



September 4, 2026

Submitted electronically via <http://www.regulations.gov>

United States Department of Homeland Security
Washington, DC 20528

United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Re: Comments Responding to “Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies” [Docket No. FBI-2026-0001]

To Whom It May Concern:

The Commercial Drone Alliance (“CDA”) appreciates the opportunity to submit comments in response to the Department of Homeland Security (“DHS”) and Department of Justice (“DOJ”) (collectively, the “Departments”) interim final rule titled *Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies* (hereafter the “IFR”).¹ The IFR represents a significant milestone in implementing the SAFER SKIES Act and establishing the regulatory framework through which qualified State, local, Tribal, and territorial (“SLTT”) agencies may exercise counter-UAS (“C-UAS”) authorities.²

The CDA applauds the Administration’s continued efforts to strengthen airspace sovereignty, including through Executive Order (“EO”) 14305, *Restoring American Airspace Sovereignty*, and implementation activities that have followed.³ The CDA has long supported practical measures to address the risks posed by unauthorized drone activity while preserving the many public benefits enabled by lawful drone operations. The IFR marks a logical next step in that process by expanding

¹ 91 Fed. Reg. 41466 (July 6, 2026) (codified at 6 C.F.R. pt. 124 and 28 C.F.R. pt. 124) [hereinafter “IFR”].

² 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) (largely codified in 6 U.S.C. § 124n) [hereinafter “SAFER SKIES Act”].

³ See Exec. Order No. 14,305, 90 Fed. Reg. 24719 (June 11, 2025).

access to C-UAS capabilities beyond the limited federal task force and deputization model that has existed to date.

CDA has consistently advocated for a balanced approach that advances both security and innovation, as the need for effective C-UAS capabilities does not diminish the importance of preserving the benefits enabled by lawful drone operations. Effective C-UAS authorities are essential to protecting people, critical infrastructure, and major public events, and should be implemented while preserving operational certainty for lawful commercial and public safety drone users. To this end, the SAFER SKIES framework should continue to promote both airspace security and the growth of the domestic drone industry, including appropriate safeguards and accountability mechanisms to ensure the lawful and appropriate use of C-UAS authorities in shared airspace.

CDA generally supports the IFR and believes it reflects congressional intent in enacting the SAFER SKIES Act. As discussed below, several targeted refinements would further strengthen implementation by: (1) clarifying the scope of detection technologies covered by the IFR; (2) addressing training capacity constraints and ensuring certification frameworks can scale alongside demand; (3) increasing flexibility for advance notice and notification requirements; (4) establishing long-term solutions for spectrum authorizations; (5) clarifying the scope, purpose, and administration of the Authorized Technologies List (“ATL”) and Authorized Systems List (“ASL”); (6) ensuring that the ATL incorporates non-radio-frequency mitigation capabilities; and (7) creating a more scalable framework for testing, evaluation, training, and certification activities. Collectively, these recommendations are intended to help ensure that the SAFER SKIES framework remains practical, scalable, and capable of advancing both airspace security and continued growth across the domestic drone industry.

I. About the Commercial Drone Alliance

The CDA advocates for U.S. leadership in advanced aviation and actively participates in legislative, regulatory, and policy efforts to facilitate the safe and secure development and expansion of domestic commercial drone operations. The CDA works with all levels of government to collaborate on policies for industry growth and educates the public on the safe and responsible use of commercial drones to achieve economic benefits and humanitarian gains.⁴

The CDA’s membership includes commercial and public safety UAS operators, manufacturers, data service providers, end users across a wide range of industry sectors, drone security companies, and critical infrastructure and fixed-site owners and operators. Many CDA members both rely on drones to support their operations and face the risks posed by unauthorized drone activity. This combination of critical infrastructure stakeholders, drone operators, and technology providers gives CDA a unique perspective on the need to expand effective C-UAS capabilities while preserving freedom of maneuver in the National Airspace System (“NAS”) for lawful commercial and public safety drone operations.

⁴ Learn more at <https://www.commercialdronealliance.org>.

