation Administration, the Federal Communications Commission, and the National Telecommunications and Information Administration, consistent with 6 U.S.C. 124n(d)(2)(A)(iii) and section 8606(a)(4) of the SAFER SKIES Act.

(b) *General requirement.* An SLTT law enforcement or correctional agency exercising authority under 6 U.S.C. 124n(a)(2) may deploy only systems within technology categories listed on the Authorized Technologies List. When the Authorized Systems List has been populated for a given technology category, the agency may deploy only specific systems listed on the Authorized Systems List within that category, subject to the advance coordination requirements of § 124.9. For technology categories on the Authorized Technologies List for which the Authorized Systems List has not yet been populated, the agency may deploy specific systems within those categories provided that an operator holds Mitigation Certification covering that technology category and has completed manufacturer or vendor training on the specific system to be deployed, subject to the advance coordination requirements of § 124.9.

(c) *Scope of the list requirement.* When operating under the authorities or statutory reliefs in 6 U.S.C. 124n(a)(2), SLTT law enforcement or correctional agencies may employ only listed technology categories, and, where the Authorized Systems List is populated, listed systems. Technology that an SLTT law enforcement or correctional agency may lawfully employ without the authorities or reliefs provided by 6 U.S.C. 124n(a)(2) is not subject to the requirements of this section and remains available to

agencies on the same basis as before the SAFER SKIES Act. The detection and warning training curriculum will address the distinction between technology categories subject to and not subject to this section.

(d) *Mitigation technology and training alignment.* An SLTT law enforcement or correctional agency may employ mitigation systems only in those technology categories covered by the NCUTC mitigation courses completed by its mitigation-certified personnel. NCUTC may create an additional mitigation module covering the technology category when a new technology category is added to the Authorized Technologies List. Mitigation-certified personnel who completed the NCUTC mitigation course prior to the addition of this new content must successfully complete additional NCUTC training on the new technology category prior to using any system on the Authorized Systems List under that category.

(e) *Scope of interception authority.* Systems may be used to intercept communications to or from an unmanned aircraft or UAS only to the extent necessary to support an action described in 6 U.S.C. 124n(b)(1). Any interception, acquisition, maintenance, use of, or access to communications to or from an unmanned aircraft or UAS under this section must be conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law.

(f) *Maintenance of the lists.* The Authorized Technologies List and Authorized Systems List, including the criteria and procedures for evaluating, listing, renewing, suspending, and removing technology categories and systems, are established and maintained through the interagency process described in 6 U.S.C. 124n(d)(2)(A)(iii) and section 8606(a)(4) of the SAFER SKIES Act. The Authorized Systems List is updated by that interagency process and published on the designated interagency C-UAS portal. Each RF-emitting system listed on the Authorized Systems List will have completed a

system-level spectrum evaluation through the interagency process before listing, addressing potential interference with non-Federal spectrum users, compatibility with Federal spectrum users, and potential interference with aviation safety systems. System-level evaluations are reviewed and renewed at intervals determined through the interagency process and upon any system change to its operating capabilities, functions, radio frequency characteristics, or power levels that may alter its radio frequency characteristics, capabilities, functions, or assessed configurations. Minor updates that do not alter a system's performance, capabilities, functions, radio frequency characteristics, or assessed configurations do not require renewed evaluation.

(g) *Emergency suspension.* Upon receipt of an emergency suspension notice issued through the interagency process for the Authorized Technologies List and Authorized Systems List, an SLTT law enforcement or correctional agency must immediately cease deployment of the affected system or technology category. Grounds for emergency suspension include discovery of a critical safety defect, identification of a supply chain compromise or cybersecurity vulnerability, a determination that a system's radio frequency characteristics differ materially from those evaluated during spectrum evaluation, or a finding by any agency participating in the interagency process that continued deployment poses an unacceptable risk. The SLTT law enforcement or correctional agency may not resume deployment of the affected system or technology category until the suspension is lifted or the system or category is restored to the applicable list, and the agency must comply with any conditions attached to the lifting of the suspension or the restoration of the system or category to the applicable list.

§ 124.8 C-UAS Operations Plan.

(a) *Requirement and function.* Each mitigation operation, and each detection and warning operation conducted under this part using systems that require the authority of, or relief from certain laws under, 6 U.S.C. 124n, must be authorized by a C-UAS

Operations Plan signed by the agency's Agency Approving Official. Section 124.12 sets out the conditions specific to detection and warning operations. The signed C-UAS Operations Plan is the instrument authorizing the operation on behalf of the SLTT law enforcement or correctional agency and certifies that the operation is consistent with the agency's implementation or detection and warning policy, that the operators are agency personnel who hold the required training and certification, and that the risk-based assessment factors of paragraph (e) of this section have been addressed. The agency may not commence mitigation operations until both the advance coordination process under § 124.9 and the signed C-UAS Operations Plan are complete.

(b) *Legal counsel certification.* The C-UAS Operations Plan must include a certification by the agency's legal counsel or, for an agency without in-house counsel, the applicable prosecuting authority, that the plan has been reviewed for legal sufficiency. The certification may take the form of a signature block, stamp, or attestation on the plan.

(c) *Form.* The C-UAS Operations Plan must be prepared on the standardized form prescribed by the Attorney General. The form is structured to use short-answer fields, selection-based fields, and map or diagram attachments, and does not require narrative legal analysis or repetition of standing procedures addressed in the agency's implementation policy. The form may use conditional fields keyed to the type of operation, so that each operation completes only the fields applicable to it; for a detection and warning operation, the fields specific to mitigation, such as mitigation-system parameters and render safe planning, do not apply.

(d) *Content.* The C-UAS Operations Plan must address, at a minimum and to the extent applicable to the operation:

(1) Operation identification, including the submitting agency, points of contact, the Agency Approving Official, the operation type, planned dates, geographic location, venue type, any Special Event Assessment Rating or National Special Security Event

designation, and the identification of any mutual aid agencies;

(2) Systems and airspace, including the systems to be deployed by reference to the Authorized Systems List or Authorized Technologies List category; a description of each system's configuration and the hardware version, firmware revision, and software version of each system as deployed; RF-emitting system parameters; class of airspace; and anticipated flight restrictions;

(3) Coordination confirmation, including operator certification status, compliance with the agency implementation policy, the legal counsel certification, and compliance with the privacy and civil liberties requirements of this part; and

(4) Operational planning elements, including deployment configuration and spectrum deconfliction, personnel and team assignments, render safe and contingency planning, known authorized manned and unmanned aviation and deconfliction processes and procedures, communications, investigative response and data handling, and demobilization.

(e) *Risk-based assessment.* The C-UAS Operations Plan must address the following factors: potential impacts to aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace; procedures to comply with any technical and siting limitations; options for mitigating identified potential impacts; potential consequences if potential impacts are not mitigated; the ability to provide reasonable advance notice to aircraft operators of both manned and unmanned aircraft; the setting and character of the facility or asset; for National Special Security Events and Special Event Assessment Rating events, the event characteristics; and the potential consequences to public safety if UAS threats are not mitigated. For National Special Security Events and Special Event Assessment Rating events, a plan that identifies the systems, airspace environment, and coordination elements from which the assessment can be derived satisfies this paragraph without separately addressing each factor in narrative

form. Nothing in this part may be interpreted as limiting the authority of the Administrator of the Federal Aviation Administration to manage the navigable airspace, assess potential aviation safety risks, and implement such mitigations as the Administrator determines appropriate.

(f) *Timing and submission.* The C-UAS Operations Plan must be completed before the commencement of operations and submitted to the Federal Bureau of Investigation and Department of Homeland Security through the designated Federal C-UAS coordination portal as a supplement to the advance notification not fewer than 7 calendar days before the commencement of operations, or as early as practicable when the applicable notification timeline does not permit 7 calendar days. For a detection and warning operation that is not subject to the advance notification requirement of § 124.9, the C-UAS Operations Plan must be submitted through the designated Federal C-UAS coordination portal before the commencement of operations, for situational awareness and recordkeeping; such submission is not an advance notification under § 124.9 and does not trigger Federal Aviation Administration or Federal Communications Commission coordination. The plan may be updated after submission to reflect changes resulting from Federal Aviation Administration or Federal Communications Commission coordination. Material updates must be resubmitted promptly. Federal Aviation Administration and Federal Communications Commission coordination is valid for the system configuration and the firmware and software version coordinated for the operation. A change in configuration, firmware, or software version does not require re-coordination if it does not materially change the system's radio frequency emission characteristics, its operating frequencies and power levels, or other factors potentially impacting aviation safety from those previously coordinated. A change that would operate outside the frequencies or power levels coordinated for the operation requires re-coordination before deployment; a summary of the change must be provided to the

Federal Aviation Administration and Federal Communications Commission to determine if re-coordination is necessary. The Federal Aviation Administration and the Federal Communications Commission may identify by guidance categories of configuration, firmware, or software changes that are deemed to materially affect radio frequency emission characteristics and require re-coordination. Federal review of the C-UAS Operations Plan is for deconfliction and situational awareness purposes and does not constitute approval or disapproval of the operation. For an event, area, or period in which a high volume of simultaneous operations is anticipated, the Federal Bureau of Investigation, in coordination with the Federal Aviation Administration, may establish an earlier submission deadline for affected operations and will communicate that deadline to affected agencies in advance through the designated portal or the lead C-UAS agency.

(g) *Relationship to implementation policy.* The C-UAS Operations Plan is an event-specific or operation-specific document. Standing tactical procedures required by § 124.6(a) must be addressed in the agency's implementation policy, and the C-UAS Operations Plan must reference the implementation policy by title and version rather than repeating standing procedures.

(h) *Operational windows.* (1) An individual C-UAS Operations Plan may authorize operations for a period not to exceed 30 consecutive calendar days, except as provided in paragraph (h)(2) of this section. For operations requiring a longer duration, the agency must submit a renewal plan before the expiration of the current operational window; the renewal plan may incorporate the prior plan by reference and address only material changes. The agency must submit a renewal plan, through the designated Federal C-UAS coordination portal under § 124.8(f), before the expiration of the current operational window.

(2) For fixed-site facilities for which SLTT law enforcement and correctional agencies conduct ongoing persistent-protection operations, including correctional

facilities, critical infrastructure sites, other permanent facilities with a continuing C-UAS mission, and venues where the agency expects to provide recurring C-UAS coverage within the authorization period, the Agency Approving Official may authorize a standing operational window of up to 365 calendar days, renewable upon submission of a renewal plan. The advance notification for a standing operational window must specify the venue and anticipated events or coverage periods; for a detection and warning operation not subject to the advance notification requirement of § 124.9, the C-UAS Operations Plan must specify the venue, the area covered, which may be stated as a radius around the site, and the anticipated coverage periods. Material changes, including a new event, new systems, or a changed threat environment, require an update to the advance notification under § 124.9(a) or, for such a detection and warning operation, an updated C-UAS Operations Plan. Federal coordination requirements continue to apply to each event within a standing window, including lead C-UAS agency coordination under § 124.10 and per-event coordination among the Department of Transportation, the Federal Aviation Administration, and the Federal Communications Commission.

(3) No C-UAS Operations Plan may authorize an indefinite or open-ended operational window.

§ 124.9 Advance coordination, notification, and authorization.

(a) *Advance notification.* (1) Before conducting any mitigation operation under 6 U.S.C. 124n(a)(2), an SLTT law enforcement or correctional agency must submit an advance notification through the designated Federal C-UAS coordination portal not fewer than 30 calendar days before the commencement of the operational period. When 30 calendar days is not feasible, the agency must submit the advance notification as early as the circumstances permit, with sufficient lead time to allow the Federal Bureau of Investigation, the Department of Homeland Security, the Department of Transportation, the Federal Aviation Administration, and the Federal Communications Commission to

complete their respective reviews, and must include a brief explanation of the circumstances that prevented submission within the 30-day standard.

(2) The advance notification is a coordination document that routes the relevant data elements to each recipient agency through a single submission. The advance notification is not a request for approval by the Department of Justice or the Department of Homeland Security, and the absence of a response from the Department of Justice or the Department of Homeland Security does not affect the agency's authority to proceed.

(3) The advance notification must identify the submitting SLTT law enforcement or correctional agency, the planned dates and geographic location of the operation, the systems to be deployed by reference to the Authorized Systems List or Authorized Technologies List category, RF-emitting system parameters, a characterization of the airspace and operational environment, and confirmation of operator certification status and compliance with the agency implementation policy and the privacy requirements of this part.

(b) *C-UAS Operations Plan.* Each mitigation operation must also be authorized by a C-UAS Operations Plan in accordance with § 124.8. The agency may not commence mitigation operations until both the advance coordination process under this section and the signed C-UAS Operations Plan are complete. The SLTT law enforcement or correctional agency must also submit a comparable advance notification to the State if required by State law or policy.

(c) *FBI and DHS notification and routing.* The Attorney General, through the Federal Bureau of Investigation and the Department of Homeland Security, receives the advance notification for purposes of deconflicting planned SLTT law enforcement or correctional agency C-UAS operations with any ongoing or planned Federal C-UAS, law enforcement, or national security operations. Until the portal is fully established, an SLTT law enforcement or correctional agency must notify the Federal Bureau of

Investigation and Department of Homeland Security through a channel designated by the Federal Bureau of Investigation and Department of Homeland Security for that purpose.

(d) *DOT/FAA coordination.* Before conducting any mitigation operation, an SLTT law enforcement or correctional agency must coordinate with the Department of Transportation and the Federal Aviation Administration through the coordination mechanism the Federal Aviation Administration has designated. The agency must provide the systems to be deployed, the geographic coordinates of each proposed deployment and enforcement location, the expected duration of the operation, and a characterization of the airspace environment. The Administrator of the Federal Aviation Administration may establish such flight restrictions as the Administrator determines necessary in his sole discretion for reasons of aviation safety. The absence of a formal flight restriction does not preclude mitigation action in exigent circumstances when a credible threat exists and the requirements of this part are otherwise satisfied.

(e) *Categorical FAA determinations.* The Federal Aviation Administration may issue categorical determinations for specific combinations of authorized technologies, geographic locations, and airspace environments. When a proposed mitigation operation falls within the parameters of a categorical determination by the Federal Aviation Administration, individual case-by-case Federal Aviation Administration coordination is not required, provided the agency operates within the conditions specified in the determination and notifies the Federal Aviation Administration through the Federal Aviation Administration-designated coordination mechanism.

(f) *FCC authorization.* Before deploying any C-UAS system (whether detection and warning only or mitigation) that involves the emission of radio waves, an SLTT law enforcement or correctional agency must obtain authorization to use that system consistent with Title III of the Communications Act of 1934, as amended. The system must comply with any relevant regulations, policies, and guidance administered by the

Federal Communications Commission, and an SLTT law enforcement or correctional agency must submit a request to the Federal Communications Commission through the advance notification process and as directed by the Federal Communications Commission. The Federal Communications Commission will also issue waivers, as appropriate, to C-UAS equipment vendors and manufacturers to allow them to import and sell C-UAS mitigation equipment that employs radio frequency interdiction technologies or electronic counter measures to authorized SLTT law enforcement and correctional agencies.

(g) *Emergency exception.* When a credible threat poses an imminent risk to human life and advance coordination under this section is not practicable, an SLTT law enforcement or correctional agency may take mitigation action. The agency must complete the notifications required by this section as soon as practicable, and in any event within two hours of the action. If the mitigation action involves an RF-emitting C-UAS system, the agency must additionally comply with the real-time notification requirements of § 124.11. Each invocation of this exception must be documented in the post-operation report with a specific explanation of why advance coordination was not feasible. This exception may not be invoked as a routine alternative to advance coordination, and a pattern of repeated invocations may result in compliance review under § 124.16, accreditation or certification suspension, and penalties under section 8605(f) of the SAFER SKIES Act. The compliance audit program will establish the criteria for identifying patterns of emergency invocations that warrant review.

(h) *Federal coordination.* Before conducting any operation under this part within a security or protection mission overseen by a Federal Government entity, or within an area, facility, waterway, or other area over which a Federal Government entity exercises a security or protection responsibility, the agency must coordinate with that Federal Government entity through the advance coordination process under § 124.9 before

conducting the operation. The Federal Aviation Administration's general regulatory authority over the navigable airspace does not by itself trigger this requirement; airspace safety coordination is addressed in § 124.8 and § 124.11.

(i) *Detection and warning operations.* Detection and warning operations that do not actively transmit radio frequency energy and do not affect aviation safety are not subject to the advance coordination requirements of this section.

§ 124.10 Interagency and lead-agency coordination.

(a) *Early coordination and notice of intent.* For operations in support of National Special Security Events, events rated Special Event Assessment Rating 1 through 3, or other events where Federal C-UAS operations are anticipated, an SLTT law enforcement or correctional agency should notify the local FBI field office of its intent to provide C-UAS coverage as early as practicable and before the 30-day advance notification standard of § 124.9. The designated Federal C-UAS coordination portal includes a notice-of-intent function that allows an agency to register its intent to cover a future event without completing the full advance notification. A notice of intent is informational only and does not trigger the advance coordination process, the Federal Aviation Administration or Federal Communications Commission review, or any timeline obligation.

(b) *Special event coordination.* When the Federal Bureau of Investigation receives an SLTT law enforcement or correctional agency advance notification or notice of intent for an event at which Federal C-UAS operations are also planned or under consideration, the Federal Bureau of Investigation will present the notification to the interagency C-UAS coordination process maintained by the Department of Justice and the Department of Homeland Security, will serve as the conduit for SLTT law enforcement and correctional agency equities in that process, and will communicate the results to the SLTT law enforcement or correctional agency, including any Federal operational parameters or deconfliction requirements that may affect the SLTT law

enforcement or correctional agency C-UAS operation. The interagency coordination process does not approve or disapprove SLTT law enforcement or correctional agency C-UAS operations.

(c) *Tactical coordination under a lead C-UAS agency.* An SLTT law enforcement or correctional agency conducting C-UAS operations at an event or location for which a lead C-UAS agency has been designated must operate under the tactical coordination of the lead C-UAS agency for the duration of the event. Tactical coordination includes the assignment of system deployment locations, operating frequencies, detection and mitigation sectors, ground intercept team sectors, render safe locations, communications channels, and risk to persons and property on the surface or in the air. The SLTT law enforcement or correctional agency's C-UAS Operations Plan for the event must be developed in coordination with the lead C-UAS agency and must conform to the lead agency's overall C-UAS operational framework for the event. An SLTT law enforcement or correctional agency coordinating with a lead C-UAS agency acts under its own certified authority under 6 U.S.C. 124n(a)(2); tactical coordination merely integrates the SLTT law enforcement or correctional agency C-UAS operation into a unified C-UAS posture. Where geographic responsibilities are divided among multiple Federal agencies, the SLTT law enforcement or correctional agency must coordinate with the sector-level lead Federal agency responsible for the geographic area in which the SLTT law enforcement or correctional agency intends to operate. Whenever Federal and SLTT operations will be conducted at the same event, or whenever the Federal and SLTT operations will overlap in geographic area and time, the Federal agency will be the lead C-UAS agency. An SLTT law enforcement or correctional agency may serve as the lead C-UAS agency only where multiple SLTT agencies are operating in the same area and no Federal agency is involved.

