

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of	)	
	)	
Protecting Against National Security Threats to	)	ET Docket No. 21-232
the Communications Supply Chain through the	)	
Equipment Authorization Program	)	

COMMENTS OF THE COMMERCIAL DRONE ALLIANCE

Katy Milner
HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
katy.milner@hlc.com
+1 202-637-6432

Lisa Ellman
Chief Executive Officer
COMMERCIAL DRONE ALLIANCE
555 Thirteenth Street, NW
Washington, DC 20004
lellman@commercialdronealliance.org

September 8, 2026

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY	1
II.	THE COMMISSION SHOULD PRESERVE THE BENEFITS OF ITS LONGSTANDING AND EFFICIENT EQUIPMENT AUTHORIZATION PROCESS FOR TRUSTED MANUFACTURERS.....	2
A.	An Across-the-Board Certification Requirement for the UAS Sector Would Burden American Manufacturers and Weaken the Domestic Drone Industry’s Global Competitiveness.	2
B.	The Commission Should Preserve Manufacturers’ Ability to Rely on Pre-Certified Modules.	4
III.	THE COMMISSION SHOULD NOT REQUIRE HBOM AND SBOM DISCLOSURES AS PART OF THE EQUIPMENT CERTIFICATION PROCESS.	4
IV.	THE COMMISSION SHOULD ESTABLISH CLEAR AND WORKABLE DEFINITIONS OF KEY COVERED LIST TERMS.	8
A.	The Commission Should Adopt Its Proposed Definition of “Produced in a Foreign Country.”	8
B.	The FCC Should Adopt a Revised Version of Its Proposed “Produced By” Definition.	8
C.	The Commission Should Adopt Its Proposed Definition of “UAS Critical Components.”	9
V.	EXEMPTIONS, SAFE HARBORS, AND REASONABLE IMPLEMENTATION PERIODS ARE KEY TO SUPPORTING DOMESTIC MANUFACTURING AND ACHIEVING AMERICAN DRONE DOMINANCE.....	10
VI.	CONCLUSION	12

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of	)	
	)	
Protecting Against National Security Threats to	)	ET Docket No. 21-232
the Communications Supply Chain through the	)	
Equipment Authorization Program	)	

COMMENTS OF THE COMMERCIAL DRONE ALLIANCE

I. INTRODUCTION AND SUMMARY

The Commercial Drone Alliance (“CDA”)¹ respectfully submits these comments in response to the Federal Communications Commission’s (“FCC” or “Commission”) *Third Further Notice of Proposed Rulemaking* (“FNPRM”) on strengthening the Commission’s equipment authorization framework to address national security risks to the communications supply chain.² The future of aviation is unmanned. America, rather than China or any other adversary, must lead. The CDA therefore strongly supports the Administration’s and Chairman Carr’s commitment to protecting national security through the equipment authorization program, strengthening U.S. leadership in unmanned aircraft systems (“UAS”), and promoting a secure and resilient domestic drone ecosystem.

To achieve these goals most effectively and without inadvertently creating negative consequences for trusted drone industry manufacturers and operators, the CDA respectfully

¹ The CDA is the leading advocacy organization representing domestic and allied commercial UAS and counter-UAS systems manufacturers and operators in the United States. We focus on restoring U.S. leadership in commercial drones, buttressing the domestic drone industrial base, and enabling scaled operations of commercial drones nationwide. Learn more at www.commercialdronealliance.org.

² See Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, ET Docket No. 21-232, *Third Report and Order and Third Further Notice of Proposed Rulemaking*, FCC 26-50 (rel. July 23, 2026).

offers a few important modifications to the Commission’s proposals. The Commission should utilize a more surgical approach in revising its equipment authorization program to strengthen U.S. national security while promoting domestic economic strength, competitiveness, and innovation in the UAS industry. Specifically, the Commission should:

1. Reduce unnecessary bureaucratic red tape by requiring equipment certification only for equipment posing meaningful national security risk;
2. Not require disclosure of hardware bill of materials (“HBOMs”) and software bill of materials (“SBOMs”) as part of the equipment certification process, which would slow the pace of American innovation;
3. Codify clear definitions of “produced in a foreign country” and “UAS critical components” to align with the Commission’s existing interpretations of these terms;
4. Provide safe harbors or exemptions for companies that demonstrate their products do not pose national security risks; and
5. Adopt reasonable implementation timelines that will help the American drone industry lead globally.