II. Guiding Principles

Reflecting both the diversity of CDA's membership and its longstanding commitment to advancing airspace security alongside continued growth of the domestic drone industry, the recommendations in this comment are guided by several core principles that we believe are essential to achieving the IFR's objectives:

- A. A Secure Airspace is Paramount to Enabling Scalable Drone Operations.** The CDA strongly supports efforts to address the growing risks posed by careless, clueless, and criminal drone operations. Effective airspace security is a prerequisite to the continued expansion of commercial and public safety UAS operations and is critical to maintaining public trust in the drone industry. The federal government does not have the resources to protect every mass gathering event, critical infrastructure facility, correctional institution, or other sensitive location where drone-related threats may arise. It is therefore both practical and appropriate—with the necessary safeguards, training, and oversight in place—to enable qualified SLTT agencies to help address credible drone threats. At the same time, the success of this framework will depend on the availability of sufficient training, resources, and operational support to ensure that implementation keeps pace with demand.
- B. Security and Innovation Must Advance Together.** Drone security and drone innovation are not competing objectives. Rather, they are two sides of the same coin and serve as mutually reinforcing components of a safe, scalable, and sustainable low-altitude aviation ecosystem. The same technological advances that have enabled drones to deliver significant public benefits across critical infrastructure, emergency response, agriculture, logistics, and countless other sectors have also increased the need for effective tools to identify and address unauthorized operations. At the same time, implementation of C-UAS authorities must account for the growing number of lawful commercial and public safety drone operations taking place throughout the NAS. C-UAS implementation should strengthen public safety and airspace security without unnecessarily burdening lawful commercial and public safety drone operations. Indeed, one foreseeable implementation risk of the IFR is the misidentification of a lawful UAS flight as a threat. Effective airspace security therefore depends not only on identifying and mitigating unauthorized operations, but also on ensuring that legitimate operations can continue safely and without unnecessary disruption. Achieving that objective will also require agencies exercising C-UAS authorities to understand and appropriately utilize available airspace awareness and identification tools, including Remote Identification ("Remote ID"), when distinguishing lawful operations from potential threats.
- C. C-UAS Authorities Should Be Implemented Using a Risk-Based Approach.** Regulatory requirements and operational restrictions should be tailored to demonstrated risks. Not every technology, operation, or use case presents the same legal, operational, or security considerations. Implementation of the IFR should avoid unnecessarily broad interpretations that could sweep in activities that do not require the statutory authorities or

legal protections provided by the SAFER SKIES Act. A risk-based framework will better distinguish between technologies that implicate existing legal constraints and those that may be lawfully deployed outside the Part 124 structure. Similarly, training resources should be prioritized where they are most needed, including jurisdictions responsible for protecting major public events, critical infrastructure, correctional facilities, and other locations presenting heightened risk profiles already protected by a permanent or temporary flight restriction.

- D. A Clear, Predictable, and Scalable Framework Is Critical to Long-Term Success.** The effectiveness of the IFR will ultimately depend on whether it can function at scale across thousands of public safety agencies and the increasing complexity of the NAS. Clear regulatory guidance is essential to ensure that SLTT agencies, manufacturers, critical infrastructure operators, and commercial drone users understand when authorization is required, how compliance obligations apply, and which activities remain permissible outside the Part 124 framework without additional authorization. Regulatory uncertainty and implementation bottlenecks risk slowing deployment of needed security capabilities while also creating challenges for lawful operators. The final rule should therefore prioritize a framework capable of supporting implementation across thousands of public safety agencies and scalable in real-world operational environments as C-UAS technology use continues to grow.