(d) *Coordination required.* An SLTT law enforcement or correctional agency that

does not accept tactical coordination by the designated lead C-UAS agency may not conduct C-UAS operations, including detection and warning operations using systems requiring the authority of and relief from certain laws under the Act, within the geographic area and time period covered by the lead-agency designation.

(e) *Overlapping SLTT operations.* When the Federal Bureau of Investigation and Department of Homeland Security receive advance notifications from two or more SLTT law enforcement or correctional agencies for C-UAS operations that overlap in geographic area and time, the Federal Bureau of Investigation and Department of Homeland Security will notify all affected SLTT law enforcement and correctional agencies of the overlap. The affected agencies must designate a lead C-UAS agency for the overlapping area and time period, or establish a joint operational coordination arrangement, before any agency commences mitigation operations in the overlapping area. The designation or arrangement must be documented and provided to the Federal Bureau of Investigation and Department of Homeland Security. If the agencies cannot reach agreement within 48 hours of the Federal Bureau of Investigation and Department of Homeland Security's notification, the Federal Bureau of Investigation and Department of Homeland Security may designate operational parameters for the overlapping area, including frequency deconfliction assignments and geographic boundaries for each agency's mitigation operations.

(f) *Deconfliction direction.* If the deconfliction process identifies a conflict between a planned SLTT law enforcement or correctional agency C-UAS operation and an ongoing or planned Federal C-UAS, law enforcement, or national security operation that cannot be resolved through coordination, the Department of Justice, acting through the Federal Bureau of Investigation and in coordination with the Department of Homeland Security, may direct the SLTT law enforcement or correctional agency to modify the operational parameters of, or postpone, the planned operation until the

conflict is resolved.

(g) *Emergency exception preserved.* This section does not affect an SLTT agency's authority to respond to an imminent risk to human life under § 124.9(g), including at an event with a designated lead C-UAS agency; however, the agency must notify the lead C-UAS agency immediately upon taking emergency action and must coordinate with the lead agency as soon as practicable thereafter.

(h) The requirements in paragraphs (a) through (g) of this section are established under the Attorney General's oversight authority pursuant to 6 U.S.C. 124n(d)(1) and the coordination obligations of 6 U.S.C. 124n(b)(4) and (d)(3); they do not transfer or diminish the SLTT agency's statutory authority and relief from certain laws under 6 U.S.C. 124n(a)(2).

§ 124.11 Real-time air traffic control notification.

(a) *Notification required.* Any SLTT law enforcement or correctional agency, or its personnel, that activates a C-UAS system for mitigation purposes must, within five minutes of activation or as soon as operationally practicable, provide verbal or electronic notification to the notification point designated by the Federal Aviation Administration for real-time C-UAS coordination, using the procedures established under paragraph (b) of this section. Detection and warning operations do not require notification or coordination under this section.

(b) *Notification procedures.* An SLTT law enforcement or correctional agency must comply with the notification and reporting procedures jointly established by the Department of Homeland Security, the Department of Justice, and the Federal Aviation Administration for real-time communication to air traffic control of C-UAS mitigation actions using a radio frequency-emitting C-UAS system. The notification must identify the type of C-UAS action, the time of activation, and the location. The NCUTC will include training on these notification procedures in the mitigation training course.

(c) *Notification upon termination.* Upon termination of the mitigation action, the SLTT law enforcement or correctional agency must provide a follow-up notification to the designated Federal Aviation Administration notification point confirming the time of termination.

(d) *Non-RF mitigation.* Mitigation actions that do not involve radio frequency-emitting systems do require notification under this section unless the Department of Transportation or Federal Aviation Administration's applicable notification procedures established under this section provide otherwise. Such actions remain subject to the advance coordination and post-operation reporting requirements of §§ 124.9 and 124.13.

§ 124.12 Detection and warning operations.

(a) *Scope.* This section governs detection and warning operations using systems whose operation requires the authority of and relief from certain laws under 6 U.S.C. 124n(a)(2). Detection and warning activity conducted using systems that do not require the authority of the Act or the relief it provides from certain laws is not subject to this part.

(b) *Conditions.* An SLTT law enforcement or correctional agency may conduct detection and warning operations under this section if:

(1) All personnel conducting detection and warning operations hold a current Detection and Warning Certification;

(2) The agency deploys only systems within technology categories listed on the Authorized Technologies List and, where populated, specific systems listed on the Authorized Systems List;

(3) The agency has adopted an implementation policy under § 124.6(a) or a detection and warning policy under § 124.6(g), has completed the applicable portal attestation, and has authorized the operation by a C-UAS Operations Plan under § 124.8; and

(4) The agency complies with the privacy, data handling, and retention requirements of § 124.14.

(c) *Coordination.* No per-operation (that is, for each individual deployment or activation of a C-UAS system) advance notification, Federal Aviation Administration coordination, or Federal Communications Commission coordination is required for detection and warning operations that employ only systems that do not emit radio frequency energy and do not affect aviation safety. Such operations must be authorized by a C-UAS Operations Plan under § 124.8, which documents operational authority, data handling and retention, and legal review. For detection and warning operations involving RF-emitting systems, such as active warning broadcast systems, the advance coordination requirements of § 124.9 apply, and the operation must be authorized by a C-UAS Operations Plan under § 124.8.

(d) *Reporting.* The 48-hour reporting requirement of § 124.13 does not require per-event reporting of detection and warning operations. Each SLTT law enforcement or correctional agency conducting detection and warning operations under this section must report detection activity in the semiannual operational summary required by § 124.13, including the detection systems deployed by Authorized Technologies List category, the locations at which systems were deployed, the total number of detection events recorded, instances of retention of records of communication beyond 180 days, and any data-sharing arrangements. A physical seizure or confiscation under 6 U.S.C. 124n(b)(1)(E) that results from a detection and warning operation is a 6 U.S.C. 124n action, but it is documented through the agency's normal evidence-handling procedures and is not separately reported under this part. The recovery of a crashed or abandoned unmanned aircraft that does not involve the use of 6 U.S.C. 124n authority is not a 6 U.S.C. 124n confiscation and is not subject to the reporting requirements of this part.

(e) *Prohibition on mitigation.* Personnel holding only a Detection and Warning

Certification are not authorized to take any mitigation action or any other action that affects an unmanned aircraft in flight, regardless of the operator's ultimate objective. If a detection operation identifies a credible threat requiring mitigation, this rule requires that the agency respond through mitigation-certified personnel operating under §§ 124.8 and 124.9 or through coordination with Federal C-UAS assets. This prohibition is absolute and is not subject to the emergency exception of § 124.9(g), which is available only to an agency with mitigation-certified personnel and authorized mitigation capability.

§ 124.13 Post-operation reporting.

(a) *Report required.* Any SLTT law enforcement or correctional agency exercising authority under 6 U.S.C. 124n(a)(2) must submit a post-operation report as required by 6 U.S.C. 124n(d)(2)(C)(i) within 48 hours of whichever occurs first:

(1) Taking any mitigation action described in 6 U.S.C. 124n(b)(1)(C), (D), or (F);

(2) Any confiscation of an unmanned aircraft or UAS under 6 U.S.C. 124n(b)(1)(E); or

(3) The conclusion of an operation where notification was provided.

(b) *Other confiscations*. A confiscation that does not occur pursuant to 6 U.S.C. 124n(b)(1)(E) may be documented through the agency's normal evidence-handling procedures and does not need to be separately reported under this part.

(c) *Content.* The post-operation report must contain:

(1) Confirmation whether the planned operation did or did not occur as notified;

(2) The date, time, and geographic location of the reportable action;

(3) A brief description of the credible threat that a UAS or unmanned aircraft posed to the safety or security of people, a facility, or an asset; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; or a correctional facility necessitating the action;

(4) The type of capability employed, including the specific system or systems

used by reference to the Authorized Systems List and Authorized Technologies List category, or where the Authorized Systems List had not yet been populated for a particular Authorized Technologies List category at the time of the action, the Authorized Technologies List category; and in all cases the make, model, hardware version, firmware revision, and software version of the system or systems as deployed;

(5) Any known operational effects, including the seizure, disabling, damage, or destruction of a UAS or unmanned aircraft; any reported effects on other aviation systems, spectrum users, or persons and property on the surface or in the air; any aviation accident; whether a temporary flight restriction was granted or denied; and any other harm, damage, or loss to a person or to private property;

(6) Any issues, anomalies, or deviations encountered during the operation; and

(7) Summary operational statistics, including the number of UAS detected, counted as confirmed detections attributable to a distinct unmanned aircraft and reported in good faith with reasonable deduplication; warnings issued; mitigation actions taken; UAS or unmanned aircraft seized or confiscated; and any criminal charges, citations, regulatory enforcement actions, or arrests resulting from the operation.

(d) *Submission mechanism.* Reports must be submitted through the designated Federal C-UAS coordination portal. Submission through the portal satisfies the notification requirement to both the Attorney General and the Secretary of Homeland Security, as the portal routes reports to the Federal Bureau of Investigation and Department of Homeland Security automatically.

(e) *Immediate notification for unintended consequences.* If a detection, warning, or mitigation action results in unintended consequences, including interference with manned aviation or lawfully operating UAS, property damage, injury, or system malfunction affecting third parties, the SLTT law enforcement or correctional agency must immediately notify the Federal Bureau of Investigation and Department of

Homeland Security by the most expedient means available, in addition to the 48-hour post-operation report. The Federal Bureau of Investigation will notify the Office of the Deputy Attorney General, the Department of Transportation, the Federal Aviation Administration, the Federal Communications Commission, and other affected agencies as appropriate.

(f) *Consolidated reporting.* Where multiple reportable events occur within a 48 hour period, an SLTT law enforcement or correctional agency may submit a single consolidated post-operation report covering all actions taken during the period, due within 48 hours of the first reportable event, provided that each action is documented with the data elements required by paragraph (c) of this section and that any action resulting in unintended consequences is reported immediately under paragraph (e) of this section.

(g) *Recurring venue reporting.* For recurring venue operations conducted under a standing operational window authorized by § 124.8(h), each discrete event within the authorization period must be reported separately.

(h) *Semiannual operational summary.* Each SLTT law enforcement or correctional agency exercising authority under this part must submit a semiannual operational summary through the designated Federal C-UAS coordination portal, covering total operations conducted, mitigation actions taken, detection activity, instances of retention of records of communication beyond 180 days, instances in which control communications were disclosed outside the originating agency organized by the legal basis for their disclosure, compliance issues identified, and lessons learned. The summary must also report the requests the agency received for C-UAS protection from critical infrastructure or airport owners or operators that are not SLTT law enforcement or correctional agencies, the number of those requests to which it provided protection, and the number it was unable to support as well as the reasons it was unable to provide

support.

(i) *Reporting to support congressional and oversight requirements.* The Federal Bureau of Investigation will compile information from post-operation reports and semiannual summaries to support the biannual report required by 6 U.S.C. 124n(d)(2)(D) and the semiannual briefings required by 6 U.S.C. 124n(g), in coordination with the Secretary of Homeland Security and the Secretary of Transportation. The compilation will include:

(1) The frequency, location, and circumstances of SLTT law enforcement and correctional agencies' mitigation deployments and the types of mitigation employed;

(2) A list of any aviation security or safety incidents, and any aviation accidents, that occurred due to SLTT law enforcement and correctional agencies' deployment of C-UAS technologies;

(3) Recommendations for improving SLTT law enforcement and correctional agencies' C-UAS training, oversight, compliance, and execution, and the compliance audits required by section 8606(b)(2) of the SAFER SKIES Act; and

(4) A determination whether SLTT law enforcement and correctional agencies are able to fully protect critical infrastructure from the UAS threat and, if not, recommendations on how to expand C-UAS authorities to critical infrastructure owners. This determination is informed by the protection-request data reported under paragraph (h) of this section.

(5) Instances in which records of communications were retained beyond 180 days, or in which control communications were disclosed outside the originating agency.

§ 124.14 Privacy and civil liberties.

(a) *General.* In exercising authority under 6 U.S.C. 124n(a)(2), an SLTT law enforcement or correctional agency and its personnel must comply with the requirements of 6 U.S.C. 124n(e), including the implementation of privacy protections with respect to

the interception, acquisition, access, maintenance, use, and dissemination of communications, consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law. All operations under this part must comply with the requirements of the Fourth Amendment and the policies of the applicable SLTT law enforcement or correctional agency with respect to searches and seizures, and individual searches and seizures conducted during C-UAS operations remain subject to the Fourth Amendment reasonableness requirement.

(b) *First Amendment.* No C-UAS authority under this part may be used solely to seize, monitor, deter, interfere with, or disrupt individuals exercising rights protected by the First Amendment to the Constitution of the United States. When C-UAS operations are conducted at events or locations where individuals are exercising First Amendment rights, personnel must take affirmative steps to minimize the collection, retention, and dissemination of information about those individuals, and must not use C-UAS-derived information to identify, track, or build records on individuals based on their exercise of protected rights.

(c) *Scope of interception.* Communications may be intercepted or acquired only to the extent necessary to support an action described in 6 U.S.C. 124n(b)(1).

(1) Material captured that is not control communications is incidental capture. Agencies must configure systems to minimize incidental capture, and incidentally captured material determined not to be relevant to a C-UAS, law enforcement, or national security purpose must not be reviewed, retained, or disseminated and must be purged as soon as practicable.

(2) During the contemporaneous C-UAS operation, personnel may view incidentally captured material only to the extent necessary for C-UAS detection, tracking, identification, or mitigation purposes and may not use it for general surveillance or monitoring. If it becomes apparent that the captured video, audio, or other data stream is

not control communications, the interception of such communications must be discontinued, and the interception of incidentally captured material must be documented in the post-operation report. When a system's configuration permits adjustment of the scope of interception, such as frequency range, geographic coverage, or signal type, operators must use the narrowest configuration consistent with operational effectiveness.

(3) For standing detection deployments exceeding 30 days, the agency must conduct a review, not less than quarterly, to confirm that the scope of interception remains proportionate to the operational need, that incidental collection of non-UAS communications is being minimized, and that data handling and purge procedures are being executed on schedule. The review may be conducted on a program-wide basis for facilities.

(4) Where identifying the threat requires processing the control signaling of all unmanned aircraft in range, the control communications of an unmanned aircraft determined not to pose a threat may not be retained or used beyond what is needed to make the threat determination and must be purged on the same schedule as other incidental material.

(d) *Records of communications and retention.* (1) Control communications captured, recorded, or maintained by SLTT C-UAS systems constitute records of communications to or from a UAS within the meaning of 6 U.S.C. 124n(e)(3) and must be maintained only for as long as necessary, and in no event for more than 180 days, unless the Agency Approving Official or the agency's chief legal officer determines that maintenance of such records is necessary to investigate or prosecute a violation of law, to directly support an ongoing security operation, for the purpose of any litigation, or is required under Federal, State, local, Tribal, or territorial law, consistent with 6 U.S.C. 124n(e)(3).

(2) Data retained under the ongoing security operation exception must be

reviewed at 90-day intervals and purged when the operation concludes, unless another exception applies.

(3) When an agency determines that records of communications will be retained beyond 180 days under any exception, the agency must notify the Federal Bureau of Investigation through the portal within 30 days of the determination.

(4) Pattern data, once extracted and recorded independently, is not a record of communications and is not subject to the 180-day limit. Data generated by systems whose operation does not implicate the electronic surveillance laws referenced in the notwithstanding clause of 6 U.S.C. 124n(a)(2) is likewise not subject to the 180-day limit.

(5) For data retained under the investigation or prosecution exception, the existence of an open investigative or prosecutorial case file documenting the data as evidence satisfies the required determination. For data retained under any other exception, the Agency Approving Official or the agency's chief legal officer must document the specific basis for retention. If an agency has neither an Agency Approving Official nor a chief legal officer, an official holding a rank not below a Senior Executive or Senior Official, or its equivalent, must document the specific basis for retention.

(6) A standing operational window authorized under § 124.8(h) does not itself constitute an ongoing security operation for purposes of the retention exception; that exception applies only when a specific, identified threat or other intelligence justifies continued retention of specific records to support a discrete protective objective, and the 90-day review must assess whether the specific security basis for retention continues to exist.

(7) The exception for retention required under Federal, State, local, Tribal, or territorial law applies when a specific provision of law affirmatively requires retention of the particular type of data at issue, not when a general records retention schedule

incidentally encompasses C-UAS data.

(e) *Dissemination.* (1) Control communications acquired under this part may be disclosed outside the disseminating agency only as authorized by 6 U.S.C. 124n(e)(4): when necessary to investigate or prosecute a violation of law; to support the Department of Defense, a Federal law enforcement agency, or the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory, statutory, or other enforcement action relating to an action described in 6 U.S.C. 124n(b)(1); or as otherwise required by law.

(2) This part does not prohibit the use, as evidence in a subsequent proceeding, of information lawfully obtained incidental to an SLTT law enforcement or correctional agency C-UAS operation, consistent with applicable law.

(3) At the time of any dissemination of control communications, the disseminating agency must document, in the audit trail required by paragraph (g) of this section, the 6 U.S.C. 124n(e)(4) basis for the dissemination, the category of recipient, whether the handling caveat required by paragraph (f) of this section was conveyed, and whether the dissemination included control communications.

(4) A real-time detection feed is governed by the substantive character of the data it transmits. A feed that transmits control communications acquired under this part is subject to the requirements of this section applicable to such data and the limitations under 6 U.S.C. 124n(e)(1), (2), and (4). A feed that transmits only data described in paragraph (e)(6) of this section is not subject to those limitations.

(5) Pattern data that contains no control communications may be disseminated consistent with the agency's standard data handling and information sharing policies and applicable law. Before disseminating pattern data beyond the agency, the disseminating agency must verify anonymization in accordance with its implementation policy and screen the product for operationally sensitive information that would reveal specific

coverage patterns, capabilities, gaps, or methods. Public release of pattern data products requires approval at the level designated by the agency's implementation policy.

(6) Data not acquired using the authorities or reliefs provided by 6 U.S.C. 124n, including data generated by systems whose operation does not implicate the electronic surveillance laws referenced in the notwithstanding clause of 6 U.S.C. 124n(a)(2), is not subject to the disclosure limitations of paragraph (e)(1) of this section and may be shared consistent with the agency's standard data handling and information sharing policies and applicable law. Sharing for situational awareness with recipients that are not law enforcement or correctional agencies, including critical infrastructure owners or operators and the public, is limited to data described in this paragraph, unless the disclosure of control communications is authorized under paragraph (e)(1) of this section.