Adopting these recommendations will help the Commission advance American drone dominance while furthering its important and ongoing efforts to mitigate national security threats in the communications supply chain.

II. THE COMMISSION SHOULD PRESERVE THE BENEFITS OF ITS LONGSTANDING AND EFFICIENT EQUIPMENT AUTHORIZATION PROCESS FOR TRUSTED MANUFACTURERS.

A. An Across-the-Board Certification Requirement for the UAS Sector Would Burden American Manufacturers and Weaken the Domestic Drone Industry’s Global Competitiveness.

The Commission proposes to amend section 2.907(c) of its rules³ to require any device from a Covered List sector to undergo the certification process for equipment authorization, even if the device would be eligible for authorization through the Supplier’s Declaration of

³ See 47 C.F.R. § 2.907(c).

Conformity (“SDoC”) process or otherwise exempt.⁴ The Commission should modify this proposal to ensure that American drone companies are not subject to regulatory burdens that would impede industry growth and innovation.

Requiring certification for all devices in Covered List sectors would impose substantial additional costs, regulatory burdens, and delays on American UAS manufacturers, regardless of actual risk level, while offering little corresponding national security benefit. Because certification is more costly and time-consuming than the SDoC process, an across-the-board requirement for the UAS sector would compel manufacturers to shift resources away from development and innovation efforts and extend the time to bring products to market. Such a requirement would also divert Commission resources from examination and scrutiny of manufacturers and products that pose a real and present threat to American security. Requiring certification would impede the nimbleness and flexibility that American manufacturers need to compete effectively in a highly competitive global marketplace—including with manufacturing giants in China. The Commission should avoid requiring certification across the board, as doing so would needlessly create a substantial financial and regulatory burden on all UAS, including those manufactured in America.

To avoid these harmful impacts to the American drone industry, the Commission should instead pursue more targeted solutions. For example, the Commission could mandate that UAS produced in foreign adversary countries or by foreign entities of concern must obtain equipment certification. The Commission could also consider whether it can achieve its transparency and oversight objectives by requiring registration of products authorized via SDoC, as the

⁴ See *FNPRM* ¶ 154.

Commission proposes in the *FNPRM*.⁵ Registration, along with a streamlined process for revoking equipment authorized on the basis of improper declarations, would provide the necessary oversight without the costs and significant bureaucratic delays to innovation associated with full certification.

B. The Commission Should Preserve Manufacturers' Ability to Rely on Pre-Certified Modules.

To ensure that American companies can continue to innovate at a rapid pace, the Commission should also preserve the modular certification framework on which many American UAS manufacturers rely for efficient product development and market entry. Host products should still have the option to integrate pre-certified modules without the need to undergo certification themselves.⁶ The module itself is already subject to the rigorous certification process, effectively protecting against security risk. If the module continues to operate under the conditions for which it was certified, requiring the host to recertify the transmitter would simply duplicate the compliance showing that was already made, adding unnecessary regulatory red tape that threatens to delay innovation and time to market for cutting-edge, domestically produced technologies to the American public.

III. THE COMMISSION SHOULD NOT REQUIRE HBOM AND SBOM DISCLOSURES AS PART OF THE EQUIPMENT CERTIFICATION PROCESS.

The Commission seeks comment on whether manufacturers applying for equipment certification should be required to provide detailed HBOMs and SBOMs at the time of application and update the Commission with any changes to that information throughout the

⁵ See *id.* ¶ 213.

⁶ See Transmitter Module Equipment Authorization Guide, Knowledge Database Publication, Federal Communications Commission, Office of Engineering and Technology (Nov. 15, 2024), <https://tinyurl.com/y98psf4h>.

product's lifecycle.⁷ Alternatively, the Commission asks whether it should apply this new requirement only to devices in Covered List sectors, such as UAS.⁸

The Commission's national security goals can be achieved through a more tailored approach that does not impose undue burdens on the American drone industry. The CDA urges the Commission to decline to require HBOMs and SBOMs for UAS sector applicants seeking equipment certification for the following reasons.