III. General Areas of Support

The CDA supports several aspects of the IFR and believes the rule generally reflects congressional intent in enacting the SAFER SKIES Act. In particular, we wish to highlight the following areas of support:

- A. General Framework for SAFER SKIES Act Implementation.** The CDA supports the IFR's establishment of a practical framework for implementing the SAFER SKIES Act and expanding access to C-UAS capabilities for SLTT agencies. For many years, stakeholders have recognized the need for a clear process by which qualified SLTT agencies can exercise limited C-UAS authorities with appropriate oversight, training, and coordination. While, as discussed below, certain aspects of the rule would benefit from additional clarification and refinement, the CDA supports the Departments' efforts to translate the statute into an operational framework capable of supporting real-world deployments.
- B. Training, Certification, and Operational Oversight Framework.** The CDA supports the IFR's emphasis on training as a prerequisite to exercising C-UAS authorities. Detection and mitigation activities carry important legal, operational, and safety considerations, and standardized training helps promote accountability and responsible use of these authorities. In particular, the CDA supports the requirement in § 124.3(e)(1) that personnel seeking Mitigation Certification hold a Part 107 Remote Pilot Certificate. Individuals authorized to mitigate a UAS should possess a baseline understanding of airspace, aviation safety principles, and the regulatory framework governing drone operations. The

CDA also supports the IFR's centralized approach to training, certification, and operational oversight. The combination of centrally administered certification requirements and the designation of an Agency Approving Official establishes a clear chain of responsibility for the exercise of C-UAS authorities. This framework promotes consistency across jurisdictions while providing the federal awareness, guidance, and oversight necessary to help ensure that accredited SLTT agencies exercise these authorities safely and responsibly.

- C. Mutual Aid Provisions.** The CDA supports the inclusion of a framework for mutual aid agreements and regional approaches to C-UAS operations in § 124.4(c). Not every jurisdiction responsible for protecting critical infrastructure, correctional facilities, major transportation assets, or large public gathering venues has the resources necessary to maintain a dedicated C-UAS program or specialized personnel. This is particularly true for smaller jurisdictions that may nonetheless be responsible for protecting critical infrastructure, major sporting events, or other large gatherings. The mutual aid framework helps extend access to C-UAS capabilities in a cost-effective manner and reflects the practical reality that regional cooperation will often be necessary to support implementation of the SAFER SKIES Act across the diverse communities, facilities, and events the rule is intended to protect. Mutual aid arrangements also provide a practical mechanism for sharing expertise and operational capabilities while still ensuring compliance with the rule's certification and training requirements.
- D. Accountability and Oversight Mechanisms.** The CDA supports the IFR's emphasis on accountability and oversight in the exercise of C-UAS authorities. The significant authorities provided under the SAFER SKIES Act should be accompanied by clear lines of responsibility, robust operational safeguards, and appropriate federal visibility into how those authorities are used. The IFR's accreditation, training, certification, planning, and reporting requirements help promote responsible implementation while reinforcing public confidence in the safe and effective use of C-UAS capabilities by accredited SLTT agencies. The CDA also supports the inclusion of enforcement and compliance mechanisms under § 124.16 as an important means of deterring misuse of these authorities.

IV. Recommendations

Consistent with the guiding principles outlined above, the CDA offers the following recommendations to further improve the IFR and help ensure that its implementation advances both the security objectives of the SAFER SKIES Act and the long-term development of the domestic drone industry:

A. Clarify the Scope of Detection Technologies Covered by the IFR

The IFR appropriately recognizes that certain detection technologies operate outside the Part 124 framework and therefore do not require the authorities or legal protections provided by the SAFER

SKIES Act.⁵ However, uncertainty remains regarding the treatment of other detection capabilities, particularly radio frequency (RF)-based detection systems. As a result, SLTT agencies, critical infrastructure operators, technology providers, and other stakeholders may face uncertainty regarding which technologies require authorization under Part 124, and which may continue to operate under existing legal authorities.

This uncertainty is significant because many drone detection technologies have been lawfully deployed for years by entities that are not seeking to operate under the authorities provided by the SAFER SKIES Act. Critical infrastructure operators, airports, correctional facilities, sports and entertainment venues, and other stakeholders routinely rely on detection technologies to maintain awareness of drone activity and distinguish authorized operations from potential threats. The continued use of these capabilities is important not only to individual operators, but also to broader national efforts to improve airspace awareness and strengthen security at critical sites.