(f) *Protective purpose limitation.* Because the authority of 6 U.S.C. 124n(a)(2) is limited to mitigation of a credible threat, an SLTT law enforcement or correctional agency may disseminate control communications acquired pursuant to the agency's authorities and statutory reliefs under 6 U.S.C. 124n(a)(2) only for law enforcement action arising from the UAS activity that prompted the C-UAS operation, or for aviation safety. An SLTT law enforcement or correctional agency may not disseminate such control communications for use in an investigation or enforcement action unrelated to UAS activity unless the communications are independently obtainable through lawful means not dependent on the authorities and statutory reliefs under 6 U.S.C. 124n(a)(2). At the time of dissemination, the disseminating agency must communicate the protective purpose for which the control communications are being shared.

(g) *Audit trail.* Each SLTT law enforcement or correctional agency exercising authority under this part must maintain an audit trail sufficient to document each instance in which C-UAS authority was exercised, the basis for the action, the disposition of any data acquired, and any dissemination of data under this part. The audit trail must be

searchable and accessible to compliance auditors, protected against unauthorized modification or deletion, and retained for a minimum of 6 years. The agency's implementation policy must specify the format and system of records for the audit trail.

(h) *State and local retention conflicts.* When an SLTT law enforcement or correctional agency determines that a State, local, Tribal, or territorial records retention requirement applicable to law enforcement or correctional agency records encompasses C-UAS communications data and the agency cannot comply with both the 180-day retention limit and that retention requirement, the agency must retain the data for the period required by the applicable law and must apply the handling restrictions of this part, including the prohibition on use for unrelated law enforcement purposes and the dissemination restrictions of this section, for the full duration of retention.

(i) *Third-party acquisition.* An SLTT law enforcement or correctional agency may not request, purchase, subscribe to, or operationally rely on intercepted UAS control communications acquired by any actor lacking lawful authority and relief from certain otherwise applicable laws for the underlying interception, regardless of whether the agency directed or facilitated the original interception. An agency acquiring UAS intelligence from a third-party source must document the source's lawful authority and relief from otherwise applicable laws for any intercepted content and must apply the retention and dissemination requirements of this section to data so acquired. The agency's implementation policy must specify procedures for evaluating third-party source authority and relief from certain otherwise applicable laws, which must include review and concurrence by appropriate State, local, territorial, or Tribal legal counsel.

(j) *Vendor data sharing.* An SLTT law enforcement or correctional agency may provide operational raw sensor data to system vendors for purposes of system diagnostics, troubleshooting, and performance validation, provided that any communications content is removed before disclosure and the data is used solely for the

specific purpose identified. The agency's implementation policy must establish the conditions for vendor data sharing consistent with this paragraph and applicable privacy protections.

§ 124.15 Protection of sensitive operational information.

(a) *Sensitive system information.* Information that links the specific capabilities, vulnerabilities, operating parameters, or countermeasure effectiveness of C-UAS systems to planned or completed operations, including deployment locations, operating radio frequencies, tactical employment methods, and threat-specific mitigation approaches, must be treated as law enforcement sensitive, protected from public disclosure to the extent permitted by applicable law, and, where the information reveals a capability gap of national security concern, evaluated for classification. Other operational coordination information associated with a planned or completed operation, such as the existence, general timing, or general coverage area of a deployment, must be handled as Controlled Unclassified Information and may be shared with covered Federal and SLTT law enforcement and correctional partners, including a State-designated aviation point of contact, for a lawful government purpose. General technical specifications and evaluation data not associated with a specific planned or completed operation are not subject to these handling requirements. All information described in this paragraph remains subject to any applicable classification, export control, or proprietary restriction.

(b) *Protection from disclosure.* An SLTT law enforcement or correctional agency must take the steps available under applicable State, local, Tribal, or territorial law to protect operationally sensitive information from disclosure through public records requests or civil discovery, and should coordinate with the prosecuting authority in criminal prosecutions arising from C-UAS operations to limit testimony and pleadings to the information necessary to establish the elements of the offense. Nothing in this section requires an agency to take any action inconsistent with applicable State, local, Tribal, or

territorial public records law.

(c) *Markings.* Advance notifications, C-UAS Operations Plans, post-operation reports, and compliance audit records must be marked with appropriate sensitivity designations.

(d) *Permitted disclosures.* This section does not prohibit disclosure of sensitive system information to authorized Federal officials, to other participating SLTT agencies in the course of operational coordination, or to the public to the extent required by statute or court order.

§ 124.16 Compliance and enforcement.

(a) *Compliance audits.* The Attorney General, in coordination with the Secretary of Homeland Security and the Administrator of the Federal Aviation Administration, will periodically conduct compliance audits of SLTT law enforcement and correctional agencies exercising authority under 6 U.S.C. 124n(a)(2), as required by 6 U.S.C. 124n(d)(2)(B) and section 8606(b)(2) of the SAFER SKIES Act, to oversee compliance with this part and the privacy protections of 6 U.S.C. 124n(e) as well as to prevent misuse of C-UAS authority. The audit program will include review of post-operation reports, advance notification records, and agency implementation policies. The FAA will participate with respect to the aviation safety, airspace safety coordination, and deconfliction aspects of the compliance audits conducted under this section.

(b) *Civil fines and penalties.* An SLTT law enforcement or correctional agency, or its personnel authorized to take mitigation actions under 6 U.S.C. 124n(a)(2), that knowingly engages in such actions without Federal coordination as required by 6 U.S.C. 124n and the SAFER SKIES Act, including the advance coordination required by § 124.9, the real-time air traffic control notification required by § 124.11, and the post-action notification to the Attorney General and the Secretary of Homeland Security required by 6 U.S.C. 124n(d)(2)(C) and implemented by § 124.13(a), may be subject to a

civil fine of up to $100,000 per violation, or suspension of C-UAS authority pending review by the Attorney General or the Secretary of Homeland Security, as provided in section 8605(f) of the SAFER SKIES Act. Civil penalties will be assessed in accordance with graduated penalty levels proportionate to the severity of the violation and the factors set forth in this part, including the agency's compliance history, the availability and quality of compliance assistance from Federal partners, whether the violation resulted in actual harm, and whether the agency took prompt corrective action. A civil penalty will not be assessed for a first violation of a procedural reporting or notification requirement when the agency demonstrates a good-faith effort to comply and voluntarily self-reports the deficiency. Violations of requirements of this part other than the Federal coordination requirements described in this paragraph do not give rise to civil penalties under section 8605(f) of the SAFER SKIES Act; they are addressed through the compliance audit program of this section, certification and accreditation suspension under § 124.5, and any other remedy available under law.

(c) *Civil enforcement.* The Attorney General is authorized to bring a civil action in a United States district court to collect fines and enforce civil penalties imposed under this section against any agency or individual, as provided in section 8605(g) of the SAFER SKIES Act.

(d) *Relationship to certification or accreditation suspension.* In addition to civil penalties, the Attorney General or designee may suspend a Mitigation Certification, Detection and Warning Certification, or accreditation under § 124.5(i) for violations of this part. Certification or accreditation suspension may be imposed independently of or in conjunction with other actions described in this section.

§ 124.17 Confiscation and forfeiture.

(a) *Confiscation authority.* (1) An SLTT law enforcement or correctional agency and its personnel may seize or otherwise confiscate a UAS or unmanned aircraft as

described in 6 U.S.C. 124n(b)(1)(E). This authority is contingent on a credible threat and applies to the physical taking of possession of an unmanned aircraft that is no longer active in flight or any other UAS component, such as a ground control station.

(2) This authority does not require Mitigation Certification, the use of systems on the Authorized Technologies List or Authorized Systems List, or advance coordination under § 124.9. However, personnel exercising confiscation authority under 6 U.S.C. 124n(b)(1)(E) must hold a current Detection and Warning Certification issued by the NCUTC. An officer who seizes an unmanned aircraft or any other UAS component under traditional law enforcement authority, including an abandoned or crashed unmanned aircraft, does not require Detection and Warning Certification.

(3) Any action that employs C-UAS technology to disrupt or seize control of, damage, disable, or destroy the unmanned aircraft or UAS is an action under 6 U.S.C. 124n(b)(1)(C), (D), or (F) and requires Mitigation Certification.

(4) Personnel exercising confiscation authority should follow standard law enforcement evidence handling procedures, including maintaining chain of custody, preserving digital evidence stored on the aircraft or its flight controller, and observing applicable hazardous materials precautions.

(5) This part does not affect the authority of any law enforcement or correctional officer to take physical custody of an unmanned aircraft or UAS under traditional law enforcement authority independent of 6 U.S.C. 124n. Traditional law enforcement authority refers to the seizure authorities generally available to law enforcement under applicable Federal, State, local, Tribal, or territorial law, including seizure incident to arrest, seizure of evidence or contraband pursuant to a warrant or a recognized exception to the warrant requirement, and seizure of abandoned property. Once an unmanned aircraft or UAS is on the ground and confiscated, subsequent law enforcement actions, including threat assessment, render safe procedures, evidence collection, and search

warrant execution, are governed by traditional legal authorities, including Fourth Amendment requirements and applicable exigency or emergency doctrines, rather than by 6 U.S.C. 124n.

(6) When a C-UAS operation involves a known or suspected unmanned aircraft being used as a delivery mechanism for a hazardous device, the response to the hazardous device must be conducted by a public safety bomb squad accredited through the Hazardous Devices School, consistent with the National Guidelines for Bomb Technicians or any successor publication.

(7) The physical act of interception of a third-party unmanned aircraft while it is in flight, such as catching or netting an aircraft by hand or using a non-electronic physical device to capture it in the air, implicates 6 U.S.C. 124n(b)(1)(D), (E), or (F). Personnel conducting such actions must therefore hold a Mitigation Certification. This does not apply to the erection of physical barriers that a drone operator has an obligation to avoid, such as netting affixed to a physical structure.

(b) *Forfeiture.* Any UAS or unmanned aircraft seized by an SLTT law enforcement or correctional agency pursuant to 6 U.S.C. 124n(a)(2) is subject to forfeiture under the laws of the seizing agency's jurisdiction, as provided in 6 U.S.C. 124n(c)(2).

§ 124.18 Activities for evaluation, testing, training, and pre-operational validation.

(a) *Scope and legal basis.* An SLTT law enforcement or correctional agency that holds current accreditation under this part may conduct operational acceptance testing of acquired systems and systems under procurement consideration, on-the-job proficiency training, and interoperability training exercises to maintain C-UAS operational readiness. Testing and training do not and must not involve the mitigation of a credible threat and are not conducted under the authority of 6 U.S.C. 124n(a)(2). The operation of RF-emitting systems during testing and training is conducted under applicable Federal

Communications Commission authorization and Federal Aviation Administration coordination requirements, and only against controlled test targets owned or operated by, or operated with the consent of, the SLTT law enforcement or correctional agency. An SLTT law enforcement or correctional agency acting pursuant to this section may utilize only authorized technologies under § 124.7. The SLTT law enforcement or correctional agency is responsible for verifying that all necessary Federal Aviation Administration authorizations or regulatory relief for operation of any unmanned aircraft or UAS, including unmanned aircraft or UAS forming part of a C-UAS system, have been obtained prior to any testing, training, or exercises. Compliance with this section is a condition of maintaining certification and accreditation under this part.

(b) *Personnel.* Only personnel holding a current Mitigation Certification may operate mitigation systems during evaluation testing, training, and exercises. Testing, training, and exercises may not be used to train or evaluate uncertified personnel on the operation of mitigation systems. Contractors and vendor representatives may provide technical support and instruction on system-specific procedures but may not independently operate mitigation systems against test targets.

(c) *Evaluation testing and training activities plan.* Before conducting testing, training, or exercises involving RF-emitting C-UAS mitigation systems, the agency must prepare a written activities plan specifying the date, time, and location; the purpose; the systems and equipment to be used; the test, training, or exercise targets; the assigned operators; safety controls; privacy measures; the types of data to be collected and their planned disposition; documentation of Federal Aviation Administration and Federal Communications Commission spectrum coordination for the C-UAS activities, and documentation of any necessary Federal Aviation Administration authorizations or regulatory relief for the operator of the target unmanned aircraft or UAS and for the operation any unmanned aircraft or UAS that form part of the C-UAS system. The

activities plan must be approved by the Agency Approving Official or designee and reviewed by the agency's legal counsel.

(d) *Coordination.* Testing, training, and exercises, involving RF-emitting systems, or systems that may affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace, require advance coordination with the Federal Aviation Administration and, for spectrum authorization, with the Federal Communications Commission.

(e) *Privacy within evaluation testing and training.* The agency must favor testing, training, and exercise locations and activities that minimize exposure to non-participating third parties. The agency must not intentionally target, monitor, or collect the communications of non-participating third parties. Communications incidentally collected from non-participating third parties must be purged at the conclusion of the testing, training, or exercise activity, or as soon as practicable thereafter.

(f) *Mitigation restriction.* During testing, training, and exercises, the agency may not intentionally mitigate any UAS or unmanned aircraft that is not a controlled test target, unless necessary to protect against an imminent risk to human life or as part of an approved C-UAS Operations Plan. An action taken to protect against an imminent risk to human life must comply with the emergency exception set forth in § 124.9(g).

(g) *Pre-operational validation.* Before commencing mitigation operations at an event or facility, an agency may conduct pre-operational validation or equipment functional checks within the operational window and airspace restrictions already coordinated through the advance notification process under § 124.9. The C-UAS Operations Plan must document the pre-operational validation plan and required notifications. No separate authorization from the Department of Homeland Security or the Department of Justice beyond the advance notification is required.

(h) *Participation in Federal RTTE*. Personnel holding active Mitigation

Certification may participate in research, testing, training, and evaluation (RTTE) events conducted by Federal components under 6 U.S.C. 124n(b)(3). Personnel may engage with systems in mitigation technology categories beyond those for which they hold an active Mitigation Certification or that are not on the ATL or ASL as part of the event. Participants act under the Federal component's authority and supervision.

§ 124.19 Task force arrangements and Federal support.

(a) *Task force and deputization arrangements preserved.* Task force and deputization arrangements under 6 U.S.C. 124n(a)(1) are not affected by this part. An SLTT law enforcement or correctional agency participating in such an arrangement may continue that participation indefinitely, so long as the deputizing Federal agency continues to have C-UAS authority and relief from certain laws under 6 U.S.C. 124n(a)(1). Nothing in this part requires an agency to seek accreditation under this part, conditions any task force or deputization arrangement on accreditation, or terminates or limits any such arrangement.

(b) *Concurrent authority.* The availability of independent SLTT law enforcement and correctional agency authority under 6 U.S.C. 124n(a)(2) does not preclude continued participation in C-UAS task forces or deputization arrangements under 6 U.S.C. 124n(a)(1). An SLTT law enforcement or correctional agency and its officers may exercise independent authority and participate in Federal task force operations concurrently or at different times as operational circumstances warrant. Task force operations are governed by the policies applicable to the sponsoring Federal component.

(c) *Federal support.* An SLTT law enforcement or correctional agency may request C-UAS support from an authorized Department of Justice or Department of Homeland Security component. Such support, when provided, constitutes a Federal operation under 6 U.S.C. 124n(a)(1) and is governed by the policies applicable to the supporting component, and the requesting agency's personnel participating in the

operation do so under the Federal component's authority and supervision, consistent with applicable task force or deputization arrangements. No formal gubernatorial request is required under this part. Support from the Department of Defense, when available, is governed by the Department of Defense's own authorities, including 10 U.S.C. 130i and 2564, and applicable Department of Defense policies, not by this part.

§ 124.20 Construction.

(a) *No private right.* This part is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(b) *Manned aircraft.* Nothing in this part authorizes the use of C-UAS authority against any aircraft or aircraft system operated with a human pilot, crew, or passengers onboard.

(c) *Mass gatherings.* Consistent with 6 U.S.C. 124n(h)(5), nothing in this part provides a new basis of liability for any State, local, territorial, or Tribal law enforcement officer who participates in the protection of a mass gathering identified by the Secretary of Homeland Security or the Attorney General under 6 U.S.C. 124n(l)(3)(C)(iii)(II), acts within the scope of the officer's authority, and does not exercise the authority granted to the Secretary of Homeland Security and the Attorney General by 6 U.S.C. 124n.

(d) *Statutory scope*. Nothing in this part alters the scope of the authority of, or the statutory reliefs under 6 U.S.C. 124n(a)(2). A determination that an action does not comply with this part may give rise to administrative, civil, or other consequences provided by law, but does not by itself determine whether the action falls outside the scope of the statutory authorization in, or the relief from criminal liability available under, 6 U.S.C. 124n. Such a determination will be made by the Attorney General, in coordination with the Secretary of Homeland Security and other appropriate officials.

§ 124.21 Termination.

(a) *Termination.* Absent additional statutory authority, the authority of SLTT law enforcement and correctional agencies and their personnel under 6 U.S.C. 124n(a)(2) will terminate on December 31, 2031, as provided in 6 U.S.C. 124n(j)(2).

(b) *Savings.* Termination under paragraph (a) of this section does not affect any obligation, proceeding, or liability that arose before the termination date. Recordkeeping, retention, audit, reporting, and enforcement obligations with respect to operations conducted before the termination date, and any administrative or civil proceeding arising from those operations, survive the termination of authority under this part and remain in effect until satisfied or otherwise resolved.

§ 124.22 Severability.

If any provision of this part, or the application of any provision to any person, entity, or circumstance, is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of this part, and the application of its provisions to any other persons, entities, or circumstances, shall not be affected and shall remain in full force and effect.

DEPARTMENT OF JUSTICE

Accordingly, for the reasons set forth in the preamble, and by the authority vested in the Assistant Attorney General for the Office of Legal Policy by Attorney General Order Number 6966-2026, title 28 of the Code of Federal Regulations is amended by adding part 124 to read as follows:

PART 124—COUNTER-UNMANNED AIRCRAFT SYSTEM AUTHORITY FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL LAW ENFORCEMENT AND CORRECTIONAL AGENCIES

Sec.

Authority: 5 U.S.C. 301; 6 U.S.C. 124n, as amended by the SAFER SKIES Act (Division H, Title LXXXVI of the National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, sec. 8601–8607, 139 Stat. 718, 1938-45 (2025)).

§ 124.1 Purpose and scope.

