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

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

REPLY COMMENTS OF THE COMMERCIAL DRONE ALLIANCE

I. INTRODUCTION AND SUMMARY

The Commercial Drone Alliance ("CDA") respectfully submits these reply comments in response to the Federal Communications Commission's ("FCC" or "Commission") *Further Notice of Proposed Rulemaking* ("FNPRM") on strengthening the Commission's equipment authorization program for covered equipment and related components.[1]

The CDA is an independent non-profit organization composed of leading members of the U.S. commercial drone industry, including companies that design, manufacture, and operate unmanned aircraft systems ("UAS") and the associated technology for autonomous capabilities. We bring together commercial drone operators and end-users, manufacturers, service providers, advanced air mobility companies, drone security companies, and vertical markets, including oil and gas, precision agriculture, construction, security, communications technology, infrastructure,

[1] *See Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket No. 21-232, Second Report and Order and Second Further Notice of Proposed Rulemaking (rel. Oct. 29, 2025). Unless otherwise specified, all comments referenced in these reply comments were filed in ET Docket No. 21-232 on January 5, 2026.

newsgathering, filmmaking, and more.[2] We advise and educate all levels of government and the public on policies essential to enable U.S. leadership in commercial drones, and on the benefits arising from their safe and responsible use.

Strengthening the Commission's equipment authorization process is critical to ensuring vulnerabilities are not introduced into U.S. communications infrastructure, including UAS technologies. Legitimate national security threats persist, but overly broad restrictions could limit access to critical components needed for key national security and commercial technologies, including UAS, and risk undermining Commission and executive branch goals.[3] As the record in this proceeding shows, a targeted, risk-based approach can protect U.S. national security while preserving domestic economic strength, competitiveness, and innovation. Specifically, the Commission should:

1. Craft changes to its equipment authorization process to target problematic equipment and components based on their functionality;

2. Establish appropriate transition periods, in coordination with industry; and

3. Provide safe harbors or exemptions for companies that demonstrate their products do not pose security risks.

II. THE COMMISSION'S PROPOSAL IS OVERLY BROAD AND RISKS SIGNIFICANT UNINTENDED CONSEQUENCES.

National security threats continue to target U.S. communications networks and supply chains, and the CDA fully supports the Commission's efforts to address those risks. The Commission's existing rules prohibit authorization of devices containing modular transmitters on the Covered List where the transmitter itself would qualify as covered equipment,[4] and the

[2] Learn more at www.commercialdronealliance.org.

[3] *See, e.g.*, Executive Order 14307, "Unleashing American Drone Dominance," 90 FR 24727 (June 6, 2025).

[4] *See FNPRM* ¶ 28.

FNPRM proposes to expand this restriction to additional component parts.[5] As drafted, the proposal extends well beyond high-risk equipment and components, risking significant negative downstream impacts for domestic manufacturers and end users, and potentially diluting both government and industry resources and focus from true threat assessment.

The proposal would impose substantial burdens on domestic manufacturers, threatening U.S. economic strength, competitiveness, and innovation.[6] Drones and other equipment contain hundreds of individual components, each of which would need to be traced to its original source. The difficulties in tracing component parts were highlighted in the record:

- Garmin explains that "it would be a herculean undertaking, if possible at all, to trace the source of each component's design, manufacture, and importation."[7]
- Information Technology Industry Council explains that "[u]nlike modular transmitters, most components have no standardized identification, bill of materials structure, or traceability across supply chains," making it "extremely complex (to the point of being practically impossible) to identify the origin of all subcomponents."[8]
- NTCA emphasizes that the proposal would impose "substantial financial and staffing costs on smaller providers."[9]

Further, manufacturers cannot reasonably be expected to certify component tracing compliance where certification depends on supplier disclosures beyond their control. Information from

[5] *See id.* ¶ 58.