Current federal policy likewise reflects both the importance of expanding drone-detection capabilities and the lack of clear boundaries within the existing legal framework. FEMA's Counter-UAS Grant Program Notice of Funding Opportunity (hereafter the "FEMA NOFO") recognizes detection, identification, tracking, and monitoring capabilities as important components of a comprehensive C-UAS posture and states that individuals, private organizations, and government agencies may lawfully detect, track, and identify UAS using observable information or communications that are "readily accessible to the public."⁶ DOJ similarly acknowledged in a recent memorandum the "widely recognized complexities" in the statutes governing C-UAS activities.⁷ Further, the Administration's *Restoring American Airspace Sovereignty* EO recognizes the importance of detection-based technologies by directing updates to federal guidance and calling for additional resources to assist private critical infrastructure owners and operators in lawfully employing technologies to detect, track, and identify drones and drone signals.⁸ Similarly, the FAA's proposed changes to the airspace in its Section 2209 Notice of Proposed Rulemaking underscore the importance of situational awareness around sensitive facilities and critical infrastructure. The proposal reflects a growing recognition that effective airspace security depends on the ability of facility operators and other stakeholders to lawfully detect, identify, and monitor drone activity near protected locations.⁹ Together, these federal initiatives recognize both the importance of expanding C-UAS capacity and the reality that not all detection technologies fit neatly within a single regulatory category.

⁵ See IFR at 41470, 41474.

⁶ See U.S. Dep't of Homeland Sec. & Fed. Emergency Mgmt. Agency, *Counter-Unmanned Aircraft Systems Grant Program Notice of Funding Opportunity* 24 (2025), https://files.simpler.grants.gov/opportunities/3cabeeb1-e8fd-4426-8783-c2a0039f1a10/attachments/ab94bff9-1cd5-4e3b-9a34-3bb732ae9bf1/Counter-Unmanned_Aircraft_Systems_Grant_Program_NOFO_Final_508.pdf [hereinafter "FEMA NOFO"].

⁷ Memorandum from the Acting Att'y Gen. to All Federal Prosecutors, *Charging Policy Concerning Defense Actions Against Unmanned Aircraft Systems* (June 12, 2026), <https://www.justice.gov/olp/media/1450041/dl?inline>.

⁸ See Exec. Order No. 14,305, 90 Fed. Reg. 24719 (June 11, 2025).

⁹ See *generally* Designation—Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility, 91 Fed. Reg. 24,650 (proposed May 6, 2026) (to be codified at 14 C.F.R. pt. 74) (implementing Section 2209 of the FAA Extension, Safety, and Security Act of 2016).

Accordingly, the CDA recommends that the Departments provide additional clarifying guidance in the final rule that Part 124 applies *only* to technologies that clearly require the statutory authorities and legal protections provided by the SAFER SKIES Act. Guidance should clearly distinguish those technology categories and systems from detection capabilities that may lawfully operate without such relief. Doing so would provide greater certainty to public safety agencies, critical infrastructure operators, and technology providers, and avoid unintentionally sweeping lawful airspace awareness and drone detection technologies into a framework that was not intended to govern them.

B. Address Training Capacity Constraints

One of the principal implementation challenges facing the IFR is ensuring that training capacity scales alongside demand. The rule contemplates expanding access to C-UAS authorities across a broad range of SLTT agencies responsible for protecting critical infrastructure, correctional facilities, transportation assets, and major public gathering venues. Mitigation certification is currently tied to training provided through the FBI's National Counter-UAS Training Center ("NCUTC"). With approximately 17,000 state and local law enforcement agencies nationwide,¹⁰ a single training center is unlikely to satisfy anticipated demand as participation in the SAFER SKIES program grows. As a result, qualified agencies may face substantial delays in obtaining the certifications necessary to exercise authorities Congress authorized through the SAFER SKIES Act.

Another significant scalability challenge relates to mitigation certification and technology specific training requirements. Under § 124.7(d), agencies may employ mitigation systems only within technology categories for which personnel have completed the applicable NCUTC coursework.¹¹ As new technology categories and systems are added to the ATL and ASL, agencies should not face prolonged delays between approval of a technology category and availability of the associated training. Otherwise, implementation timelines may become dependent on training availability rather than operational need or technology readiness.