(a) *Purpose.* This part implements the authority of the Secretary of Homeland Security and the Attorney General to develop the governance framework for the exercise of all counter-unmanned aircraft system (C-UAS) actions by State, local, Tribal, and territorial (SLTT) law enforcement and correctional agencies and their personnel under 6 U.S.C. 124n(a)(2), as amended by the SAFER SKIES Act. The purpose of actions taken under this authority is to detect, identify, monitor, track, warn, and, if necessary, mitigate credible threats posed by unmanned aircraft or unmanned aircraft systems (UAS) to the safety or security of people, facilities, or assets; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; or a correctional facility.

(b) *Scope.* This part applies to all SLTT law enforcement and correctional agencies, and their personnel seeking to exercise or exercising authority under 6 U.S.C. 124n(a)(2). This part does not govern Federal agency operations under 6 U.S.C.

124n(a)(1), nor deputized SLTT personnel conducting C-UAS as part of an FBI C-UAS task force, which are subject to separate policies and guidance. An SLTT law enforcement or correctional agency that conducts only detection and warning operations using systems the operation of which requires the authority of the Act or the relief it provides from certain laws is subject principally to the Detection and Warning Certification requirement of § 124.5(c), the detection and warning policy provisions of § 124.6(g), the authorized technology requirements of § 124.7, the C-UAS Operations Plan requirement of § 124.8, the operational conditions of § 124.12, and the privacy and data handling requirements of § 124.14.

(c) *Relationship to other laws.* As provided in 6 U.S.C. 124n(a)(2), actions taken by SLTT law enforcement and correctional agencies and their personnel in compliance with this part may be taken notwithstanding section 46502 of title 49, United States Code, and sections 32, 1030, and 1367 and chapters 119 and 206 of title 18, United States Code, and notwithstanding the laws of any particular State, local, Tribal, or territorial jurisdiction. Nothing in this part vests in the Secretary of Homeland Security or the Attorney General any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration.

(d) *Comprehensive framework.* This part establishes the complete framework governing the exercise of authority under 6 U.S.C. 124n(a)(2), including the training and certification procedures required by 6 U.S.C. 124n(d)(2)(A) and the guidance required by 6 U.S.C. 124n(d)(1) on the matters this part addresses. An SLTT law enforcement or correctional agency and its personnel exercising authority under 6 U.S.C. 124n(a)(2) must conduct operations in accordance with this part. The Attorney General, the Secretary of Homeland Security, the Secretary of Transportation, and the Administrator of the Federal Aviation Administration may issue forms, templates, curricula, and other implementing materials under this part to the extent consistent with law. Where any

implementing material addresses a matter also addressed by this part, this part controls. Nothing in this part limits the authority of the Secretary of Homeland Security, the Attorney General, or the Secretary of Transportation to issue guidance under 6 U.S.C. 124n(d)(1) in their respective areas.

(e) *Parallel regulations.* Consistent with section 8606(a)(1) of the Act, identical implementing regulations appear at 6 CFR part 124 and 28 CFR part 124. The Department of Homeland Security and Department of Justice administer and interpret their respective regulations with respect to their own programs, activities, and solely held authorities. Any description in these regulations of the other Department's programs, activities, or solely held authorities is provided for context and does not itself govern the other Department's exercise of its statutory authorities.

§ 124.2 Definitions.

As used in this part:

Agency accreditation means an agency's eligibility to exercise authority under this part, established when the agency has adopted the implementation policy and completed the portal attestation required by § 124.6(d), deploys only systems within categories on the Authorized Technologies List and, where populated, on the Authorized Systems List, and ensures that its personnel hold the certifications required for the authorities exercised.

Agency Approving Official means the senior official designated by an SLTT law enforcement or correctional agency in its implementation policy under § 124.6(a)(1), or in its detection and warning policy under § 124.6(g), authorized to approve C-UAS operations on behalf of the agency. The Agency Approving Official must not be below the rank of a Senior Executive or Senior Official or its equivalent, except that for an agency in which no equivalent rank exists, the agency head or the agency head's designee may serve as Agency Approving Official. The Agency Approving Official may not serve

as a mitigation operator for an operation that official has approved.

Authorized Systems List means the subset of the Authorized Technologies List that identifies specific systems—including make, model, and hardware version—that have been authorized for operational use within one or more technology categories on the Authorized Technologies List. The Authorized Systems List is populated on a phased basis. As systems complete interagency assessment, systems may be added to the Authorized Systems List with appropriate operational limitations based on the approved capabilities, functions, and hardware version of the system.

Authorized Technologies List means the list of authorized technology categories for C-UAS operations by SLTT law enforcement and correctional agencies, maintained jointly by the Department of Justice, the Department of Homeland Security, the Department of Defense, the Department of Transportation and Federal Aviation Administration, the Federal Communications Commission, and the National Telecommunications and Information Administration, consistent with 6 U.S.C. 124n(d)(2)(A)(iii) and section 8606(a)(4) of the SAFER SKIES Act.

Control communications means any wire, oral, or electronic communication used to navigate, command, or otherwise control a UAS or unmanned aircraft, including telemetry transmitted from the aircraft to its operator, command-and-control signals transmitted from the operator to the aircraft, and any video, audio, or other data stream used by the operator to navigate the aircraft when other navigation telemetry is unavailable or insufficient. The operational role of a communication, rather than its packet type or transmission frequency, determines whether it is a control communication. Whether a communication is a control communication is determined when captured material is processed under § 124.14 and does not require an operator to determine in real time whether a particular video, audio, or data stream is being used to navigate the aircraft. Control communications also include a UAS unique identifier (such as a

manufacturer device identifier or serial-correlated number), the operator or take-off location of the UAS, and the location, velocity, and emergency status of the UAS when that information is acquired by intercepting a communication from an unmanned aircraft or unmanned aircraft system pursuant to the relief provided by 6 U.S.C. 124n. The same information is not a control communication when it is obtainable without that relief.

Correctional agency has the meaning given in section 8606(c)(2) of the SAFER SKIES Act.

Correctional facility has the meaning given in 6 U.S.C. 124n(l)(9).

Credible threat means a threat that, based on the totality of circumstances known to the operator at the time of the determination, would cause a reasonable person in the operator's position, considering the operator's training and experience, to conclude that a UAS or unmanned aircraft poses an articulable risk to the safety or security of people, a facility, or an asset; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; or a correctional facility.

(1) A credible threat may be based on, but is not limited to:

(i) Specific intelligence, including information from law enforcement databases, threat assessments, or intelligence community products;

(ii) Behavioral indicators, including operation in airspace in which UAS operations have been restricted or prohibited by the Federal Aviation Administration, operation not in compliance with Federal Aviation Administration's flight requirements, approach toward a protected interest, failure to respond to warnings, or evasive maneuvering inconsistent with normal flight operations;

(iii) Payload or physical configuration indicators, including observed attachments, modifications, or configurations inconsistent with ordinary recreational or commercial UAS use that suggest capability to cause harm or to deliver prohibited items;

(iv) Unauthorized surveillance or reconnaissance of a protected interest that by

law is protected from such activities, or interference with the operational mission of a protected interest;

(v) Indications that the UAS is being used to gain unauthorized access to, or to disclose, classified, law enforcement sensitive, or otherwise lawfully protected information; or

(vi) Pattern-based indicators, including repeated unauthorized UAS activity at a specific location (such as repeat incursions of national defense airspace in violation of 49 U.S.C. 46307), which may inform but do not independently satisfy the credible threat standard.

(2) A credible threat determination rests on the totality of the circumstances. A single indicator may establish a credible threat where it is sufficiently probative. For mitigation actions under 6 U.S.C. 124n(b)(1)(C), (D), and (F), the determination must be supported by a contemporaneous indicator that the specific unmanned aircraft system or unmanned aircraft at issue poses a current, articulable risk if unabated. For detection and warning actions under 6 U.S.C. 124n(b)(1)(A) and (B), a credible threat determination may also be supported by a reasonable basis to anticipate that one or more unmanned aircraft systems or unmanned aircraft poses an articulable risk. Activity protected by the First Amendment to the Constitution of the United States may not be considered in making a credible threat determination.

Critical infrastructure has the meaning given in subsection (e) of the Critical Infrastructures Protection Act of 2001 (Pub. L. No. 107-56, sec. 1016, 115 Stat. 272, 400-02 (codified at 42 U.S.C. 5195c)), as referenced in 6 U.S.C. 124n(l)(10).

Data purge verification means documented confirmation that records subject to purge have been deleted from all systems on which they were stored. Verification may be performed through an automated system, supervisory review, or other documented confirmation process, and must be recorded in the audit trail required by § 124.14.

Designated Federal C-UAS coordination portal means the electronic submission system designated by the Attorney General and Secretary of Homeland Security for advance notifications, notices of intent, C-UAS Operations Plans, mitigation notifications, post-operation reports, and other submissions required by this part.

Detection and Warning Certification means certification that personnel have successfully completed the online detection and warning training curriculum developed and maintained through the National Counter-UAS Training Center (NCUTC) and passed the post-course assessment. A Detection and Warning Certification authorizes the holder to exercise the authorities described in 6 U.S.C. 124n(b)(1)(A), (B), and (E). The certification is issued automatically through the NCUTC training portal upon successful completion of the curriculum and assessment and recorded in the NCUTC certification database.

Detection and warning operations means operations conducted using systems the operation of which requires the authority of, or relief from certain laws under, 6 U.S.C. 124n and involve only the actions described in 6 U.S.C. 124n(b)(1)(A) and (B). Detection and warning activity conducted using systems that do not require the authority of 6 U.S.C. 124n (including, for example, electro-optical, infrared, acoustic sensors, and radar) is not subject to this part. Operation of RF-emitting C-UAS systems remains subject to applicable Federal Communications Commission authorization requirements and Federal Aviation Administration coordination if such emission could impact the National Airspace System or other systems located at or near airports.

Detection system means a system or technology used to take an action described in 6 U.S.C. 124n(b)(1)(A) or (B)—that is, to detect, identify, monitor, or track a UAS or unmanned aircraft, or to warn its operator, and that has no capability enabled to disrupt or seize control of, or disable, damage, or destroy a UAS or unmanned aircraft.

FAA-designated coordination mechanism means the program, office, or process

designated by the Administrator of the Federal Aviation Administration for the coordination of C-UAS operations that might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace.

Hazardous Devices School means the schoolhouse operated by the Federal Bureau of Investigation at which public safety bomb technicians are certified and recertified in accordance with the National Guidelines for Bomb Technicians, or any successor publication.

Mitigation action means an action described in 6 U.S.C. 124n(b)(1)(C), (D), or (F). Detection and warning, described in 6 U.S.C. 124n(b)(1)(A) and (B), are not mitigation actions.

Mitigation Certification means certification issued by the National Counter-UAS Training Center upon successful completion of the NCUTC mitigation training course or a successor course approved by the Attorney General acting through the Director of the Federal Bureau of Investigation, authorizing the holder to exercise the authorities described in 6 U.S.C. 124n(b)(1)(C), (D), and (F), to the extent consistent with this part and applicable laws, using authorized technologies within the mitigation technology categories covered by the approved mitigation courses the holder has completed. A current Detection and Warning Certification is a prerequisite for obtaining and maintaining a Mitigation Certification.

Mitigation operation means an operation in which a mitigation system is deployed for the purpose of taking an action described in 6 U.S.C. 124n(b)(1)(C), (D), or (F), including disrupting, seizing, or exercising control of, or using reasonable force, if necessary, to disable, damage, or destroy a UAS or unmanned aircraft, whether or not a mitigation action is taken during the operation. A mitigation operation may include elements of detection and warning operations.

Mitigation system means a system or technology used or capable of being

employed to take an action described in 6 U.S.C. 124n(b)(1)(C), (D), or (F), including disrupting, seizing or exercising control of, or using force to disable, damage, or destroy a UAS or unmanned aircraft. A system with both detection and mitigation capability is a mitigation system while its mitigation capability is enabled.

National Counter-UAS Training Center (NCUTC) means the national schoolhouse operated by the Federal Bureau of Investigation and designated by the Attorney General, acting through the Director of the Federal Bureau of Investigation, as the national training center for purposes of 6 U.S.C. 124n and as the sole certifying authority for SLTT C-UAS mitigation operators under 6 U.S.C. 124n(d)(2)(A)(i).

Pattern data means a derived data product reflecting aggregated trends, frequencies, or statistical observations of UAS activity across multiple C-UAS operations that has met the anonymization standards established by the agency's implementation policy and contains no information identifying any specific aircraft, operator, or natural person.

Personnel means officers and employees with assigned duties that include the security or protection of people, facilities, or assets of SLTT law enforcement and correctional agencies, as defined in 6 U.S.C. 124n(a)(2) and (l)(6)(B). This term does not include contractors of SLTT law enforcement and correctional agencies.

Raw sensor data means unprocessed or minimally processed data generated by C-UAS detection or mitigation systems, including radio frequency signal captures, waveform recordings, radar returns, optical and infrared imagery, acoustic signatures, full sensor logs, and system telemetry. Whether a particular item of raw sensor data constitutes a control communication, and is therefore a record of communications subject to the retention limit of § 124.14, is determined by its function.

RF-emitting C-UAS system means any C-UAS system that, when employed for detection or mitigation purposes, actively transmits radio frequency energy to detect,

disrupt, disable, or seize control of a UAS or unmanned aircraft. This includes systems employing technologies for detection-only purposes, such as radars that transmit radio frequency signals, that may require a radiolocation service license to be issued from the Federal Communications Commission, and mitigation systems that employ radio frequency jamming (broadband or protocol-specific disruption of command-and-control links, video downlinks, or navigation signals) and radio frequency protocol manipulation (command injection or cyber takeover of control signals).

SLTT law enforcement agency has the meaning given in section 8606(c)(1) of the SAFER SKIES Act.

Special Event Assessment Rating means a rating assigned to an event under the special event assessment process administered by the Department of Homeland Security, or the equivalent rating under any successor event rating system.

§ 124.3 Scope of authority and mitigation standards.

(a) *Scope of authority.* An SLTT law enforcement or correctional agency exercising authority under 6 U.S.C. 124n(a)(2) may take actions described in 6 U.S.C. 124n(b)(1), which generally include detection, warning, and mitigation, that are necessary to address or eliminate a credible threat that a UAS or unmanned aircraft poses to the safety or security of people, a facility, or an asset; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; or a correctional facility. These statutory categories are functional and are not a prescribed list of property types. The determination of whether a specific property falls within these categories is made by the agency's Agency Approving Official, consistent with this part and 6 U.S.C. 124n. No "covered facility or asset" designation under 6 U.S.C. 124n(l)(3) is required for SLTT law enforcement or correctional agency operations; however, a risk-based assessment is required as part of the Operations Plan, as outlined in § 124.8. Whether the property falls within a section 124n(a)(2) category is a separate question from the credible threat

determination. The credible threat determination required by paragraph (b) of this section must be made before any mitigation action.

(b) *Credible threat determination for mitigation actions.* Before taking any mitigation action, personnel must reasonably determine, under the totality of the circumstances, that a credible threat exists, as defined in § 124.2. The determination must be made in real time by the certified and trained personnel closest to the operational situation and documented as part of the post-operation report required by § 124.13. An established pattern of unauthorized UAS activity at a specific location is relevant to the totality of the circumstances and may, in combination with a contemporaneous indicator—including, for example, a new detection event at the same location during a period consistent with the established pattern—support a credible threat determination. A contemporaneous indicator need not independently establish a threat. Considered with the totality of the circumstances, which may include an established pattern of unauthorized UAS activity, an intelligence indicator, or other contextual information, the contemporaneous indicator must provide a present-tense basis for concluding that the specific aircraft at issue poses a current risk. This operational standard governs individual mitigation decisions by authorized personnel in the application of reasonable force under the totality of the circumstances and does not limit the information or analysis that may be considered at the approval level in determining whether to authorize a C-UAS operation for a specific event or facility.

(c) *Proportionality.* Mitigation actions must be proportionate to the credible threat identified. Personnel must employ the least disruptive effective means of mitigation available under the totality of the circumstances. If equipment is available and time permits, a warning to the remote pilot-in-command should precede any mitigation action. Before taking any mitigation action that may result in the disabling, damage, or destruction of an unmanned aircraft, personnel must consider whether the threat posed by

the UAS outweighs the risk of collateral harm to public safety. A mitigation action that creates a greater risk to public safety than the threat it is intended to address is not proportionate and must not be taken. Where a non-mitigation measure is sufficient to eliminate the threat, seizure or destruction of the aircraft should be avoided when feasible. The risk of collateral harm to public safety includes the risk of falling debris, damage to persons or property on the ground, disruption to communications systems, and risks to aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace.

(d) *Protective purpose limitation.* The authority of 6 U.S.C. 124n(a)(2) is limited to the protection of people, facilities, and assets; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; and correctional facilities from credible threats posed by unmanned aircraft and UAS. C-UAS authority under this part may not be exercised for the sole purpose of collecting evidence for criminal prosecution or as a substitute for the authority provided by chapter 119 or 206 of title 18, United States Code. Evidence obtained incidental to lawful protective C-UAS operations may be used in subsequent criminal proceedings consistent with applicable law.

(e) *Mitigation operator requirement.* (1) The person who takes a mitigation action, including activating an RF-emitting system, executing a cyber-based takeover, or otherwise causing a C-UAS system to affect or otherwise impact the flight, control, or communications of a UAS or unmanned aircraft, must hold a current Mitigation Certification covering the technology category being employed, and must possess a valid 14 CFR part 107 remote pilot certificate. This requirement is not satisfied by supervision of an uncertified person by a certified operator; the certified operator must be the individual who directly executes the mitigation command or function.

(2) Support functions that do not involve the initiation of mitigation actions, such as detection system monitoring, threat triage and prioritization, ground intercept team

dispatch, communications, and administrative functions, do not require Mitigation Certification, but must be performed by personnel trained in accordance with the agency's implementation policy and, where the support function involves operation of systems requiring the authority of 6 U.S.C. 124n(a)(2) or the relief it provides from certain laws, by personnel holding a current Detection and Warning Certification.

(3) For operations involving multiple personnel performing distinct roles, the agency's implementation policy must define the roles and responsibilities of each position, identify which positions require Mitigation Certification, and which require Detection and Warning Certification only, and establish the communication and concurrence procedures between the mitigation operator and other personnel.

(f) *Independent professional judgment.* (1) The certified mitigation operator retains independent professional judgment on whether to initiate a mitigation action.

(2) A supervisor, commander, or other official, regardless of rank, may provide operational direction, tactical context, and coordination guidance to the operator, and may direct the operator to withhold or cease mitigation when broader operational considerations warrant.

(3) A supervisor, commander, or other official may not direct a certified operator to initiate a mitigation action when the operator has determined that the credible threat standard is not met or that the proportionality requirement of paragraph (c) of this section is not satisfied.