[6] *See, e.g.*, Comments of MEMA, The Vehicle Suppliers Association at 10 ("MEMA Comments") (warning "[u]nilateral restrictions that diverge from international norms risk disadvantaging U.S.-based suppliers and may accelerate fragmentation of global technology ecosystems."); Comments of USTelecom – The Broadband Association at 6 (explaining that harms include "impact[ing] U.S. economic competitiveness globally, where U.S. companies compete with [ ] economic adversaries for global device market share").

[7] Comments of Garmin International, Inc. at 8 ("Garmin Comments"). *See also* Comments of Sony Group Corporation at 1 ("Sony Comments").

[8] Comments of the Information Technology Industry Council at 4 ("ITI Comments").

[9] Comments of NTCA – The Rural Broadband Association at 10.

suppliers may be unavailable, incomplete, or erroneous.

The proposal also risks harms to end users, including critical U.S. military and economic interests. Replacing restricted components with functionally equivalent alternatives from trusted vendors poses challenges. In some cases, substitutes may exist only at higher costs, increasing prices throughout the supply chain. In other cases, functionally equivalent alternatives may not exist at all. Some manufacturers might be forced to turn to lower-quality components, but such substitutions pose reliability, safety, security, and performance risks for military, public safety, and critical infrastructure applications. For the drone industry, this would undermine the benefits we provide the American public, including enhancing worker and public safety, fighting wildfires, strengthening border security, promoting infrastructure resilience, expanding rural access to consumer goods and healthcare supplies, securing our homeland, and facilitating emergency response.

In addition, the proposal would strain Commission and certification lab resources. Banning low-risk components would expand the scope of Commission enforcement, burdening Commission resources. Certification bodies would face similar resource constraints, potentially delaying the timely certification of even fully trusted equipment.[10] These effects would hinder U.S. innovation, including in the drone industry, and harm domestic manufacturers' global competitiveness.

[10] Sony explains that certification bodies would be "expected to validate the provenance and compliance status of all component information by tracing through supply chains—requirements far beyond today's responsibility boundaries." Sony Comments at 2. MEMA notes that expanded authorization triggers "would increase demand on [TCB's] limited resources, lengthening certification timelines and delaying deployment of compliant technologies." MEMA Comments at 9.

III. THE COMMISSION SHOULD ADOPT A TARGETED, RISK-BASED APPROACH FOCUSED ON COMPONENTS THAT POSE LEGITIMATE RISKS.

The Commission should adopt a targeted, risk-based approach that addresses problematic equipment based on functionality.[11] The FCC should direct its efforts at components that present high risks, including data exfiltration and remote access control, which represent the two primary areas of risk associated with foreign adversary information and communications technology services integral to UAS technology. Many of the components in UAS do not present any security risk because they are not linked to the digital elements that handle processing, data management, or autonomous capabilities for drones. Often, imported components are fasteners, bolts, wiring, or basic motors that need not face restrictions.

A targeted approach would also enable more effective compliance. The Commission should avoid repeating the mistakes of the Biden Administration's Broadband Equity, Access, and Deployment program's Build America, Buy America restrictions, where impossible to comply with procurement rules were eventually pared back with a five-year waiver.[12] The Commission and the Trump Administration can proactively avoid these mistakes by engaging with industry, considering supply chain realities, and adopting a more targeted approach.

While foreign adversary-based bans seem reasonable initially, they have limitations. First, geopolitics are constantly changing, and the list of foreign adversaries is not static; countries trusted today could be designated tomorrow. Second, relying only on foreign adversary status creates new vulnerabilities, as companies in designated countries could simply relocate

[11] *See, e.g.*, Comments of CTIA ("CTIA Comments"); Comments of Consumer Technology Association ("CTA Comments"); Garmin Comments; MEMA Comments; NTCA Comments; Comments of the Telecommunications Industry Association.