First, the proposal to require HBOMs and SBOMs raises substantial confidentiality and cybersecurity concerns. HBOMs and SBOMs contain large amounts of proprietary and sensitive information, some of which may constitute valuable intellectual property ("IP"). The Commission should consider that its collection, dissemination, and storage of this detailed information could itself pose cyber risk. Unauthorized access to or inadvertent disclosure of this sensitive information could result in reverse engineering, disclose proprietary supply chain information that is ordinarily maintained in controlled and confidential environments, or enable bad actors to target a company's suppliers for security vulnerabilities and opportunities to introduce malware or surveillance capabilities into critical components. Companies should not be compelled to produce this information without firm assurances from the Commission that the information will be kept confidential and maintained in a secure environment.

Second, an HBOM/SBOM requirement would impose significant costs and delays on American UAS manufacturers, while providing little incremental value in advancing the Commission's national security objectives. Foreign-produced UAS are already barred from

⁷ See *FNPRM* ¶ 142. Applicants would be required to identify detailed supply chain information, including "the producer and place of production of the device itself, the producer of each component, the location of each component's production, and the percentage of component value associated with each production location." *Id.*

⁸ See *id.* ¶ 144.

receiving FCC equipment authorizations as Covered List equipment.⁹ As a result, the burdens associated with this proposal would fall primarily on American UAS manufacturers seeking authorization for eligible equipment. Collecting, validating, and maintaining this information would require significant engineering, procurement, and compliance resources. Compliance would require investment in new supplier management systems, engineering support, procurement resources, outside legal review, and periodic audits. Overall, increased compliance costs on U.S. companies are likely to slow product development, delay product launches, and lengthen certification timelines, thereby harming the drone industry’s ability to compete—and with it, American drone dominance.

Further, the requirement would not be a one-time compliance exercise, but continuous. The Commission proposes to require manufacturers to update HBOM and SBOM submissions to reflect every change throughout their product’s lifecycle. This ongoing regulatory burden could delay product improvements, increase compliance costs, and even discourage making changes to already-authorized devices that would enhance performance, reliability, security, or competitiveness.

Third, obtaining HBOM and SBOM information would require extensive supplier outreach. Drone manufacturers, like all complex product manufacturers, may lack direct contractual relationships with second-, third-, and fourth-tier suppliers. As a result, obtaining accurate producer and origin information would be impracticable or even impossible in some cases. For example, requiring applicants to identify the percentage of component value

⁹ See List of Equipment and Services Covered By Section 2 of The Secure Networks Act, Federal Communications Commission, <https://tinyurl.com/3s8x6ta2> (updated Aug. 21, 2026); 47 C.F.R. § 2.903(a).

associated with each production location is subjective, and suppliers may be unable or unwilling to share this information with drone companies.

Fourth, these burdens are not merited, as HBOMs and SBOMs may not offer meaningful or actionable information on the device’s security risk. For connected devices, factors such as the technology’s cybersecurity architecture, data-handling practices, remote-access protections, and other risk mitigations may provide more relevant information. Detailed component-level reporting is also unnecessary because applicants can be held accountable through other means, such as certifications and attestations. For example, the Commission can require applicants to certify compliance with its rules and provide representations regarding the origin of relevant equipment and components without mandating the submission of extensive HBOM and SBOM information. The Commission should implement a more targeted approach to addressing risk through its certification requirements, so as to avoid unintended negative consequences for American manufacturers and the drone industry.

If an HBOM requirement is nonetheless adopted, the Commission should not require applicants to provide granular information about subcomponents. For example, semiconductor design information should be excluded as modern semiconductors are highly integrated, multilayered components that incorporate IP, design elements, and functional building blocks drawn from numerous sources and refined through iterative innovation. Given the scale and complexity of subcomponent supply chains, for drones as well as any modern “smart” device, tracing and auditing development and design inputs would be burdensome, administratively impractical, and difficult to verify, while providing little corresponding value in advancing the Commission’s national security objectives.