For these reasons, the CDA recommends that DHS and DOJ prioritize development of a scalable training framework capable of supporting long-term implementation of the SAFER SKIES Act training requirements and increasing overall airspace security. As participation in the program grows, training opportunities should be prioritized and administered in a manner that promotes operational readiness and effective use of available resources. The Act requires establishment of a "national schoolhouse" for mitigation training, and CDA strongly supports the goal of a standardized national curriculum and consistent certification standards.¹² However, the requirement for a national schoolhouse should not be interpreted to mean that mitigation training must be delivered through a single physical training location. DHS and DOJ should consider approaches that preserve a uniform curriculum while expanding training capacity through additional approved training sites, regional

¹⁰ See Dep't of Just., Bureau of Just. Stats., *Census of State and Local Law Enforcement Agencies, 2018* 1 (2018), <https://bjs.ojp.gov/library/publications/census-state-and-local-law-enforcement-agencies-2018-statistical-tables> ("In June 2018, a total of 17,541 state and local agencies performed law enforcement functions in the United States and employed 1,214,000 full-time sworn and civilian personnel . . .").

¹¹ See IFR at 41488, 41506.

¹² SAFER SKIES Act § 8602, 139 Stat. at 1938–1943.

training opportunities, mobile education and training teams (“MTTs”), or other qualified federal training facilities. To that end, the Departments should also consider a modular training framework that combines standardized federal instruction on legal authorities, operational requirements, and safety considerations with federally approved, technology-specific training for authorized systems. When necessary, the Departments should permit interim operator qualification through manufacturer-delivered, system-specific training, consistent with §§ 124.4(b) and 124.18(b). The Departments should also ensure that training modules are developed and made available promptly when new technology categories are added to the ATL. These steps would help ensure that training remains an important safeguard while avoiding unnecessary constraints on implementation as participation in the program expands.

Finally, the Departments should also consider whether the online detection curriculum should be made available to critical infrastructure owners and operators and other stakeholders that play a role in protecting sensitive facilities but are not directly exercising authorities under Part 124. Expanding access to these awareness-focused training resources would help strengthen broader airspace security and increase coordination among key stakeholders.

C. Increase Flexibility for Advance Coordination and Notification Requirements

Per §§ 124.8 and 124.9, the IFR establishes detailed advance coordination requirements for mitigation operations, including a 30-calendar-day advance notification through a federal coordination portal before mitigation operations and a 7-calendar-day submission of the C-UAS Operations Plan before commencement. These requirements serve important objectives by promoting operational consistency and coordination among federal and SLTT stakeholders. However, these prescribed timelines may prove difficult to satisfy in certain operational environments and could limit the ability of qualified agencies to respond to evolving threat conditions.

The CDA supports the IFR’s recognition that certain facilities, venues, and locations may require recurring C-UAS coverage and appreciates the flexibility provided through standing operational windows for recurring operations under § 124.8(h)(2). This approach recognizes the reality that many C-UAS missions involve substantially similar operational circumstances conducted over extended periods of time or repeated under similar circumstances at the same venue, such as for sporting events. The ability to use standing operational windows reduces unnecessary administrative burdens and reflects the realities of protecting facilities and events that require consistent security coverage.

Even with this flexibility, implementation challenges may still arise from the separate advance notification requirements established by § 124.9. Drone-related threats are often dynamic, and agencies may receive credible intelligence, identify suspicious activity, or encounter changing operational circumstances after standard notification windows have closed. When updated threat assessments or operational requirements arise after a notice has already been submitted, agencies must have sufficient flexibility to adapt their existing operational windows without being constrained by timelines designed for more predictable circumstances.

To preserve the benefits of the standing operational framework, the CDA recommends that the Departments ensure that agencies have an established and practical mechanism for modifying or

supplementing previously submitted notifications when circumstances change. While the IFR contemplates updates for material changes for standing operational windows,¹³ additional guidance would help clarify how agencies should address newly identified threats, schedule changes, elevated threat conditions, or other developments that arise within existing operational windows but outside standard notification timelines for both standing and non-standing operational windows. To the extent DHS and DOJ intend existing provisions, including the material change process under § 124.8(h)(2) and the emergency exception under § 124.9(g), to provide sufficient flexibility to accommodate such situations, that interpretation should be clearly reflected in guidance and supported by standardized procedures. These steps would help ensure that coordination requirements remain operationally practical while preserving the security objectives of the rule.