(4) The agency's implementation policy must address the chain of command for mitigation decisions and must make clear that non-certified personnel, regardless of rank, may not direct mitigation actions that override the certified operator's professional judgment on whether the conditions for mitigation are present.

(5) An operator who declines to initiate mitigation based on a good-faith professional determination that the conditions for mitigation are not met may not be

subjected to adverse employment action for that decision.

(g) *Airspace awareness.* (1) For operations where known authorized manned or unmanned aviation is operating or anticipated in or near the area of operations, the agency's implementation policy or C-UAS Operations Plan must designate a person or position responsible for maintaining real-time awareness of known authorized aviation within the operational area and for ensuring that this information is communicated to personnel authorized to initiate mitigation actions before any mitigation is executed. For purposes of this paragraph, known authorized aviation means any manned or unmanned aircraft that has been identified in the C-UAS Operations Plan, communicated to the C-UAS team during the operation, or otherwise confirmed as lawfully operating in or near the area of operations. The designated person, or the individual filling the designated position, must have the ability to communicate directly with the mitigation operator. No mitigation action may be initiated without reasonable efforts to confirm that the target is not a known authorized aircraft.

(2) The scope and formality of this role must be commensurate with the complexity of the aviation environment. For operations with minimal or no known authorized aviation, this role may be performed as an additional duty by the certified operator or other command post personnel; for operations with significant aviation activity, the agency must designate a dedicated individual with airspace awareness and coordination responsibilities. When a target cannot be correlated with any known, authorized aircraft and meets the credible threat standard, mitigation may proceed.

§ 124.4 Authorized personnel, contractors, and mutual aid.

(a) *Officers and employees.* The authority provided by 6 U.S.C. 124n(a)(2) may be exercised only by SLTT law enforcement or correctional agency personnel. No SLTT law enforcement or correctional agency may delegate or transfer the exercise of C-UAS mitigation authority to any person or entity that is not an officer or employee of the

agency.

(b) *Prohibition on contractor exercise.* Contractors may provide technical support, system maintenance, and training assistance, but may not operate C-UAS mitigation systems, make credible threat determinations, or execute mitigation actions. An arrangement in which a contractor exercises de facto operational control of a C-UAS mitigation system during an operation, including an arrangement described as a turnkey, managed service, or operator-provided C-UAS service, constitutes an unauthorized delegation of authority and is grounds for suspension of accreditation or certification under § 124.5(i). Detection services that do not require the authority of the Act or the relief it provides from certain laws may be provided by contractors.

(c) *Mutual aid and regional C-UAS support.* (1) An SLTT law enforcement or correctional agency accredited under 6 U.S.C. 124n(d)(2) may provide C-UAS support to another SLTT law enforcement or correctional agency, including an agency that is not accredited under this part, under a mutual aid agreement, memorandum of understanding, request for assistance, task force arrangement, or other written arrangement authorized by applicable State, local, Tribal, or territorial law.

(2) When the requesting or host agency is not accredited under 6 U.S.C. 124n(d)(2), the accredited agency providing C-UAS support is the C-UAS operating agency for purposes of this part and is responsible for compliance with the applicable requirements of this part.

(3) Personnel of a non-accredited requesting or host agency may support the operation through ordinary law enforcement, correctional, public safety, evidence-handling, perimeter-security, ground-intercept, evacuation, traffic-control, or incident-command functions. Such personnel may not exercise C-UAS authority under 6 U.S.C. 124n(a)(2), operate systems whose operation requires the authority of or relief from certain laws under 6 U.S.C. 124n, make a credible-threat determination, or initiate any

mitigation action, unless those personnel independently satisfy the requirements of this part, hold the applicable certification under § 124.5, and are expressly designated in the accredited C-UAS operating agency's C-UAS Operations Plan to perform that function. Personnel so designated operate under that agency's implementation policy, Agency Approving Official approval, supervision, and compliance responsibility. An individual certification does not, by itself, authorize personnel to exercise 6 U.S.C. 124n(a)(2) authority, and this designation must be established in advance through the C-UAS Operations Plan and the mutual-aid arrangement under paragraph (c)(4) of this section.

(4) The written mutual aid arrangement must identify the requesting or host agency, the accredited agency providing C-UAS support, the legal basis for the accredited agency's personnel to operate in the host jurisdiction, the allocation of operational responsibilities, and the handling of C-UAS-derived information consistent with §§ 124.14 and 124.15.

(5) For multi-jurisdictional operations, the participating agencies must identify a lead C-UAS agency for tactical C-UAS coordination. The lead C-UAS agency must be an accredited agency unless the operation is conducted under Federal authority pursuant to § 124.19. A non-accredited requesting or host agency may serve as the lead public safety, law enforcement, correctional, or incident-command agency for the overall event or incident, but may not serve as the lead C-UAS agency unless accredited under this part.

(6) An accredited agency may enter into standing regional, county, statewide, or other multi-jurisdictional arrangements to provide recurring or on-call C-UAS support to non-accredited agencies. A standing arrangement does not itself authorize a mitigation operation; each mitigation operation remains subject to the applicable requirements of this part.

(7) Nothing in this part requires a small, rural, or otherwise resource-limited

SLTT law enforcement or correctional agency to acquire C-UAS equipment, obtain accreditation, or establish an independent C-UAS program in order to receive C-UAS support from an accredited agency.

(d) *Anti-circumvention.* (1) No SLTT law enforcement or correctional agency, officer, employee, contractor, vendor, or other person may structure or use a mutual aid, regional support, managed-service, technical-support, or other arrangement to evade the requirements of this part.

(2) Prohibited circumvention includes using an accredited agency as a nominal sponsor while a non-accredited agency, contractor, vendor, or other entity exercises de facto operational control of C-UAS activity requiring the authority of or relief from certain laws under 6 U.S.C. 124n; allowing personnel who lack the certifications required by § 124.5 to exercise C-UAS authority; using systems outside the requirements of § 124.7; avoiding the coordination, reporting, privacy, sensitive-information, or compliance requirements of this part; or acquiring third-party intercepted communications in a manner inconsistent with § 124.14(i).

(3) A mutual aid, regional support, statewide support, county support, or multi-jurisdictional C-UAS arrangement is not circumvention merely because the requesting or host agency is not accredited, provided that the C-UAS operating agency is accredited, the personnel exercising C-UAS authority hold the required certifications, and the operation is conducted in compliance with this part.

§ 124.5 Training and certification.

(a) *Training and certification structure.* This section establishes the training and certification structure implementing the requirements of 6 U.S.C. 124n(d)(2)(A). Detection and Warning Certification governs training for detection and warning operations under 6 U.S.C. 124n(b)(1)(A) and (B). Mitigation Certification governs training and certification for mitigation operations under 6 U.S.C. 124n(b)(1)(C), (D),

and (F). A current Detection and Warning Certification is a prerequisite both for initial enrollment in the mitigation training course and for mitigation recertification.

(b) *Agency implementation policy.* Before conducting any operations under this part, an SLTT law enforcement or correctional agency must adopt an agency implementation policy or detection and warning policy and complete the portal attestation in accordance with § 124.6, and must authorize each operation by a C-UAS Operations Plan in accordance with § 124.8, consistent with the other requirements and obligations of this part and applicable laws and policies.

(c) *Detection and Warning Certification.* The Attorney General, acting through the Director of the Federal Bureau of Investigation, will develop and maintain through the NCUTC an online training curriculum for detection and warning operations, accessible through a secure web-based training portal. The curriculum includes the confiscation authority of 6 U.S.C. 124n(b)(1)(E), evidence preservation, and chain of custody. Only those personnel who have completed the curriculum and passed the post-course assessment may exercise the authorities described in 6 U.S.C. 124n(b)(1)(A), (B), and (E). Upon successful completion, the NCUTC training portal automatically issues a Detection and Warning Certification. Detection and Warning Certification is issued only by the NCUTC, and detection and warning training or certification obtained from another agency or a private entity does not satisfy this requirement. Detection and warning activity conducted using systems that do not require the authority of 6 U.S.C. 124n is not subject to this requirement. Upon successful completion, the training portal records the individual's name, agency, date of completion, and certification status in the NCUTC certification database, which is the system of record for all certifications issued under this section. Each agency must maintain a roster of its certified personnel drawn from the NCUTC certification database and must verify the certification status of personnel assigned to C-UAS operations. Vendor-specific and system-level operator training is the

responsibility of each agency through its own training procedures and is not part of the detection and warning curriculum.

(d) *Mitigation training and certification.* (1) The Attorney General, acting through the Director of the Federal Bureau of Investigation, designates the NCUTC 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), as required by 6 U.S.C. 124n(d)(2)(A)(i). Only personnel who hold a valid Mitigation Certification may exercise these authorities. The NCUTC mitigation training program consists of the mitigation training course and such advanced and supplemental courses as the Attorney General, acting through the Director of the Federal Bureau of Investigation, approves. Each course is evaluated on a pass or fail basis and requires demonstrated proficiency in each mitigation technology category it covers; a person who does not demonstrate proficiency in each category does not pass that course. A person obtains Mitigation Certification by passing the mitigation training course and may extend the scope of that certification to additional mitigation technology categories by passing an advanced or supplemental course covering those additional categories. Failure to pass a particular advanced or supplemental course does not affect the scope of a certification already held.

(2) A person who holds a current Mitigation Certification under this paragraph (d) may conduct mitigation operations at a correctional facility. An abbreviated Correctional Mitigation Certification, limited to correctional-facility operations, is available for personnel who will operate only at correctional facilities.

(3) The mitigation training course under this paragraph is delivered at the NCUTC. The Attorney General, acting through the Director of the Federal Bureau of Investigation, may authorize the Federal Law Enforcement Training Centers or another qualified Federal training provider to deliver the mitigation training course at one or more additional sites, provided the NCUTC retains approval authority over curriculum and

standards, exercises oversight of the delivery, and issues all certifications upon verified completion. Any such authorization is at the sole discretion of the Attorney General, acting through the Director, confers no entitlement on any agency or training provider, and may be modified or withdrawn at any time.

(e) *Correctional mitigation training and certification*. The NCUTC offers an abbreviated Correctional Mitigation Certification for personnel who will conduct mitigation operations only at correctional facilities. The correctional course of instruction is shorter than the mitigation training course under paragraph (d) of this section because the fixed perimeter and persistent-threat environment of a correctional facility reduce the operational setup and mission-planning instruction required. The correctional course of instruction addresses the persistent-threat environment, perimeter operations, and the legal and safety considerations of correctional settings. A person who holds only the Correctional Mitigation Certification may conduct mitigation operations at a correctional facility but may not conduct other mitigation operations under this part. The NCUTC may arrange for the Federal Law Enforcement Training Centers or another qualified training provider to deliver the correctional curriculum, provided the NCUTC retains approval authority over curriculum and standards, exercises oversight of the delivery, and issues all certifications upon verified completion.

(f) *Training standards.* The mitigation training course, as administered by the NCUTC, will include instruction on the legal, operational, and technological aspects of C-UAS operations as required by section 8606(b)(1) of the SAFER SKIES Act, including FAA 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. The Attorney General, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Secretary of Transportation, and the Administrator of the Federal Aviation

Administration, will approve training program standards and may approve additional courses of instruction for specialized C-UAS operations. The mitigation training course must include scenario-based instruction on the application of the credible threat standard.

(g) *Eligible personnel.* Personnel eligible for Mitigation Certification or Detection and Warning Certification must have assigned duties that include the security or protection of people, facilities, or assets, as specified in 6 U.S.C. 124n(a)(2), and must be officers or employees of an SLTT law enforcement or correctional agency accredited by the Attorney General acting through the Director of the Federal Bureau of Investigation. The NCUTC, under the authority of the Attorney General, may establish additional attendance prerequisites.

(h) *Sufficiency of certification.* Successful completion of the applicable training requirement, combined with the use of systems within technology categories on the Authorized Technologies List and specific systems on the Authorized Systems List where populated, and compliance with the requirements of this part, satisfies the training and certification prerequisites of 6 U.S.C. 124n(d)(2)(A) for the exercise of the corresponding authorities under 6 U.S.C. 124n(a)(2).

(i) *Suspension.* The Attorney General, acting through the Director of the Federal Bureau of Investigation or the Director's designee, may suspend the Mitigation Certification or Detection and Warning Certification of any individual, or the accreditation of any SLTT law enforcement or correctional agency, for failure to comply with the requirements of this part, violation of the conditions of certification, or for any conduct that demonstrates unfitness to exercise C-UAS authority. Suspension of a certification or accreditation under this section is distinct from suspension of C-UAS authority by the Attorney General or the Secretary of Homeland Security under section 8605(f) of the SAFER SKIES Act, which is addressed in § 124.16. Neither a suspension of certification under this section nor an enforcement action against an individual under

section 8605(f) of the SAFER SKIES Act prevents or bars the responsible agency from taking any additional actions it deems necessary to address the circumstances that led to suspension or enforcement action by the Attorney General or designee.

(j) *Suspension notice.* A suspension will be communicated in writing and will specify the basis for the action and any available remedial steps. The suspension notice must include the factual basis for the action in sufficient detail to enable the affected individual or agency to respond. In exigent circumstances, the Director of the Federal Bureau of Investigation or the Director's designee may immediately suspend a certification or accreditation pending administrative review without the requisite written notice when continued exercise of C-UAS authority poses a risk to aviation safety, public safety, or national security. In such cases, the Director or the Director's designee must provide the requisite notice within 3 days of the suspension.

(k) *Administrative review.* An individual or agency that receives a suspension notice may request administrative review within 30 calendar days of receipt. The Attorney General, acting through the Director of the Federal Bureau of Investigation, will designate a reviewing official of the Department of Justice who did not participate in or supervise the initial decision. The affected party may submit documentary evidence and written witness statements in support of its response. The reviewing official will consider the written submissions of both parties, may conduct an informal hearing at the reviewing official's discretion, and will issue a written determination within 60 calendar days of receipt of the request, stating the factual findings and the basis for the determination. The reviewing official may affirm the action, modify its terms, impose conditions for reinstatement, or reverse the action. A suspension that is affirmed remains in effect until reinstatement under paragraph (m) of this section or the expiration of the suspended certification or accreditation, whichever occurs first.

(l) *Conditions.* The Attorney General, acting through the Director of the Federal

Bureau of Investigation, may issue a certification or accreditation subject to conditions, and may modify the conditions of a certification or accreditation, consistent with the standards and procedures applicable to suspension under this section.

(m) *Reinstatement.* An individual or agency whose certification or accreditation has been suspended may apply for reinstatement after completing the remedial steps specified in the suspension notice or the reviewing official's determination. An individual Mitigation Certification may alternatively be reinstated upon the successful recompletion of the full mitigation training course.

(n) *Transition for previously trained personnel.* Personnel holding a Mitigation Certification issued by the NCUTC before the effective date of this part must complete the detection and warning curriculum under paragraph (c) of this section by September 29, 2026. During that period, the Mitigation Certification remains valid, and the Detection and Warning Certification prerequisite for Mitigation Certification is deemed satisfied. An agency's accreditation is not affected while its personnel complete the curriculum during the transition period.

§ 124.6 Agency implementation policy.

(a) *Requirement.* Before conducting any operations under this part, each SLTT law enforcement or correctional agency must adopt and maintain an agency implementation policy governing the exercise of authority under 6 U.S.C. 124n(a)(2). The agency implementation policy is comprehensive. It governs all operations the agency conducts under this part, including detection and warning operations, and it addresses the detection and warning matters listed in paragraph (g) of this section. An agency that adopts and maintains an agency implementation policy under this paragraph is not required to adopt a separate policy under paragraph (g) of this section. An agency that conducts only detection and warning operations may instead adopt the abbreviated policy under paragraph (g) of this section. The agency implementation policy must, at a

minimum:

(1) Designate an Agency Approving Official meeting the requirements of § 124.2;

(2) Designate the personnel authorized to exercise C-UAS authority and describe the recurrent training requirements applicable to such personnel;

(3) Establish procedures consistent with § 124.14 for the handling, retention, and dissemination of data acquired during C-UAS operations, including written anonymization standards specifying the aggregation thresholds, identifier suppression, and re-identification risk assessment used to qualify a data product as pattern data;

(4) Include provisions for public notification regarding the potential use of C-UAS authority within the agency's jurisdiction;

(5) Ensure compliance with the requirements of this part; and

(6) Detail standing tactical procedures governing the execution of C-UAS operations, including engagement protocols that account for the risk to persons and property on the surface and in the air before engagement, escalation procedures, use of force considerations, ground intercept team procedures, render safe procedures, evidence collection and chain-of-custody procedures, communications procedures, system operating procedures, data handling and purge procedures consistent with the retention requirements of this part, operation plan requirements, and post-operation procedures that incorporate data purge verification.

(b) *Legal counsel review.* The implementation policy must be reviewed and concurred in by the agency's legal counsel before adoption and upon each annual renewal. The review must specifically address the privacy and civil liberties requirements of this part, including the data retention, minimization, and dissemination provisions, and the interplay of proposed C-UAS operations and implementing policies with applicable State, local, Tribal, or territorial law. For an agency that has a designated official responsible for the agency's privacy and civil liberties compliance, regardless of

title, the implementation policy must also be reviewed by that official.

(c) *Alternative certification for agencies without in-house counsel.* For an agency without in-house counsel, the review required by paragraph (b) of this section may alternatively be satisfied by review and certification by a State, local, territorial, or Tribal attorney's office that the implementation policy addresses each element required by paragraph (a) of this section. An agency obtaining a certification under this paragraph (c) must document the basis for using this paragraph (c). Certification pursuant to this paragraph (c) does not relieve the agency of any compliance obligation under this part.

(d) *Portal attestation.* Upon adoption of the implementation policy, the agency head or designee must certify compliance through the Federal C-UAS coordination portal by attesting that the agency has adopted an implementation policy addressing each element required by paragraph (a) of this section. The portal records the certifying official, agency, and date of attestation. The implementation policy is not subject to pre-approval by the NCUTC. The NCUTC retains authority to audit implementation policies and to suspend certification or accreditation under § 124.5. The attestation must be renewed annually.

(e) *Retention and availability.* The agency must retain the implementation policy and make it available to the Attorney General or the Secretary of Homeland Security, or their designee, upon request, including during compliance audits under § 124.16.

(f) *Operating without attestation.* An agency that conducts operations under this part without a current portal attestation is in violation of this part, and the absence of an attestation constitutes grounds for compliance action under § 124.16.

(g) *Detection and warning policy.* An SLTT law enforcement or correctional agency that conducts only detection and warning operations requiring the authority of, or the relief from certain laws provided by, 6 U.S.C. 124n may adopt a detection and warning policy in lieu of the implementation policy required by paragraph (a) of this

section. A detection and warning policy must satisfy the requirements of this section, except that it need not include the standing tactical procedures of paragraph (a)(6) of this section. The agency must designate an Agency Approving Official under paragraph (a)(1) of this section and complete the portal attestation under paragraph (d) of this section, which must be renewed annually. For purposes of that attestation, a detection and warning policy need address only the elements of paragraph (a) of this section that apply to detection and warning operations.