IV. THE COMMISSION SHOULD ESTABLISH CLEAR AND WORKABLE DEFINITIONS OF KEY COVERED LIST TERMS.

A. The Commission Should Adopt Its Proposed Definition of “Produced in a Foreign Country.”

The CDA supports the FCC’s proposal to define “produced in a foreign country” as any equipment that does not qualify as a “domestic end product” as defined in 48 C.F.R. § 25.101(a)(1).¹⁰ Under this “Buy American standard,” manufacturers have a clear compliance benchmark. This certainty is needed, as manufacturers are making long-term sourcing, investment, and production decisions today based on the Commission’s existing rules.

B. The FCC Should Adopt a Revised Version of Its Proposed “Produced By” Definition.

The CDA supports the Commission’s proposal to interpret a device as “produced by” an entity when that entity exercises substantial responsibility for, or control over, a major stage of the process by which the device comes into existence. The CDA also agrees that a device may appropriately be considered “produced by” more than one entity where multiple parties exercise such responsibility or control. The Commission should not, however, extend the definition to encompass design or development activities occurring abroad.¹¹ Treating equipment as foreign-produced merely because some design or development activities occurred abroad would depart significantly from the ordinary meaning of “produced in” and could have significant unintended consequences for U.S. manufacturers. U.S. companies with global operations may develop drones through cross-border collaboration, including with allied countries. They may also simply conduct development work through multinational collaboration teams or leverage

¹⁰ *FNPRM* ¶ 198.

¹¹ *See id.* ¶¶ 198-199.

R&D work from overseas divisions of the company. The Commission should not adopt a definition that penalizes such arrangements.

Further, the Commission should make clear that the definition of “produced by” does not extend to routine commercial relationships, participation in standards-development activities, licensing arrangements, or other commonplace business practices that facilitate innovation, interoperability, and specialization throughout the global technology ecosystem. Many of these efforts contribute to American technological leadership and should be encouraged rather than blocked. Often, these arrangements reflect longstanding and pro-competitive commercial practices that enable companies to leverage specialized expertise, improve efficiency, increase consumer choice, and accelerate innovation. The Commission should therefore ensure that such relationships are not inadvertently swept within the scope of the “produced by” definition.

C. The Commission Should Adopt Its Proposed Definition of “UAS Critical Components.”

The CDA supports the Commission’s proposal to codify its existing definition of “UAS critical components,” drawn from the National Security Determination (“NSD”), which added foreign-produced UAS and UAS critical components to the Covered List, and the FCC’s subsequent guidance explaining that “UAS critical components” mean components designed and intended primarily for use in UAS.¹² Additionally, the Commission should continue to focus its enforcement on its statutory authorities to regulate devices that transmit radio frequencies rather than simple mechanical components. Although implementing the current restrictions has been challenging, the U.S. drone industry has, over the last eight months, adapted and invested significant resources to establish domestic sources for UAS critical components. Manufacturers

¹² *Id.* ¶¶ 202-203 (proposing to codify the FCC’s existing interpretation of “UAS critical components”). *See also Covered List FAQs: UAS and UAS Critical Components*, Federal Communications Commission, <https://tinyurl.com/2s42ysn2> (last visited September 8, 2026).

have made substantial operational, supply chain, and financial investments in reliance on the current definition of “UAS critical components.” Changing that definition now would undermine those efforts and the progress the drone industry and others have made to comply with the Commission’s latest requirements. Companies would be forced to once again restructure sourcing arrangements, and manufacturers in the drone industry that have already invested significantly to align with the existing framework would face significant, and in some cases devastating, financial consequences. The current definition appropriately targets the FCC’s national security concerns by scoping in components specifically designed for UAS rather than general purpose items that were never implicated by the NSD. Accordingly, the Commission should maintain its current definition.

V. EXEMPTIONS, SAFE HARBORS, AND REASONABLE IMPLEMENTATION PERIODS ARE KEY TO SUPPORTING DOMESTIC MANUFACTURING AND ACHIEVING AMERICAN DRONE DOMINANCE.