D. Ensure Long-Term Solutions for Spectrum Authorizations

The success of the SAFER SKIES Act depends as much on the successful implementation of the IFR as it does on a clear, long-term pathway for agencies to receive spectrum authorization from the Federal Communications Commission (“FCC”). The IFR appropriately recognizes that deployment of RF-emitting C-UAS systems may require separate FCC authorization in addition to compliance with Part 124.¹⁴ CDA applauds the FCC’s recent actions, including issuance of a Special Temporary Authority (“STA”) to support initial SAFER SKIES implementation, that have provided an important near-term mechanism for operation of approved systems.¹⁵ The temporary nature of the STA, however, also underscores the need for a longer-term regulatory solution. As agencies, manufacturers, and technology providers invest in implementation, greater certainty regarding spectrum access and FCC authorization will become increasingly important to ensuring that approved technologies can be deployed consistently and predictably in the field.

Long-term regulatory certainty is important to all stakeholders participating in the SAFER SKIES framework. SLTT agencies must be able to invest in training, equipment, and operational planning with confidence that necessary FCC authorizations will remain available. Similarly, manufacturers and technology providers require a predictable regulatory environment to support product development, testing, and deployment. Absent a durable authorization framework, otherwise qualified agencies may face uncertainty regarding their ability to continue operating approved systems after temporary authorizations expire. A clear path forward is also important from an implementation perspective. The success of the SAFER SKIES Act depends not only on certification, training, and operational approval under Part 124, but also on the ability of agencies to lawfully operate approved

¹³ See IFR at 41490, 41508.

¹⁴ See IFR at 41468; see also IFR at 41491, 41508.

¹⁵ See generally *Counter-UAS Spectrum Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies under the SAFER SKIES Act; Unleashing American Drone Dominance*, Order, DA 26-657 (OET rel. July 2, 2026); *Counter-UAS Spectrum Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies under the SAFER SKIES Act; Unleashing American Drone Dominance*, Order, DA 26-656 (WTB/OET/PSHSB/SB/MB rel. July 2, 2026); *Application of Section 333 of the Communications Act to Development or Operations of Counter Unmanned Aircraft Systems for the Federal Government and under the SAFER SKIES Act; Unleashing American Drone Dominance*, Declaratory Ruling, DA 26-655 (WB rel. July 2, 2026); *Application of Section 333 of the Communications Act to the Testing of Counter-Unmanned Aircraft Systems Technologies; Unleashing American Drone Dominance*, Declaratory Ruling, DA 26-654 (WTB/OET rel. July 2, 2026).

technologies in the field. Separate authorization processes that are duplicative or subject to recurring short-term extensions risk creating friction that could slow deployment of capabilities that Congress intended for qualified agencies.

For these reasons, the CDA encourages continued coordination among DHS, DOJ, and the FCC to establish a durable, long-term regulatory framework governing spectrum access and authorization for approved C-UAS technologies. In the near term, the FCC should consider extending the STA to avoid disruptions while a long-term framework is developed. More broadly, federal agencies should seek opportunities to reduce duplicative reviews, provide greater transparency regarding authorization pathways, and ensure that accredited agencies can continue to deploy approved technologies in a lawful and predictable manner.

E. Clarify the Scope and Purpose of the Authorized Technologies List and Authorized Systems List

As implementation of the SAFER SKIES Act moves forward, clear distinctions between technologies that require Part 124 authorization and those that may lawfully operate outside that framework will become increasingly important. Public safety agencies, critical infrastructure operators, technology providers, and other stakeholders need a clear understanding of when the authorities and legal protections provided by the Act are required and when existing legal authorities remain sufficient. Absent that clarity, uncertainty could discourage deployment of lawful airspace awareness capabilities and create confusion regarding the scope of the IFR.