§ 124.7 Authorized technologies.

(a) *Two-list authorization framework.* The technology authorization framework consists of two complementary lists. 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. Both lists are maintained jointly by the Department of Justice, the Department of Homeland Security, the Department of Defense, the Department of Transportation and Federal Aviation Administration, the Federal Communications Commission, and the National Telecommunications and Information Administration, consistent with 6 U.S.C. 124n(d)(2)(A)(iii) and section 8606(a)(4) of the SAFER SKIES Act.

(b) *General requirement.* An SLTT law enforcement or correctional agency exercising authority under 6 U.S.C. 124n(a)(2) may deploy only systems within technology categories listed on the Authorized Technologies List. When the Authorized Systems List has been populated for a given technology category, the agency may deploy only specific systems listed on the Authorized Systems List within that category, subject to the advance coordination requirements of § 124.9. For technology categories on the Authorized Technologies List for which the Authorized Systems List has not yet been

populated, the agency may deploy specific systems within those categories provided that an operator holds Mitigation Certification covering that technology category and has completed manufacturer or vendor training on the specific system to be deployed, subject to the advance coordination requirements of § 124.9.

(c) *Scope of the list requirement.* When operating under the authorities or statutory reliefs in 6 U.S.C. 124n(a)(2), SLTT law enforcement or correctional agencies may employ only listed technology categories, and, where the Authorized Systems List is populated, listed systems. Technology that an SLTT law enforcement or correctional agency may lawfully employ without the authorities or reliefs provided by 6 U.S.C. 124n(a)(2) is not subject to the requirements of this section and remains available to agencies on the same basis as before the SAFER SKIES Act. The detection and warning training curriculum will address the distinction between technology categories subject to and not subject to this section.

(d) *Mitigation technology and training alignment.* An SLTT law enforcement or correctional agency may employ mitigation systems only in those technology categories covered by the NCUTC mitigation courses completed by its mitigation-certified personnel. NCUTC may create an additional mitigation module covering the technology category when a new technology category is added to the Authorized Technologies List. Mitigation-certified personnel who completed the NCUTC mitigation course prior to the addition of this new content must successfully complete additional NCUTC training on the new technology category prior to using any system on the Authorized Systems List under that category.

(e) *Scope of interception authority.* Systems may be used to intercept communications to or from an unmanned aircraft or UAS only to the extent necessary to support an action described in 6 U.S.C. 124n(b)(1). Any interception, acquisition, maintenance, use of, or access to communications to or from an unmanned aircraft or

UAS under this section must be conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law.

(f) *Maintenance of the lists.* The Authorized Technologies List and Authorized Systems List, including the criteria and procedures for evaluating, listing, renewing, suspending, and removing technology categories and systems, are established and maintained through the interagency process described in 6 U.S.C. 124n(d)(2)(A)(iii) and section 8606(a)(4) of the SAFER SKIES Act. The Authorized Systems List is updated by that interagency process and published on the designated interagency C-UAS portal. Each RF-emitting system listed on the Authorized Systems List will have completed a system-level spectrum evaluation through the interagency process before listing, addressing potential interference with non-Federal spectrum users, compatibility with Federal spectrum users, and potential interference with aviation safety systems. System-level evaluations are reviewed and renewed at intervals determined through the interagency process and upon any system change to its operating capabilities, functions, radio frequency characteristics, or power levels that may alter its radio frequency characteristics, capabilities, functions, or assessed configurations. Minor updates that do not alter a system's performance, capabilities, functions, radio frequency characteristics, or assessed configurations do not require renewed evaluation.

(g) *Emergency suspension.* Upon receipt of an emergency suspension notice issued through the interagency process for the Authorized Technologies List and Authorized Systems List, an SLTT law enforcement or correctional agency must immediately cease deployment of the affected system or technology category. Grounds for emergency suspension include discovery of a critical safety defect, identification of a supply chain compromise or cybersecurity vulnerability, a determination that a system's radio frequency characteristics differ materially from those evaluated during spectrum

evaluation, or a finding by any agency participating in the interagency process that continued deployment poses an unacceptable risk. The SLTT law enforcement or correctional agency may not resume deployment of the affected system or technology category until the suspension is lifted or the system or category is restored to the applicable list, and the agency must comply with any conditions attached to the lifting of the suspension or the restoration of the system or category to the applicable list.

§ 124.8 C-UAS Operations Plan.

(a) *Requirement and function.* Each mitigation operation, and each detection and warning operation conducted under this part using systems that require the authority of, or relief from certain laws under, 6 U.S.C. 124n, must be authorized by a C-UAS Operations Plan signed by the agency's Agency Approving Official. Section 124.12 sets out the conditions specific to detection and warning operations. The signed C-UAS Operations Plan is the instrument authorizing the operation on behalf of the SLTT law enforcement or correctional agency and certifies that the operation is consistent with the agency's implementation or detection and warning policy, that the operators are agency personnel who hold the required training and certification, and that the risk-based assessment factors of paragraph (e) of this section have been addressed. The agency may not commence mitigation operations until both the advance coordination process under § 124.9 and the signed C-UAS Operations Plan are complete.

(b) *Legal counsel certification.* The C-UAS Operations Plan must include a certification by the agency's legal counsel or, for an agency without in-house counsel, the applicable prosecuting authority, that the plan has been reviewed for legal sufficiency. The certification may take the form of a signature block, stamp, or attestation on the plan.

(c) *Form.* The C-UAS Operations Plan must be prepared on the standardized form prescribed by the Attorney General. The form is structured to use short-answer fields, selection-based fields, and map or diagram attachments, and does not require

narrative legal analysis or repetition of standing procedures addressed in the agency's implementation policy. The form may use conditional fields keyed to the type of operation, so that each operation completes only the fields applicable to it; for a detection and warning operation, the fields specific to mitigation, such as mitigation-system parameters and render safe planning, do not apply.

(d) *Content.* The C-UAS Operations Plan must address, at a minimum and to the extent applicable to the operation:

(1) Operation identification, including the submitting agency, points of contact, the Agency Approving Official, the operation type, planned dates, geographic location, venue type, any Special Event Assessment Rating or National Special Security Event designation, and the identification of any mutual aid agencies;

(2) Systems and airspace, including the systems to be deployed by reference to the Authorized Systems List or Authorized Technologies List category; a description of each system's configuration and the hardware version, firmware revision, and software version of each system as deployed; RF-emitting system parameters; class of airspace; and anticipated flight restrictions;

(3) Coordination confirmation, including operator certification status, compliance with the agency implementation policy, the legal counsel certification, and compliance with the privacy and civil liberties requirements of this part; and

(4) Operational planning elements, including deployment configuration and spectrum deconfliction, personnel and team assignments, render safe and contingency planning, known authorized manned and unmanned aviation and deconfliction processes and procedures, communications, investigative response and data handling, and demobilization.

(e) *Risk-based assessment.* The C-UAS Operations Plan must address the following factors: potential impacts to aviation safety, civilian aviation and aerospace

operations, aircraft airworthiness, or the use of the airspace; procedures to comply with any technical and siting limitations; options for mitigating identified potential impacts; potential consequences if potential impacts are not mitigated; the ability to provide reasonable advance notice to aircraft operators of both manned and unmanned aircraft; the setting and character of the facility or asset; for National Special Security Events and Special Event Assessment Rating events, the event characteristics; and the potential consequences to public safety if UAS threats are not mitigated. For National Special Security Events and Special Event Assessment Rating events, a plan that identifies the systems, airspace environment, and coordination elements from which the assessment can be derived satisfies this paragraph without separately addressing each factor in narrative form. Nothing in this part may be interpreted as limiting the authority of the Administrator of the Federal Aviation Administration to manage the navigable airspace, assess potential aviation safety risks, and implement such mitigations as the Administrator determines appropriate.

(f) *Timing and submission.* The C-UAS Operations Plan must be completed before the commencement of operations and submitted to the Federal Bureau of Investigation and Department of Homeland Security through the designated Federal C-UAS coordination portal as a supplement to the advance notification not fewer than 7 calendar days before the commencement of operations, or as early as practicable when the applicable notification timeline does not permit 7 calendar days. For a detection and warning operation that is not subject to the advance notification requirement of § 124.9, the C-UAS Operations Plan must be submitted through the designated Federal C-UAS coordination portal before the commencement of operations, for situational awareness and recordkeeping; such submission is not an advance notification under § 124.9 and does not trigger Federal Aviation Administration or Federal Communications Commission coordination. The plan may be updated after submission to reflect changes

resulting from Federal Aviation Administration or Federal Communications Commission coordination. Material updates must be resubmitted promptly. Federal Aviation Administration and Federal Communications Commission coordination is valid for the system configuration and the firmware and software version coordinated for the operation. A change in configuration, firmware, or software version does not require re-coordination if it does not materially change the system's radio frequency emission characteristics, its operating frequencies and power levels, or other factors potentially impacting aviation safety from those previously coordinated. A change that would operate outside the frequencies or power levels coordinated for the operation requires re-coordination before deployment; a summary of the change must be provided to the Federal Aviation Administration and Federal Communications Commission to determine if re-coordination is necessary. The Federal Aviation Administration and the Federal Communications Commission may identify by guidance categories of configuration, firmware, or software changes that are deemed to materially affect radio frequency emission characteristics and require re-coordination. Federal review of the C-UAS Operations Plan is for deconfliction and situational awareness purposes and does not constitute approval or disapproval of the operation. For an event, area, or period in which a high volume of simultaneous operations is anticipated, the Federal Bureau of Investigation, in coordination with the Federal Aviation Administration, may establish an earlier submission deadline for affected operations and will communicate that deadline to affected agencies in advance through the designated portal or the lead C-UAS agency.

(g) *Relationship to implementation policy.* The C-UAS Operations Plan is an event-specific or operation-specific document. Standing tactical procedures required by § 124.6(a) must be addressed in the agency's implementation policy, and the C-UAS Operations Plan must reference the implementation policy by title and version rather than repeating standing procedures.

(h) *Operational windows.* (1) An individual C-UAS Operations Plan may authorize operations for a period not to exceed 30 consecutive calendar days, except as provided in paragraph (h)(2) of this section. For operations requiring a longer duration, the agency must submit a renewal plan before the expiration of the current operational window; the renewal plan may incorporate the prior plan by reference and address only material changes. The agency must submit a renewal plan, through the designated Federal C-UAS coordination portal under § 124.8(f), before the expiration of the current operational window.

(2) For fixed-site facilities for which SLTT law enforcement and correctional agencies conduct ongoing persistent-protection operations, including correctional facilities, critical infrastructure sites, other permanent facilities with a continuing C-UAS mission, and venues where the agency expects to provide recurring C-UAS coverage within the authorization period, the Agency Approving Official may authorize a standing operational window of up to 365 calendar days, renewable upon submission of a renewal plan. The advance notification for a standing operational window must specify the venue and anticipated events or coverage periods; for a detection and warning operation not subject to the advance notification requirement of § 124.9, the C-UAS Operations Plan must specify the venue, the area covered, which may be stated as a radius around the site, and the anticipated coverage periods. Material changes, including a new event, new systems, or a changed threat environment, require an update to the advance notification under § 124.9(a) or, for such a detection and warning operation, an updated C-UAS Operations Plan. Federal coordination requirements continue to apply to each event within a standing window, including lead C-UAS agency coordination under § 124.10 and per-event coordination among the Department of Transportation, the Federal Aviation Administration, and the Federal Communications Commission.

(3) No C-UAS Operations Plan may authorize an indefinite or open-ended

operational window.

§ 124.9 Advance coordination, notification, and authorization.

(a) *Advance notification.* (1) Before conducting any mitigation operation under 6 U.S.C. 124n(a)(2), an SLTT law enforcement or correctional agency must submit an advance notification through the designated Federal C-UAS coordination portal not fewer than 30 calendar days before the commencement of the operational period. When 30 calendar days is not feasible, the agency must submit the advance notification as early as the circumstances permit, with sufficient lead time to allow the Federal Bureau of Investigation, the Department of Homeland Security, the Department of Transportation, the Federal Aviation Administration, and the Federal Communications Commission to complete their respective reviews, and must include a brief explanation of the circumstances that prevented submission within the 30-day standard.

(2) The advance notification is a coordination document that routes the relevant data elements to each recipient agency through a single submission. The advance notification is not a request for approval by the Department of Justice or the Department of Homeland Security, and the absence of a response from the Department of Justice or the Department of Homeland Security does not affect the agency's authority to proceed.

(3) The advance notification must identify the submitting SLTT law enforcement or correctional agency, the planned dates and geographic location of the operation, the systems to be deployed by reference to the Authorized Systems List or Authorized Technologies List category, RF-emitting system parameters, a characterization of the airspace and operational environment, and confirmation of operator certification status and compliance with the agency implementation policy and the privacy requirements of this part.

(b) *C-UAS Operations Plan.* Each mitigation operation must also be authorized by a C-UAS Operations Plan in accordance with § 124.8. The agency may not

commence mitigation operations until both the advance coordination process under this section and the signed C-UAS Operations Plan are complete. The SLTT law enforcement or correctional agency must also submit a comparable advance notification to the State if required by State law or policy.

(c) *FBI and DHS notification and routing.* The Attorney General, through the Federal Bureau of Investigation and the Department of Homeland Security, receives the advance notification for purposes of deconflicting planned SLTT law enforcement or correctional agency C-UAS operations with any ongoing or planned Federal C-UAS, law enforcement, or national security operations. Until the portal is fully established, an SLTT law enforcement or correctional agency must notify the Federal Bureau of Investigation and Department of Homeland Security through a channel designated by the Federal Bureau of Investigation and Department of Homeland Security for that purpose.

(d) *DOT/FAA coordination.* Before conducting any mitigation operation, an SLTT law enforcement or correctional agency must coordinate with the Department of Transportation and the Federal Aviation Administration through the coordination mechanism the Federal Aviation Administration has designated. The agency must provide the systems to be deployed, the geographic coordinates of each proposed deployment and enforcement location, the expected duration of the operation, and a characterization of the airspace environment. The Administrator of the Federal Aviation Administration may establish such flight restrictions as the Administrator determines necessary in his sole discretion for reasons of aviation safety. The absence of a formal flight restriction does not preclude mitigation action in exigent circumstances when a credible threat exists and the requirements of this part are otherwise satisfied.

(e) *Categorical FAA determinations.* The Federal Aviation Administration may issue categorical determinations for specific combinations of authorized technologies, geographic locations, and airspace environments. When a proposed mitigation operation

falls within the parameters of a categorical determination by the Federal Aviation Administration, individual case-by-case Federal Aviation Administration coordination is not required, provided the agency operates within the conditions specified in the determination and notifies the Federal Aviation Administration through the Federal Aviation Administration-designated coordination mechanism.

(f) *FCC authorization.* Before deploying any C-UAS system (whether detection and warning only or mitigation) that involves the emission of radio waves, an SLTT law enforcement or correctional agency must obtain authorization to use that system consistent with Title III of the Communications Act of 1934, as amended. The system must comply with any relevant regulations, policies, and guidance administered by the Federal Communications Commission, and an SLTT law enforcement or correctional agency must submit a request to the Federal Communications Commission through the advance notification process and as directed by the Federal Communications Commission. The Federal Communications Commission will also issue waivers, as appropriate, to C-UAS equipment vendors and manufacturers to allow them to import and sell C-UAS mitigation equipment that employs radio frequency interdiction technologies or electronic counter measures to authorized SLTT law enforcement and correctional agencies.

(g) *Emergency exception.* When a credible threat poses an imminent risk to human life and advance coordination under this section is not practicable, an SLTT law enforcement or correctional agency may take mitigation action. The agency must complete the notifications required by this section as soon as practicable, and in any event within two hours of the action. If the mitigation action involves an RF-emitting C-UAS system, the agency must additionally comply with the real-time notification requirements of § 124.11. Each invocation of this exception must be documented in the post-operation report with a specific explanation of why advance coordination was not

feasible. This exception may not be invoked as a routine alternative to advance coordination, and a pattern of repeated invocations may result in compliance review under § 124.16, accreditation or certification suspension, and penalties under section 8605(f) of the SAFER SKIES Act. The compliance audit program will establish the criteria for identifying patterns of emergency invocations that warrant review.

(h) *Federal coordination.* Before conducting any operation under this part within a security or protection mission overseen by a Federal Government entity, or within an area, facility, waterway, or other area over which a Federal Government entity exercises a security or protection responsibility, the agency must coordinate with that Federal Government entity through the advance coordination process under § 124.9 before conducting the operation. The Federal Aviation Administration's general regulatory authority over the navigable airspace does not by itself trigger this requirement; airspace safety coordination is addressed in § 124.8 and § 124.11.

(i) *Detection and warning operations.* Detection and warning operations that do not actively transmit radio frequency energy and do not affect aviation safety are not subject to the advance coordination requirements of this section.

§ 124.10 Interagency and lead-agency coordination.

(a) *Early coordination and notice of intent.* For operations in support of National Special Security Events, events rated Special Event Assessment Rating 1 through 3, or other events where Federal C-UAS operations are anticipated, an SLTT law enforcement or correctional agency should notify the local FBI field office of its intent to provide C-UAS coverage as early as practicable and before the 30-day advance notification standard of § 124.9. The designated Federal C-UAS coordination portal includes a notice-of-intent function that allows an agency to register its intent to cover a future event without completing the full advance notification. A notice of intent is informational only and does not trigger the advance coordination process, the Federal Aviation Administration or

Federal Communications Commission review, or any timeline obligation.

(b) *Special event coordination.* When the Federal Bureau of Investigation receives an SLTT law enforcement or correctional agency advance notification or notice of intent for an event at which Federal C-UAS operations are also planned or under consideration, the Federal Bureau of Investigation will present the notification to the interagency C-UAS coordination process maintained by the Department of Justice and the Department of Homeland Security, will serve as the conduit for SLTT law enforcement and correctional agency equities in that process, and will communicate the results to the SLTT law enforcement or correctional agency, including any Federal operational parameters or deconfliction requirements that may affect the SLTT law enforcement or correctional agency C-UAS operation. The interagency coordination process does not approve or disapprove SLTT law enforcement or correctional agency C-UAS operations.

