

Public Comment of The Box Commons on FCC Public Notice DA 26-314A1, Unleashing American Drone Dominance

The Box Commons

April 22, 2026

The Box Commons c/o Northwest Registered Agent LLC 30 N Gould Street, Suite N Sheridan, WY 82801 info@theboxcommons.org

April 22, 2026

Federal Communications Commission 45 L Street NE Washington, DC 20554

Re: Comment on Public Notice DA 26-314A1, *Unleashing American Drone Dominance*, 91 Fed. Reg. (April 16, 2026), Document ID 2026-07381

Dear Commissioners and Staff of the Wireless Telecommunications Bureau and Office of Engineering and Technology,

1. Introduction

The Box Commons is a Wyoming nonprofit corporation organized as a Section 501(c)(6) standards body for credentialing and conformance assessment of autonomous and AI-enabled systems. We submit this comment in response to the Commission’s April 1, 2026 Public Notice seeking input on actions to advance U.S. drone production, spectrum access, and deployment.

The Box Commons takes no position on specific spectrum allocation questions, which fall within the Commission’s core engineering and spectrum management expertise. We write to address one area where a credentialing standards body can contribute directly: the Public Notice’s inquiry into establishing a **trusted supplier framework** and providing **regulatory clarity and technical access for U.S. manufacturers**.

2. The Trust Definition Gap

The Public Notice contemplates the possibility of publishing a “trusted UAS list” for state, local, tribal, and territorial partners, and asks how the Commission can provide regulatory clarity to domestic manufacturers seeking to fill the gap left by the December 2025 addition of all foreign-made UAS and components to the Covered List.

This framing identifies a real need, but a government-maintained supplier list — however carefully curated — faces a structural limitation: it is static at the moment of publication, while the systems it aims to characterize are dynamic. An unmanned aircraft system that meets trust criteria at the time of listing may diverge from those criteria as firmware is updated, software components are revised, communications modules are substituted, or operational design domains expand. The trust

question for autonomous and semi-autonomous UAS is not only *who manufactured this system* but *what can this system be verified to do, as of today, against published criteria*.

This is not a novel observation. Professor Ella Atkins of the University of Michigan, in her work on certifiable autonomous flight management, has identified the core challenge: autonomous aerospace systems require certification frameworks that account for the behavioral and software-defined nature of their safety properties, rather than relying solely on the physical, hardware-oriented testing paradigms that govern conventional aircraft certification. See E. Atkins, “Certifiable Autonomous Flight Management for Unmanned Aircraft Systems,” in *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2009 Symposium*, National Academy of Engineering (2010); E. Atkins, “Intelligent Systems for Unmanned Aircraft Safety Certification,” AIAA Aerospace Sciences Meeting, Nashville, TN (2012). The same insight applies to the trust determination the Commission now considers for UAS suppliers: trust in an autonomous system must be verifiable against defined criteria, not merely asserted at the point of sale and assumed thereafter.

3. Credential-Based Trust as a Complement to Supplier Lists

We respectfully suggest that the Commission consider a credential-based trust model as a complement to — not a replacement for — any supplier list the Commission may publish. A credential-based model would operate as follows:

(a) Published technical criteria for UAS trust. The Commission, in coordination with existing standards development organizations such as ASTM International (particularly Committee F38 on Unmanned Aircraft Systems) and the ANSI UAS Standardization Collaborative, would identify or reference published, version-controlled technical criteria against which UAS systems can be assessed. These criteria might address, for example, communications security, spectrum compliance, supply chain transparency, firmware integrity, and remote identification conformance.

(b) Independent conformance assessment. A UAS manufacturer or system integrator seeking “trusted” status would undergo assessment by a conformity assessment body operating under ISO/IEC 17065:2012 and accredited under ISO/IEC 17011:2017 — the same accreditation architecture that underlies FedRAMP, FIPS 140-3 cryptographic module validation, and Common Criteria evaluations. This model is well-established in adjacent federal contexts and does not require the Commission to build or operate a new assessment infrastructure.

(c) Machine-readable credentials. The result of conformance assessment would be expressed as a machine-readable, cryptographically verifiable credential — a record that a specified UAS configuration, as of a specified date, meets specified criteria as confirmed by a specified accredited assessor. Such credentials can travel with systems across jurisdictions, can be verified programmatically by state and local agencies considering procurement decisions, and can be revoked or superseded when system configurations change.

(d) Continuous conformance. Because UAS systems evolve through software and firmware updates, a credential-based model would include provisions for periodic reassessment or continuous reporting, ensuring that a system’s trust status reflects its current configuration rather than its configuration at initial assessment.

This four-element pattern is not novel. It is the architecture by which trust is already operationalized in federal cybersecurity (FedRAMP), cryptographic validation (FIPS 140-3), and international product certification (Common Criteria). The Commission’s UAS trust framework would benefit from this proven architecture rather than requiring the Commission itself to maintain a continuously

updated list — a burden that would scale linearly with the number of domestic manufacturers the Commission seeks to encourage.

4. Relevance to State, Local, Tribal, and Territorial Partners

The Public Notice specifically asks about coordination with SLTT agencies, including whether such agencies currently procure UAS from foreign adversaries and how the Commission can help prioritize U.S.-made alternatives. A credential-based trust model directly serves this need: rather than requiring each SLTT procurement office to independently evaluate UAS suppliers against its own criteria, a nationally recognized credential provides a common, portable basis for procurement decisions. The credential does the verification work once; every SLTT agency that recognizes it benefits.

This is analogous to the role played by UL (Underwriters Laboratories) product safety certifications in building and electrical codes — local authorities having jurisdiction do not independently test every electrical product, but instead recognize certifications issued by accredited testing laboratories against published standards.

5. The Box Commons’s Standing Offer

The Box Commons respectfully offers to participate, at no cost to the Commission, in any proceeding, workshop, or technical advisory effort the Commission may convene to develop a trusted UAS supplier framework. We have ongoing engagement with NIST on AI agent identity and authorization, with CEN/CENELEC JTC 21 on European AI conformity assessment standards, and with state-level autonomous entity registry processes. We welcome the opportunity to contribute draft credential schemas, assessment criteria mapping, and conformance testing specifications drawing on this work.

6. Conclusion

The Commission’s Public Notice reflects a sound instinct: that U.S. drone dominance requires not only spectrum access and manufacturing incentives, but also a trust framework that gives government and commercial users confidence in the systems they procure. We respectfully suggest that this trust framework will be most durable and scalable if it is built on the proven conformance assessment architecture that the federal government already uses in adjacent domains, rather than on a government-maintained list that must be continuously updated. The Box Commons stands ready to support the Commission in this effort.

Respectfully submitted,

Brice Love Acting Executive Director The Box Commons info@theboxcommons.org