As it moves forward with making modifications to the equipment authorization program, the Commission should make safe harbors or exemptions from new requirements and restrictions available to qualified UAS companies that can demonstrate that their products or operations are secure and trustworthy. Specifically, the Commission should make permanent its current exemptions from the Covered List for UAS and UAS critical components that have been granted a Conditional Approval, are included on the Blue UAS Cleared List, or qualify as “domestic end products” under the Buy American standard. Extending the duration of these exemptions would allow the Commission to focus its oversight and enforcement resources on higher-risk equipment while providing companies the certainty they need to invest in domestic production capacity.

The Commission should also exempt equipment used by Part 135/108 FAA-certificated manufacturer-operators¹³ and vertically integrated domestic manufacturer-operators who do not sell UAS to third parties. Much of this equipment has undergone extensive testing and safety review by the FAA for civilian use, with strict cybersecurity requirements applied, and has been proven to present no national security vulnerabilities. Additionally, Part 135 operators are required to have economic authority to operate in the United States from the Department of Transportation, proving their domestic financial qualifications. As a matter of principle, U.S.-based companies that source critical components from suppliers in the United States or non-adversarial countries should not be subject to the same requirements as foreign adversary manufacturers.

Finally, the Commission seeks comment on the appropriate transition periods and timelines for complying with its proposals if adopted.¹⁴ While domestic manufacturing initiatives are underway, much of the global UAS supply chain today remains heavily concentrated outside of the United States.¹⁵ Transitioning to U.S.-made UAS and UAS critical components will require time and investment, including capital, workforce development, testing, certification, procurement, and deployment. The CDA is supportive of these efforts and the growth of the U.S. component-manufacturer marketplace, but cautions that burdensome new requirements could harm the same domestic component industrial base that the Commission seeks to support, as aggregate demand for drone technology may simply decline.

¹³ See 14 C.F.R. Part 135.

¹⁴ See *FNPRM* ¶¶ 146, 158, 207.

¹⁵ See Josh Chin et al., *The U.S. Wants to Break China's Drone Dominance. Here's Where It Will Struggle.*, Wall St. J. (May 2, 2026), <https://tinyurl.com/484jb7a8>.

Defense funding alone cannot sustain a robust domestic industrial base over the long term. It is therefore vital to ensure that commercial demand for domestic dual-use drone technology in the United States remains high enough to support the investment and financial security of domestic component manufacturers in the years to come. Costs for domestic products will naturally be higher in the short term as manufacturing capacity grows, making it even more important to give domestic end users, including both operators and platform manufacturers, sufficient runway to plan for any necessary transitions. For example, the Department of War's Office of Strategic Capital's recent efforts to expand access to financing for strategic manufacturing and supply chain investments can help accelerate the development of domestic production capacity and reduce reliance on foreign suppliers over time, which the CDA greatly appreciates.¹⁶ As these investments begin to strengthen the industrial base, a predictable transition period will remain essential to avoid disruptions to current critical operations.

Accordingly, any new requirements should have effective dates that align with the timelines for domestic alternatives being brought to market with sufficient quality and in sufficient quantities to meet American industry needs. Appropriate transition periods are critical to minimize disruption to the U.S. economy and innovation.

VI. CONCLUSION

The CDA supports the Commission's efforts to protect national security and achieve American drone dominance. A surgical approach that targets high-risk equipment, as discussed herein, will best advance these objectives while preserving U.S. economic competitiveness,

¹⁶ See Press Release, Off. Strategic Cap., U.S. Dept. War, The Office of Strategic Capital Signs \$820 Million Conditional Loan Commitment with Performance Drone Works to Expand Domestic Drone Component Manufacturing (July 31, 2026), <https://tinyurl.com/msubwzds>.

innovation, and leadership, including in the UAS sector. The CDA commends the Commission for its efforts on this important issue and appreciates the opportunity to contribute.

Respectfully submitted,

Katy Milner
HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
katy.milner@hlc.com
+1 202-637-6432

/s/ Lisa Ellman
Lisa Ellman
Chief Executive Officer
COMMERCIAL DRONE ALLIANCE
555 Thirteenth Street, NW
Washington, DC 20004
lellman@commercialdronealliance.org

September 8, 2026