(c) *Tactical coordination under a lead C-UAS agency.* An SLTT law enforcement or correctional agency conducting C-UAS operations at an event or location for which a lead C-UAS agency has been designated must operate under the tactical coordination of the lead C-UAS agency for the duration of the event. Tactical coordination includes the assignment of system deployment locations, operating frequencies, detection and mitigation sectors, ground intercept team sectors, render safe locations, communications channels, and risk to persons and property on the surface or in the air. The SLTT law enforcement or correctional agency's C-UAS Operations Plan for the event must be developed in coordination with the lead C-UAS agency and must conform to the lead agency's overall C-UAS operational framework for the event. An SLTT law enforcement or correctional agency coordinating with a lead C-UAS agency acts under its own certified authority under 6 U.S.C. 124n(a)(2); tactical coordination merely integrates the SLTT law enforcement or correctional agency C-UAS operation

into a unified C-UAS posture. Where geographic responsibilities are divided among multiple Federal agencies, the SLTT law enforcement or correctional agency must coordinate with the sector-level lead Federal agency responsible for the geographic area in which the SLTT law enforcement or correctional agency intends to operate. Whenever Federal and SLTT operations will be conducted at the same event, or whenever the Federal and SLTT operations will overlap in geographic area and time, the Federal agency will be the lead C-UAS agency. An SLTT law enforcement or correctional agency may serve as the lead C-UAS agency only where multiple SLTT agencies are operating in the same area and no Federal agency is involved.

(d) *Coordination required.* An SLTT law enforcement or correctional agency that does not accept tactical coordination by the designated lead C-UAS agency may not conduct C-UAS operations, including detection and warning operations using systems requiring the authority of and relief from certain laws under the Act, within the geographic area and time period covered by the lead-agency designation.

(e) *Overlapping SLTT operations.* When the Federal Bureau of Investigation and Department of Homeland Security receive advance notifications from two or more SLTT law enforcement or correctional agencies for C-UAS operations that overlap in geographic area and time, the Federal Bureau of Investigation and Department of Homeland Security will notify all affected SLTT law enforcement and correctional agencies of the overlap. The affected agencies must designate a lead C-UAS agency for the overlapping area and time period, or establish a joint operational coordination arrangement, before any agency commences mitigation operations in the overlapping area. The designation or arrangement must be documented and provided to the Federal Bureau of Investigation and Department of Homeland Security. If the agencies cannot reach agreement within 48 hours of the Federal Bureau of Investigation and Department of Homeland Security's notification, the Federal Bureau of Investigation and Department

of Homeland Security may designate operational parameters for the overlapping area, including frequency deconfliction assignments and geographic boundaries for each agency's mitigation operations.

(f) *Deconfliction direction.* If the deconfliction process identifies a conflict between a planned SLTT law enforcement or correctional agency C-UAS operation and an ongoing or planned Federal C-UAS, law enforcement, or national security operation that cannot be resolved through coordination, the Department of Justice, acting through the Federal Bureau of Investigation and in coordination with the Department of Homeland Security, may direct the SLTT law enforcement or correctional agency to modify the operational parameters of, or postpone, the planned operation until the conflict is resolved.

(g) *Emergency exception preserved.* This section does not affect an SLTT agency's authority to respond to an imminent risk to human life under § 124.9(g), including at an event with a designated lead C-UAS agency; however, the agency must notify the lead C-UAS agency immediately upon taking emergency action and must coordinate with the lead agency as soon as practicable thereafter.

(h) The requirements in paragraphs (a) through (g) of this section are established under the Attorney General's oversight authority pursuant to 6 U.S.C. 124n(d)(1) and the coordination obligations of 6 U.S.C. 124n(b)(4) and (d)(3); they do not transfer or diminish the SLTT agency's statutory authority and relief from certain laws under 6 U.S.C. 124n(a)(2).

§ 124.11 Real-time air traffic control notification.

(a) *Notification required.* Any SLTT law enforcement or correctional agency, or its personnel, that activates a C-UAS system for mitigation purposes must, within five minutes of activation or as soon as operationally practicable, provide verbal or electronic notification to the notification point designated by the Federal Aviation Administration

for real-time C-UAS coordination, using the procedures established under paragraph (b) of this section. Detection and warning operations do not require notification or coordination under this section.

(b) *Notification procedures.* An SLTT law enforcement or correctional agency must comply with the notification and reporting procedures jointly established by the Department of Homeland Security, the Department of Justice, and the Federal Aviation Administration for real-time communication to air traffic control of C-UAS mitigation actions using a radio frequency-emitting C-UAS system. The notification must identify the type of C-UAS action, the time of activation, and the location. The NCUTC will include training on these notification procedures in the mitigation training course.

(c) *Notification upon termination.* Upon termination of the mitigation action, the SLTT law enforcement or correctional agency must provide a follow-up notification to the designated Federal Aviation Administration notification point confirming the time of termination.

(d) *Non-RF mitigation.* Mitigation actions that do not involve radio frequency-emitting systems do require notification under this section unless the Department of Transportation or Federal Aviation Administration's applicable notification procedures established under this section provide otherwise. Such actions remain subject to the advance coordination and post-operation reporting requirements of §§ 124.9 and 124.13.

§ 124.12 Detection and warning operations.

(a) *Scope.* This section governs detection and warning operations using systems whose operation requires the authority of and relief from certain laws under 6 U.S.C. 124n(a)(2). Detection and warning activity conducted using systems that do not require the authority of the Act or the relief it provides from certain laws is not subject to this part.

(b) *Conditions.* An SLTT law enforcement or correctional agency may conduct

detection and warning operations under this section if:

(1) All personnel conducting detection and warning operations hold a current Detection and Warning Certification;

(2) The agency deploys only systems within technology categories listed on the Authorized Technologies List and, where populated, specific systems listed on the Authorized Systems List;

(3) The agency has adopted an implementation policy under § 124.6(a) or a detection and warning policy under § 124.6(g), has completed the applicable portal attestation, and has authorized the operation by a C-UAS Operations Plan under § 124.8; and

(4) The agency complies with the privacy, data handling, and retention requirements of § 124.14.

(c) *Coordination.* No per-operation (that is, for each individual deployment or activation of a C-UAS system) advance notification, Federal Aviation Administration coordination, or Federal Communications Commission coordination is required for detection and warning operations that employ only systems that do not emit radio frequency energy and do not affect aviation safety. Such operations must be authorized by a C-UAS Operations Plan under § 124.8, which documents operational authority, data handling and retention, and legal review. For detection and warning operations involving RF-emitting systems, such as active warning broadcast systems, the advance coordination requirements of § 124.9 apply, and the operation must be authorized by a C-UAS Operations Plan under § 124.8.

(d) *Reporting.* The 48-hour reporting requirement of § 124.13 does not require per-event reporting of detection and warning operations. Each SLTT law enforcement or correctional agency conducting detection and warning operations under this section must report detection activity in the semiannual operational summary required by § 124.13,

including the detection systems deployed by Authorized Technologies List category, the locations at which systems were deployed, the total number of detection events recorded, instances of retention of records of communication beyond 180 days, and any data-sharing arrangements. A physical seizure or confiscation under 6 U.S.C. 124n(b)(1)(E) that results from a detection and warning operation is a 6 U.S.C. 124n action, but it is documented through the agency's normal evidence-handling procedures and is not separately reported under this part. The recovery of a crashed or abandoned unmanned aircraft that does not involve the use of 6 U.S.C. 124n authority is not a 6 U.S.C. 124n confiscation and is not subject to the reporting requirements of this part.

(e) *Prohibition on mitigation.* Personnel holding only a Detection and Warning Certification are not authorized to take any mitigation action or any other action that affects an unmanned aircraft in flight, regardless of the operator's ultimate objective. If a detection operation identifies a credible threat requiring mitigation, this rule requires that the agency respond through mitigation-certified personnel operating under §§ 124.8 and 124.9 or through coordination with Federal C-UAS assets. This prohibition is absolute and is not subject to the emergency exception of § 124.9(g), which is available only to an agency with mitigation-certified personnel and authorized mitigation capability.

§ 124.13 Post-operation reporting.

(a) *Report required.* Any SLTT law enforcement or correctional agency exercising authority under 6 U.S.C. 124n(a)(2) must submit a post-operation report as required by 6 U.S.C. 124n(d)(2)(C)(i) within 48 hours of whichever occurs first:

(1) Taking any mitigation action described in 6 U.S.C. 124n(b)(1)(C), (D), or (F);

(2) Any confiscation of an unmanned aircraft or UAS under 6 U.S.C. 124n(b)(1)(E); or

(3) The conclusion of an operation where notification was provided.

(b) *Other confiscations*. A confiscation that does not occur pursuant to 6 U.S.C.

124n(b)(1)(E) may be documented through the agency's normal evidence-handling procedures and does not need to be separately reported under this part.

(c) *Content.* The post-operation report must contain:

(1) Confirmation whether the planned operation did or did not occur as notified;

(2) The date, time, and geographic location of the reportable action;

(3) A brief description of the credible threat that a UAS or unmanned aircraft posed to the safety or security of people, a facility, or an asset; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; or a correctional facility necessitating the action;

(4) The type of capability employed, including the specific system or systems used by reference to the Authorized Systems List and Authorized Technologies List category, or where the Authorized Systems List had not yet been populated for a particular Authorized Technologies List category at the time of the action, the Authorized Technologies List category; and in all cases the make, model, hardware version, firmware revision, and software version of the system or systems as deployed;

(5) Any known operational effects, including the seizure, disabling, damage, or destruction of a UAS or unmanned aircraft; any reported effects on other aviation systems, spectrum users, or persons and property on the surface or in the air; any aviation accident; whether a temporary flight restriction was granted or denied; and any other harm, damage, or loss to a person or to private property;

(6) Any issues, anomalies, or deviations encountered during the operation; and

(7) Summary operational statistics, including the number of UAS detected, counted as confirmed detections attributable to a distinct unmanned aircraft and reported in good faith with reasonable deduplication; warnings issued; mitigation actions taken; UAS or unmanned aircraft seized or confiscated; and any criminal charges, citations, regulatory enforcement actions, or arrests resulting from the operation.

(d) *Submission mechanism.* Reports must be submitted through the designated Federal C-UAS coordination portal. Submission through the portal satisfies the notification requirement to both the Attorney General and the Secretary of Homeland Security, as the portal routes reports to the Federal Bureau of Investigation and Department of Homeland Security automatically.

(e) *Immediate notification for unintended consequences.* If a detection, warning, or mitigation action results in unintended consequences, including interference with manned aviation or lawfully operating UAS, property damage, injury, or system malfunction affecting third parties, the SLTT law enforcement or correctional agency must immediately notify the Federal Bureau of Investigation and Department of Homeland Security by the most expedient means available, in addition to the 48-hour post-operation report. The Federal Bureau of Investigation will notify the Office of the Deputy Attorney General, the Department of Transportation, the Federal Aviation Administration, the Federal Communications Commission, and other affected agencies as appropriate.

(f) *Consolidated reporting.* Where multiple reportable events occur within a 48 hour period, an SLTT law enforcement or correctional agency may submit a single consolidated post-operation report covering all actions taken during the period, due within 48 hours of the first reportable event, provided that each action is documented with the data elements required by paragraph (c) of this section and that any action resulting in unintended consequences is reported immediately under paragraph (e) of this section.

(g) *Recurring venue reporting.* For recurring venue operations conducted under a standing operational window authorized by § 124.8(h), each discrete event within the authorization period must be reported separately.

(h) *Semiannual operational summary.* Each SLTT law enforcement or

correctional agency exercising authority under this part must submit a semiannual operational summary through the designated Federal C-UAS coordination portal, covering total operations conducted, mitigation actions taken, detection activity, instances of retention of records of communication beyond 180 days, instances in which control communications were disclosed outside the originating agency organized by the legal basis for their disclosure, compliance issues identified, and lessons learned. The summary must also report the requests the agency received for C-UAS protection from critical infrastructure or airport owners or operators that are not SLTT law enforcement or correctional agencies, the number of those requests to which it provided protection, and the number it was unable to support as well as the reasons it was unable to provide support.

(i) *Reporting to support congressional and oversight requirements.* The Federal Bureau of Investigation will compile information from post-operation reports and semiannual summaries to support the biannual report required by 6 U.S.C. 124n(d)(2)(D) and the semiannual briefings required by 6 U.S.C. 124n(g), in coordination with the Secretary of Homeland Security and the Secretary of Transportation. The compilation will include:

(1) The frequency, location, and circumstances of SLTT law enforcement and correctional agencies' mitigation deployments and the types of mitigation employed;

(2) A list of any aviation security or safety incidents, and any aviation accidents, that occurred due to SLTT law enforcement and correctional agencies' deployment of C-UAS technologies;

(3) Recommendations for improving SLTT law enforcement and correctional agencies' C-UAS training, oversight, compliance, and execution, and the compliance audits required by section 8606(b)(2) of the SAFER SKIES Act; and

(4) A determination whether SLTT law enforcement and correctional agencies are

able to fully protect critical infrastructure from the UAS threat and, if not, recommendations on how to expand C-UAS authorities to critical infrastructure owners. This determination is informed by the protection-request data reported under paragraph (h) of this section.

(5) Instances in which records of communications were retained beyond 180 days, or in which control communications were disclosed outside the originating agency.

§ 124.14 Privacy and civil liberties.

(a) *General.* In exercising authority under 6 U.S.C. 124n(a)(2), an SLTT law enforcement or correctional agency and its personnel must comply with the requirements of 6 U.S.C. 124n(e), including the implementation of privacy protections with respect to the interception, acquisition, access, maintenance, use, and dissemination of communications, consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law. All operations under this part must comply with the requirements of the Fourth Amendment and the policies of the applicable SLTT law enforcement or correctional agency with respect to searches and seizures, and individual searches and seizures conducted during C-UAS operations remain subject to the Fourth Amendment reasonableness requirement.

(b) *First Amendment.* No C-UAS authority under this part may be used solely to seize, monitor, deter, interfere with, or disrupt individuals exercising rights protected by the First Amendment to the Constitution of the United States. When C-UAS operations are conducted at events or locations where individuals are exercising First Amendment rights, personnel must take affirmative steps to minimize the collection, retention, and dissemination of information about those individuals, and must not use C-UAS-derived information to identify, track, or build records on individuals based on their exercise of protected rights.

(c) *Scope of interception.* Communications may be intercepted or acquired only

to the extent necessary to support an action described in 6 U.S.C. 124n(b)(1).

(1) Material captured that is not control communications is incidental capture. Agencies must configure systems to minimize incidental capture, and incidentally captured material determined not to be relevant to a C-UAS, law enforcement, or national security purpose must not be reviewed, retained, or disseminated and must be purged as soon as practicable.

(2) During the contemporaneous C-UAS operation, personnel may view incidentally captured material only to the extent necessary for C-UAS detection, tracking, identification, or mitigation purposes and may not use it for general surveillance or monitoring. If it becomes apparent that the captured video, audio, or other data stream is not control communications, the interception of such communications must be discontinued, and the interception of incidentally captured material must be documented in the post-operation report. When a system's configuration permits adjustment of the scope of interception, such as frequency range, geographic coverage, or signal type, operators must use the narrowest configuration consistent with operational effectiveness.

(3) For standing detection deployments exceeding 30 days, the agency must conduct a review, not less than quarterly, to confirm that the scope of interception remains proportionate to the operational need, that incidental collection of non-UAS communications is being minimized, and that data handling and purge procedures are being executed on schedule. The review may be conducted on a program-wide basis for facilities.

(4) Where identifying the threat requires processing the control signaling of all unmanned aircraft in range, the control communications of an unmanned aircraft determined not to pose a threat may not be retained or used beyond what is needed to make the threat determination and must be purged on the same schedule as other incidental material.

(d) *Records of communications and retention.* (1) Control communications captured, recorded, or maintained by SLTT C-UAS systems constitute records of communications to or from a UAS within the meaning of 6 U.S.C. 124n(e)(3) and must be maintained only for as long as necessary, and in no event for more than 180 days, unless the Agency Approving Official or the agency's chief legal officer determines that maintenance of such records is necessary to investigate or prosecute a violation of law, to directly support an ongoing security operation, for the purpose of any litigation, or is required under Federal, State, local, Tribal, or territorial law, consistent with 6 U.S.C. 124n(e)(3).

(2) Data retained under the ongoing security operation exception must be reviewed at 90-day intervals and purged when the operation concludes, unless another exception applies.

(3) When an agency determines that records of communications will be retained beyond 180 days under any exception, the agency must notify the Federal Bureau of Investigation through the portal within 30 days of the determination.

(4) Pattern data, once extracted and recorded independently, is not a record of communications and is not subject to the 180-day limit. Data generated by systems whose operation does not implicate the electronic surveillance laws referenced in the notwithstanding clause of 6 U.S.C. 124n(a)(2) is likewise not subject to the 180-day limit.

(5) For data retained under the investigation or prosecution exception, the existence of an open investigative or prosecutorial case file documenting the data as evidence satisfies the required determination. For data retained under any other exception, the Agency Approving Official or the agency's chief legal officer must document the specific basis for retention. If an agency has neither an Agency Approving Official nor a chief legal officer, an official holding a rank not below a Senior Executive

or Senior Official, or its equivalent, must document the specific basis for retention.

(6) A standing operational window authorized under § 124.8(h) does not itself constitute an ongoing security operation for purposes of the retention exception; that exception applies only when a specific, identified threat or other intelligence justifies continued retention of specific records to support a discrete protective objective, and the 90-day review must assess whether the specific security basis for retention continues to exist.

(7) The exception for retention required under Federal, State, local, Tribal, or territorial law applies when a specific provision of law affirmatively requires retention of the particular type of data at issue, not when a general records retention schedule incidentally encompasses C-UAS data.

(e) *Dissemination.* (1) Control communications acquired under this part may be disclosed outside the disseminating agency only as authorized by 6 U.S.C. 124n(e)(4): when necessary to investigate or prosecute a violation of law; to support the Department of Defense, a Federal law enforcement agency, or the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory, statutory, or other enforcement action relating to an action described in 6 U.S.C. 124n(b)(1); or as otherwise required by law.

(2) This part does not prohibit the use, as evidence in a subsequent proceeding, of information lawfully obtained incidental to an SLTT law enforcement or correctional agency C-UAS operation, consistent with applicable law.

(3) At the time of any dissemination of control communications, the disseminating agency must document, in the audit trail required by paragraph (g) of this section, the 6 U.S.C. 124n(e)(4) basis for the dissemination, the category of recipient, whether the handling caveat required by paragraph (f) of this section was conveyed, and whether the dissemination included control communications.

(4) A real-time detection feed is governed by the substantive character of the data it transmits. A feed that transmits control communications acquired under this part is subject to the requirements of this section applicable to such data and the limitations under 6 U.S.C. 124n(e)(1), (2), and (4). A feed that transmits only data described in paragraph (e)(6) of this section is not subject to those limitations.