The IFR establishes the ATL and ASL to identify technology categories and systems that may be used by accredited agencies when exercising authorities provided by 6 U.S.C. § 124n. While these lists serve an important role in the Part 124 framework, they do not encompass all technologies that may lawfully be used for drone detection or airspace-awareness purposes. As discussed in Section IV.A *supra*, the IFR expressly recognizes that certain technologies fall outside the scope of Part 124 and do not require the statutory authorities or legal protections provided by the SAFER SKIES Act. Yet use of the word “Authorized” within the names of the ATL and ASL could reasonably be interpreted to suggest that technologies *not* included on either list are somehow unauthorized. For stakeholders unfamiliar with these distinctions, this creates a risk that lawful technologies operating outside the Part 124 framework will be incorrectly viewed as requiring inclusion on one of the lists before they may be deployed.

This concern extends beyond terminology. As implementation proceeds, the ATL and ASL are likely to become the primary reference point for agencies, technology providers, and infrastructure operators seeking to understand what technologies may be used within the SAFER SKIES framework. If the scope and purpose of the lists are not clearly communicated, the practical result could be uncertainty regarding technologies that have long been deployed for airspace awareness and security purposes outside the SLTT context. Such uncertainty would be inconsistent with broader federal efforts to expand drone detection and airspace awareness capabilities.

For these reasons, the CDA recommends that DHS and DOJ make clear in both the final rule and accompanying guidance that the ATL and ASL are not intended to identify every technology that

may be lawfully procured or deployed by an SLTT agency. Rather, the lists are intended to identify technologies and systems that require the authorities or legal protections provided by the SAFER SKIES Act. A technology's absence from the ATL or ASL should not be interpreted to mean that it is unlawful, unavailable for procurement, or unsuitable for deployment. The CDA further encourages the Departments to consider whether alternative terminology, such as a "Part 124 Covered Technologies List" and "Part 124 Covered Systems List," would better communicate the intended scope of the framework and reduce stakeholder confusion. At a minimum, this distinction should be reinforced through both the Detection Certification and Mitigation Certification training programs to ensure that accredited agencies understand the limited purpose of the lists and the distinction between technologies that require SAFER SKIES authorities and those that may lawfully operate outside the Part 124 framework.

The CDA also encourages the Departments to provide greater transparency regarding the process by which technologies and systems are evaluated for inclusion on the ATL and ASL. While Part 124 establishes the framework for maintaining the lists, the criteria, procedures, and timelines governing inclusion are not set forth in the rule itself, and stakeholders have limited visibility into how technologies are evaluated or how listing decisions are made.¹⁶ Greater transparency would promote confidence in the framework, provide more predictable pathways for technology adoption, and help ensure that the lists remain responsive to evolving operational needs and technological developments. To support long-term implementation, DHS and DOJ should consider publishing general listing criteria, establishing target review timelines, providing applicants with a written explanation when a technology or system is not selected for inclusion, and creating a mechanism for reconsideration where appropriate. The Departments should also evaluate whether manufacturers should be permitted to submit technologies and systems directly for consideration rather than solely through accredited agencies.¹⁷ These measures would improve transparency, reduce administrative friction, and help ensure that the ATL and ASL remain scalable and capable of supporting the long-term objectives of the SAFER SKIES Act.

F. Ensure the Authorized Technologies List Incorporates Non-RF Mitigation Capabilities

Several provisions of the IFR expressly contemplate non-RF mitigation activities. For example, § 124.17(a)(7) specifically addresses in-flight physical interception and requires personnel conducting such actions to hold Mitigation Certification.¹⁸ These provisions reflect the reality that mitigation may be accomplished through a variety of technological approaches—not just through RF-based means—and that different operational environments may require different tools. As implementation of the SAFER SKIES Act moves forward, it will be important to ensure that accredited agencies retain access to a diverse range of mitigation capabilities to address evolving threats while supporting the rule's

¹⁶ See IFR at 41472 ("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.").

¹⁷ See IFR at 41472.

¹⁸ See *id.* at 41475, 41497, 41514.

proportionality requirements.