[12] *See* Dep't of Com., *Limited General Applicability Nonavailability Waiver of the Buy America Domestic Content Procurement Preference as Applied to Recipients of Broadband Equity, Access, and Deployment Program* (Feb. 22, 2024), https://tinyurl.com/22xvrj7j.

operations or funnel banned equipment into the United States through back doors. Third, blanket bans risk creating a false sense of security that true bad actors can exploit. For these reasons, the Commission should rely on technical security determinations, rather than foreign adversary status, in determining whether to ban equipment.

IV. IF THE COMMISSION ADOPTS ITS PROPOSALS, IT SHOULD IMPLEMENT SUFFICIENT TRANSITION TIMEFRAMES BASED ON INDUSTRY INPUT.

The FNPRM seeks comment on the appropriate transition period for implementing a prohibition on equipment containing certain component parts.[13] Commenters agree that transition periods must be sufficient to account for the practical realities of compliance and permit technology companies to continue to meet the needs of their customers. If the Commission adopts its proposals, transition timeframes should provide enough time for supply chain and operational adjustments, and the Commission should work with industry on determining appropriate time periods.

Component-level prohibitions would require "re-design, re-sourcing, re-qualification, and re-certification of equipment, new contracts with alternative suppliers, and logistical planning for gradual field replacement."[14] A component-level sourcing requirement "could require a major redesign of the entire product, involving substantial cost and years to complete."[15] These tasks would have an additional layer of complexity for the drone industry, which must engage with the Federal Aviation Administration on drone design and safety (and re-engage when changes are made).

The CDA joins commenters in urging the Commission to consider industry input in

[13] *See FNPRM* ¶ 61.

[14] ITI Comments at 5.

[15] CTA Comments at 7.

establishing the transition periods.[16] The Commission lacks full visibility into sector-specific supply chain challenges, including sourcing options, manufacturing schedules, and impacts on end users. Without industry input, transition periods could be set too short, causing supply chain disruptions, higher costs, and unintended risks to U.S. national and economic security. Industry input can help ensure the timeframes adopted promote compliance while minimizing negative impacts.

V. SAFE HARBORS OR EXEMPTIONS SHOULD BE AVAILABLE TO COMPANIES MEETING CERTAIN CRITERIA.

Safe harbors or exemptions to the Commission's rules should be available to companies if they are able to demonstrate minimal or no risk to national security, even if their products contain components of concern. Safe harbors allow the industry and Commission to focus efforts on high-risk components. Companies could be eligible for safe harbors or exemptions by demonstrating:

1. Components are non-sensitive (e.g., screws, paint, or other non-critical parts);
2. The company has robust controls or mitigation strategies (such as vertical integration of manufacturer and operator, tightly controlled data pipelines, limits on external access, encryption, or redundancies implemented) to prevent compromise of the components by malicious actors; or
3. Certification from a qualified federal agency (e.g., Department of Homeland Security, Department of War, Department of Commerce) confirming that products present no national security risk.

VI. CONCLUSION

The CDA supports the Commission's efforts to strengthen its equipment authorization process with respect to covered equipment and agrees that eliminating national security risks in U.S. communications networks and equipment requires U.S. manufacturers to reduce reliance on

[16] *See* CTIA Comments at 15.

foreign adversary technology. By making the changes to its proposals discussed herein, the Commission can further national security objectives while avoiding unintended negative consequences to U.S. economy, national security, and innovation, including in the UAS sector.

Restrictions on insecure equipment are critical, but they are only one part of the solution. Key consumer electronics components have been produced overseas for half a century, creating significant challenges for U.S. manufacturers seeking to compete. Domestic manufacturers face challenges such as higher labor and material costs, a shortage of skilled labor, and a changing regulatory environment. The CDA encourages the Administration to complement the equipment authorization restrictions alongside incentives (such as tax credits and subsidies) to provide companies the support needed to make these critical transitions. The CDA commends the Commission for its efforts on this important issue and appreciates the opportunity to contribute.

Respectfully submitted,

/s Katy Milner

Katy Milner
FCC Counsel to CDA
HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
+1 202-637-6432

February 2, 2026