(5) Pattern data that contains no control communications may be disseminated consistent with the agency's standard data handling and information sharing policies and applicable law. Before disseminating pattern data beyond the agency, the disseminating agency must verify anonymization in accordance with its implementation policy and screen the product for operationally sensitive information that would reveal specific coverage patterns, capabilities, gaps, or methods. Public release of pattern data products requires approval at the level designated by the agency's implementation policy.

(6) Data not acquired using the authorities or reliefs provided by 6 U.S.C. 124n, including data generated by systems whose operation does not implicate the electronic surveillance laws referenced in the notwithstanding clause of 6 U.S.C. 124n(a)(2), is not subject to the disclosure limitations of paragraph (e)(1) of this section and may be shared consistent with the agency's standard data handling and information sharing policies and applicable law. Sharing for situational awareness with recipients that are not law enforcement or correctional agencies, including critical infrastructure owners or operators and the public, is limited to data described in this paragraph, unless the disclosure of control communications is authorized under paragraph (e)(1) of this section.

(f) *Protective purpose limitation.* Because the authority of 6 U.S.C. 124n(a)(2) is limited to mitigation of a credible threat, an SLTT law enforcement or correctional agency may disseminate control communications acquired pursuant to the agency's authorities and statutory reliefs under 6 U.S.C. 124n(a)(2) only for law enforcement action arising from the UAS activity that prompted the C-UAS operation, or for aviation

safety. An SLTT law enforcement or correctional agency may not disseminate such control communications for use in an investigation or enforcement action unrelated to UAS activity unless the communications are independently obtainable through lawful means not dependent on the authorities and statutory reliefs under 6 U.S.C. 124n(a)(2). At the time of dissemination, the disseminating agency must communicate the protective purpose for which the control communications are being shared.

(g) *Audit trail.* Each SLTT law enforcement or correctional agency exercising authority under this part must maintain an audit trail sufficient to document each instance in which C-UAS authority was exercised, the basis for the action, the disposition of any data acquired, and any dissemination of data under this part. The audit trail must be searchable and accessible to compliance auditors, protected against unauthorized modification or deletion, and retained for a minimum of 6 years. The agency's implementation policy must specify the format and system of records for the audit trail.

(h) *State and local retention conflicts.* When an SLTT law enforcement or correctional agency determines that a State, local, Tribal, or territorial records retention requirement applicable to law enforcement or correctional agency records encompasses C-UAS communications data and the agency cannot comply with both the 180-day retention limit and that retention requirement, the agency must retain the data for the period required by the applicable law and must apply the handling restrictions of this part, including the prohibition on use for unrelated law enforcement purposes and the dissemination restrictions of this section, for the full duration of retention.

(i) *Third-party acquisition.* An SLTT law enforcement or correctional agency may not request, purchase, subscribe to, or operationally rely on intercepted UAS control communications acquired by any actor lacking lawful authority and relief from certain otherwise applicable laws for the underlying interception, regardless of whether the agency directed or facilitated the original interception. An agency acquiring UAS

intelligence from a third-party source must document the source's lawful authority and relief from otherwise applicable laws for any intercepted content and must apply the retention and dissemination requirements of this section to data so acquired. The agency's implementation policy must specify procedures for evaluating third-party source authority and relief from certain otherwise applicable laws, which must include review and concurrence by appropriate State, local, territorial, or Tribal legal counsel.

(j) *Vendor data sharing.* An SLTT law enforcement or correctional agency may provide operational raw sensor data to system vendors for purposes of system diagnostics, troubleshooting, and performance validation, provided that any communications content is removed before disclosure and the data is used solely for the specific purpose identified. The agency's implementation policy must establish the conditions for vendor data sharing consistent with this paragraph and applicable privacy protections.

§ 124.15 Protection of sensitive operational information.

(a) *Sensitive system information.* Information that links the specific capabilities, vulnerabilities, operating parameters, or countermeasure effectiveness of C-UAS systems to planned or completed operations, including deployment locations, operating radio frequencies, tactical employment methods, and threat-specific mitigation approaches, must be treated as law enforcement sensitive, protected from public disclosure to the extent permitted by applicable law, and, where the information reveals a capability gap of national security concern, evaluated for classification. Other operational coordination information associated with a planned or completed operation, such as the existence, general timing, or general coverage area of a deployment, must be handled as Controlled Unclassified Information and may be shared with covered Federal and SLTT law enforcement and correctional partners, including a State-designated aviation point of contact, for a lawful government purpose. General technical specifications and

evaluation data not associated with a specific planned or completed operation are not subject to these handling requirements. All information described in this paragraph remains subject to any applicable classification, export control, or proprietary restriction.

(b) *Protection from disclosure.* An SLTT law enforcement or correctional agency must take the steps available under applicable State, local, Tribal, or territorial law to protect operationally sensitive information from disclosure through public records requests or civil discovery, and should coordinate with the prosecuting authority in criminal prosecutions arising from C-UAS operations to limit testimony and pleadings to the information necessary to establish the elements of the offense. Nothing in this section requires an agency to take any action inconsistent with applicable State, local, Tribal, or territorial public records law.

(c) *Markings.* Advance notifications, C-UAS Operations Plans, post-operation reports, and compliance audit records must be marked with appropriate sensitivity designations.

(d) *Permitted disclosures.* This section does not prohibit disclosure of sensitive system information to authorized Federal officials, to other participating SLTT agencies in the course of operational coordination, or to the public to the extent required by statute or court order.

§ 124.16 Compliance and enforcement.

(a) *Compliance audits.* The Attorney General, in coordination with the Secretary of Homeland Security and the Administrator of the Federal Aviation Administration, will periodically conduct compliance audits of SLTT law enforcement and correctional agencies exercising authority under 6 U.S.C. 124n(a)(2), as required by 6 U.S.C. 124n(d)(2)(B) and section 8606(b)(2) of the SAFER SKIES Act, to oversee compliance with this part and the privacy protections of 6 U.S.C. 124n(e) as well as to prevent misuse of C-UAS authority. The audit program will include review of post-operation reports,

advance notification records, and agency implementation policies. The FAA will participate with respect to the aviation safety, airspace safety coordination, and deconfliction aspects of the compliance audits conducted under this section.

(b) *Civil fines and penalties.* An SLTT law enforcement or correctional agency, or its personnel authorized to take mitigation actions under 6 U.S.C. 124n(a)(2), that knowingly engages in such actions without Federal coordination as required by 6 U.S.C. 124n and the SAFER SKIES Act, including the advance coordination required by § 124.9, the real-time air traffic control notification required by § 124.11, and the post-action notification to the Attorney General and the Secretary of Homeland Security required by 6 U.S.C. 124n(d)(2)(C) and implemented by § 124.13(a), may be subject to a civil fine of up to $100,000 per violation, or suspension of C-UAS authority pending review by the Attorney General or the Secretary of Homeland Security, as provided in section 8605(f) of the SAFER SKIES Act. Civil penalties will be assessed in accordance with graduated penalty levels proportionate to the severity of the violation and the factors set forth in this part, including the agency's compliance history, the availability and quality of compliance assistance from Federal partners, whether the violation resulted in actual harm, and whether the agency took prompt corrective action. A civil penalty will not be assessed for a first violation of a procedural reporting or notification requirement when the agency demonstrates a good-faith effort to comply and voluntarily self-reports the deficiency. Violations of requirements of this part other than the Federal coordination requirements described in this paragraph do not give rise to civil penalties under section 8605(f) of the SAFER SKIES Act; they are addressed through the compliance audit program of this section, certification and accreditation suspension under § 124.5, and any other remedy available under law.

(c) *Civil enforcement.* The Attorney General is authorized to bring a civil action in a United States district court to collect fines and enforce civil penalties imposed under

this section against any agency or individual, as provided in section 8605(g) of the SAFER SKIES Act.

(d) *Relationship to certification or accreditation suspension.* In addition to civil penalties, the Attorney General or designee may suspend a Mitigation Certification, Detection and Warning Certification, or accreditation under § 124.5(i) for violations of this part. Certification or accreditation suspension may be imposed independently of or in conjunction with other actions described in this section.

§ 124.17 Confiscation and forfeiture.

(a) *Confiscation authority.* (1) An SLTT law enforcement or correctional agency and its personnel may seize or otherwise confiscate a UAS or unmanned aircraft as described in 6 U.S.C. 124n(b)(1)(E). This authority is contingent on a credible threat and applies to the physical taking of possession of an unmanned aircraft that is no longer active in flight or any other UAS component, such as a ground control station.

(2) This authority does not require Mitigation Certification, the use of systems on the Authorized Technologies List or Authorized Systems List, or advance coordination under § 124.9. However, personnel exercising confiscation authority under 6 U.S.C. 124n(b)(1)(E) must hold a current Detection and Warning Certification issued by the NCUTC. An officer who seizes an unmanned aircraft or any other UAS component under traditional law enforcement authority, including an abandoned or crashed unmanned aircraft, does not require Detection and Warning Certification.

(3) Any action that employs C-UAS technology to disrupt or seize control of, damage, disable, or destroy the unmanned aircraft or UAS is an action under 6 U.S.C. 124n(b)(1)(C), (D), or (F) and requires Mitigation Certification.

(4) Personnel exercising confiscation authority should follow standard law enforcement evidence handling procedures, including maintaining chain of custody, preserving digital evidence stored on the aircraft or its flight controller, and observing

applicable hazardous materials precautions.

(5) This part does not affect the authority of any law enforcement or correctional officer to take physical custody of an unmanned aircraft or UAS under traditional law enforcement authority independent of 6 U.S.C. 124n. Traditional law enforcement authority refers to the seizure authorities generally available to law enforcement under applicable Federal, State, local, Tribal, or territorial law, including seizure incident to arrest, seizure of evidence or contraband pursuant to a warrant or a recognized exception to the warrant requirement, and seizure of abandoned property. Once an unmanned aircraft or UAS is on the ground and confiscated, subsequent law enforcement actions, including threat assessment, render safe procedures, evidence collection, and search warrant execution, are governed by traditional legal authorities, including Fourth Amendment requirements and applicable exigency or emergency doctrines, rather than by 6 U.S.C. 124n.

(6) When a C-UAS operation involves a known or suspected unmanned aircraft being used as a delivery mechanism for a hazardous device, the response to the hazardous device must be conducted by a public safety bomb squad accredited through the Hazardous Devices School, consistent with the National Guidelines for Bomb Technicians or any successor publication.

(7) The physical act of interception of a third-party unmanned aircraft while it is in flight, such as catching or netting an aircraft by hand or using a non-electronic physical device to capture it in the air, implicates 6 U.S.C. 124n(b)(1)(D), (E), or (F). Personnel conducting such actions must therefore hold a Mitigation Certification. This does not apply to the erection of physical barriers that a drone operator has an obligation to avoid, such as netting affixed to a physical structure.

(b) *Forfeiture.* Any UAS or unmanned aircraft seized by an SLTT law enforcement or correctional agency pursuant to 6 U.S.C. 124n(a)(2) is subject to

forfeiture under the laws of the seizing agency's jurisdiction, as provided in 6 U.S.C. 124n(c)(2).

§ 124.18 Activities for evaluation, testing, training, and pre-operational validation.

(a) *Scope and legal basis.* An SLTT law enforcement or correctional agency that holds current accreditation under this part may conduct operational acceptance testing of acquired systems and systems under procurement consideration, on-the-job proficiency training, and interoperability training exercises to maintain C-UAS operational readiness. Testing and training do not and must not involve the mitigation of a credible threat and are not conducted under the authority of 6 U.S.C. 124n(a)(2). The operation of RF-emitting systems during testing and training is conducted under applicable Federal Communications Commission authorization and Federal Aviation Administration coordination requirements, and only against controlled test targets owned or operated by, or operated with the consent of, the SLTT law enforcement or correctional agency. An SLTT law enforcement or correctional agency acting pursuant to this section may utilize only authorized technologies under § 124.7. The SLTT law enforcement or correctional agency is responsible for verifying that all necessary Federal Aviation Administration authorizations or regulatory relief for operation of any unmanned aircraft or UAS, including unmanned aircraft or UAS forming part of a C-UAS system, have been obtained prior to any testing, training, or exercises. Compliance with this section is a condition of maintaining certification and accreditation under this part.

(b) *Personnel.* Only personnel holding a current Mitigation Certification may operate mitigation systems during evaluation testing, training, and exercises. Testing, training, and exercises may not be used to train or evaluate uncertified personnel on the operation of mitigation systems. Contractors and vendor representatives may provide technical support and instruction on system-specific procedures but may not independently operate mitigation systems against test targets.

(c) *Evaluation testing and training activities plan.* Before conducting testing, training, or exercises involving RF-emitting C-UAS mitigation systems, the agency must prepare a written activities plan specifying the date, time, and location; the purpose; the systems and equipment to be used; the test, training, or exercise targets; the assigned operators; safety controls; privacy measures; the types of data to be collected and their planned disposition; documentation of Federal Aviation Administration and Federal Communications Commission spectrum coordination for the C-UAS activities, and documentation of any necessary Federal Aviation Administration authorizations or regulatory relief for the operator of the target unmanned aircraft or UAS and for the operation any unmanned aircraft or UAS that form part of the C-UAS system. The activities plan must be approved by the Agency Approving Official or designee and reviewed by the agency's legal counsel.

(d) *Coordination.* Testing, training, and exercises, involving RF-emitting systems, or systems that may affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace, require advance coordination with the Federal Aviation Administration and, for spectrum authorization, with the Federal Communications Commission.

(e) *Privacy within evaluation testing and training.* The agency must favor testing, training, and exercise locations and activities that minimize exposure to non-participating third parties. The agency must not intentionally target, monitor, or collect the communications of non-participating third parties. Communications incidentally collected from non-participating third parties must be purged at the conclusion of the testing, training, or exercise activity, or as soon as practicable thereafter.

(f) *Mitigation restriction.* During testing, training, and exercises, the agency may not intentionally mitigate any UAS or unmanned aircraft that is not a controlled test target, unless necessary to protect against an imminent risk to human life or as part of an

approved C-UAS Operations Plan. An action taken to protect against an imminent risk to human life must comply with the emergency exception set forth in § 124.9(g).

(g) *Pre-operational validation.* Before commencing mitigation operations at an event or facility, an agency may conduct pre-operational validation or equipment functional checks within the operational window and airspace restrictions already coordinated through the advance notification process under § 124.9. The C-UAS Operations Plan must document the pre-operational validation plan and required notifications. No separate authorization from the Department of Homeland Security or the Department of Justice beyond the advance notification is required.

(h) *Participation in Federal RTTE*. Personnel holding active Mitigation Certification may participate in research, testing, training, and evaluation (RTTE) events conducted by Federal components under 6 U.S.C. 124n(b)(3). Personnel may engage with systems in mitigation technology categories beyond those for which they hold an active Mitigation Certification or that are not on the ATL or ASL as part of the event. Participants act under the Federal component's authority and supervision.

§ 124.19 Task force arrangements and Federal support.

(a) *Task force and deputization arrangements preserved.* Task force and deputization arrangements under 6 U.S.C. 124n(a)(1) are not affected by this part. An SLTT law enforcement or correctional agency participating in such an arrangement may continue that participation indefinitely, so long as the deputizing Federal agency continues to have C-UAS authority and relief from certain laws under 6 U.S.C. 124n(a)(1). Nothing in this part requires an agency to seek accreditation under this part, conditions any task force or deputization arrangement on accreditation, or terminates or limits any such arrangement.

(b) *Concurrent authority.* The availability of independent SLTT law enforcement and correctional agency authority under 6 U.S.C. 124n(a)(2) does not preclude continued

participation in C-UAS task forces or deputization arrangements under 6 U.S.C. 124n(a)(1). An SLTT law enforcement or correctional agency and its officers may exercise independent authority and participate in Federal task force operations concurrently or at different times as operational circumstances warrant. Task force operations are governed by the policies applicable to the sponsoring Federal component.

(c) *Federal support.* An SLTT law enforcement or correctional agency may request C-UAS support from an authorized Department of Justice or Department of Homeland Security component. Such support, when provided, constitutes a Federal operation under 6 U.S.C. 124n(a)(1) and is governed by the policies applicable to the supporting component, and the requesting agency's personnel participating in the operation do so under the Federal component's authority and supervision, consistent with applicable task force or deputization arrangements. No formal gubernatorial request is required under this part. Support from the Department of Defense, when available, is governed by the Department of Defense's own authorities, including 10 U.S.C. 130i and 2564, and applicable Department of Defense policies, not by this part.

§ 124.20 Construction.

(a) *No private right.* This part is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(b) *Manned aircraft.* Nothing in this part authorizes the use of C-UAS authority against any aircraft or aircraft system operated with a human pilot, crew, or passengers onboard.

(c) *Mass gatherings.* Consistent with 6 U.S.C. 124n(h)(5), nothing in this part provides a new basis of liability for any State, local, territorial, or Tribal law enforcement officer who participates in the protection of a mass gathering identified by the Secretary

of Homeland Security or the Attorney General under 6 U.S.C. 124n(l)(3)(C)(iii)(II), acts within the scope of the officer's authority, and does not exercise the authority granted to the Secretary of Homeland Security and the Attorney General by 6 U.S.C. 124n.

(d) *Statutory scope*. Nothing in this part alters the scope of the authority of, or the statutory reliefs under 6 U.S.C. 124n(a)(2). A determination that an action does not comply with this part may give rise to administrative, civil, or other consequences provided by law, but does not by itself determine whether the action falls outside the scope of the statutory authorization in, or the relief from criminal liability available under, 6 U.S.C. 124n. Such a determination will be made by the Attorney General, in coordination with the Secretary of Homeland Security and other appropriate officials.

§ 124.21 Termination.

(a) *Termination.* Absent additional statutory authority, the authority of SLTT law enforcement and correctional agencies and their personnel under 6 U.S.C. 124n(a)(2) will terminate on December 31, 2031, as provided in 6 U.S.C. 124n(j)(2).

(b) *Savings.* Termination under paragraph (a) of this section does not affect any obligation, proceeding, or liability that arose before the termination date. Recordkeeping, retention, audit, reporting, and enforcement obligations with respect to operations conducted before the termination date, and any administrative or civil proceeding arising from those operations, survive the termination of authority under this part and remain in effect until satisfied or otherwise resolved.

§ 124.22 Severability.

If any provision of this part, or the application of any provision to any person, entity, or circumstance, is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of this part, and the application of its provisions to any other persons, entities, or circumstances, shall not be affected and shall remain in full force and effect.

_____

Markwayne Mullin,
Secretary of Homeland Security

_____

Daniel E. Burrows,
Assistant Attorney General,
Office of Legal Policy,
Department of Justice
[FR Doc. 2026-13609 Filed: 7/1/2026 4:15 pm; Publication Date: 7/6/2026]