For these reasons, the CDA recommends that DHS and DOJ include a non-RF technology category on the ATL covering physical interception and capture technologies. If evaluation of such a category cannot be completed before publication of the final rule, the Departments should establish and publish a target timeline for its consideration. Doing so would better align the ATL with the broader range of mitigation activities already contemplated elsewhere in the IFR and help ensure that accredited agencies have access to a diverse set of mitigation tools appropriate for different operational environments and threat scenarios. The CDA further recommends that DHS and DOJ provide additional guidance on how mitigation technologies will be categorized and incorporated into the ATL, including confirmation that classification will be based on the mechanism by which they affect the target aircraft. Such clarification would help ensure that physical interception and other non-RF mitigation systems are evaluated within the appropriate technology category and provide greater certainty regarding how innovative mitigation approaches may be incorporated into the SAFER SKIES framework over time.

G. Clarify the Role of Designated Test Ranges and Expand Physical Capacity for Testing, Training, and Certification

Section 124.18 establishes an important framework for operational acceptance testing, proficiency training, and pre-operational validation activities. The CDA supports the Departments' recognition that accredited agencies must be able to test systems, maintain operator proficiency, and validate equipment before deployment. As participation in the SAFER SKIES program expands, the testing and evaluation framework must be capable of scaling alongside training and certification requirements. Even without broadening the training bottleneck, the Departments project growth from approximately 46 certified agencies today to roughly 1,500 detection-tier agencies and 150 mitigation-tier agencies within two years.¹⁹ If the framework is to remain responsive to evolving threats, the pathway for evaluating new technologies must be as scalable as the authorities the rule is designed to support.

The IFR also leaves unanswered questions regarding how new technologies move through the evaluation and authorization process. Section 124.18(a) does not extend the authorities provided by 6 U.S.C. § 124n(a)(2) to operational acceptance testing, proficiency training, interoperability exercises, or pre-operational validation activities, and instead directs participants to existing FAA and FCC coordination and authorization mechanisms.²⁰ At the same time, testing and training activities are generally limited to technologies authorized under § 124.7. While § 124.18(h) contemplates participation in Federal research, testing, training, and evaluation ("RTTE") activities involving technologies not yet included on the ATL, the rule does not establish a recurring process or published schedule for those activities. As a result, it is unclear how emerging technologies can consistently

¹⁹ See *id.* at 41480.

²⁰ See *id.* at 41475 ("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.")

generate the operational data and evaluation record necessary to support future listing decisions, particularly as participation in the SAFER SKIES program expands.

To support long-term implementation, the CDA recommends that DHS and DOJ establish a more predictable and scalable framework for testing and evaluation activities. In particular, the Departments should clarify the role that existing FAA-recognized UAS Test Sites, designated test ranges, and other authorized facilities may play in supporting activities conducted under § 124.18, including whether such facilities may assist with preparing the mandated evaluation testing and training activities plan and coordination requirements while the accredited agency retains responsibility for compliance with Part 124.

The CDA further recommends that the Departments establish a standing or programmatic pathway for FAA and FCC coordination of recurring testing, proficiency training, and validation activities, rather than requiring agencies to navigate separate authorization processes for routine events. The Departments should also conduct RTTE activities on a recurring schedule and provide greater visibility into the process by which new technologies may be evaluated for future consideration on the ATL. These steps would help ensure that the framework remains capable of evaluating emerging technologies at the pace of innovation while supporting the scalable implementation Congress envisioned.

V. Conclusion

The CDA appreciates the opportunity to provide comments on the IFR and applauds the Departments' efforts to implement the SAFER SKIES Act in a manner that expands access to C-UAS capabilities for qualified SLTT agencies while preserving the safety and efficiency of the NAS. A clear, predictable, and scalable framework requires the ability to identify and address implementation challenges as they emerge. As C-UAS authorities continue to expand, the CDA encourages continued engagement among DHS, DOJ, SLTT agencies, UAS operators, manufacturers, and critical infrastructure stakeholders. Doing so will help ensure that the framework evolves alongside changing technologies and threats.

We look forward to continued engagement as the final rule comes to fruition and to continued collaboration with DHS, DOJ, and other stakeholders to advance both airspace security and American leadership in drone innovation.



Lisa Ellman
Chief Executive Officer
Commercial Drone Alliance