U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

March 25, 2025

Ms. Elizabeth Cannon
Executive Director
Office Of Information and Communications
Technology And Services
Bureau of Industry and Security
U.S. Department of Commerce

Re: Comments on the Bureau of Industry and Security, U.S. Department of Commerce; Advance Notice of Proposed Rulemaking; Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems (Docket No. 241213-0327)

Dear Director Cannon:

The U.S. Chamber of Commerce (the "Chamber") welcomes this opportunity to comment on the Commerce Department's Bureau of Industry and Security's ("BIS") advanced notice of proposed rulemaking ("ANPRM") on *Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems*.[1]

The Chamber applauds BIS for issuing an ANPRM to address the risks posed by untrusted unmanned aircraft systems ("UAS" or "drones") to the United States. The national security objectives of the ANPRM align with the Chamber's consistent advocacy for narrowly tailored and properly scoped measures to safeguard national security without unnecessarily disrupting normal business activities.

Although we believe UAS will have tremendous benefit, we understand the need for safeguards. Further, the Chamber appreciated the thoughtful and deliberative approach that BIS pursued in its final rule on connected vehicles, and we encourage BIS to apply the same deliberative and consultative approach in this rulemaking to mitigate national security threats in the UAS supply chain.

Overall, we urge BIS to appropriately scope UAS restrictions, create processes for general and specific authorizations, consider marketplace impacts of regulations, ensure intragovernmental coordination, and pursue policies that bolster the UAS industry.

I. Appropriately Scope Restrictions on UAS Systems and Components

[1] Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems, Advance Notice of Proposed Rulemaking, Docket No. 241213-0327 (rel. Jan. 3, 2025) ("ANPRM").

The Chamber believes BIS should pursue a tailored and risk-based approach for UAS ICTS restrictions.

First, BIS should adopt the definition of UAS consistent with the FAA's definition in 49 U.S.C. 44801(12). This definition is well known to nearly all stakeholders considering it is the basis of FAA regulation of UAS. Moreover, this definition was included in American Security Drone Act ("ASDA"), which aims to achieve a similar objective to BIS' ANPRM.[2]

Second, BIS should pursue a system-level focus to apply restrictions to UAS generally as well as security sensitive component parts. BIS appropriately recognized the threats posed by foreign adversary UAS and focusing on UAS generally will cover known entities of concern and the risks they pose to the United States.

Third, we encourage BIS to consider risk-based restrictions on security sensitive components when the capabilities and use case of the UAS indicate a potentially high security threat and other mitigation protocols are deemed insufficient to protect national security. These may include communications links and the controller but exclude passive components. This would align with existing laws such as the ASDA, which tailors restrictions to components that pose an unacceptable risk to national security.[3] In establishing component restrictions, BIS should clearly identify criteria that need to be met, as well as the specific products and components within their purview. This identification need not identify products from specific suppliers but rather should list well-defined categories of UAS products and components.

II. Create a Process for Specific and General Authorizations

BIS is seeking feedback on whether a process should be created to "request specific authorization to engage in certain transactions involving foreign adversary ICTS" in the event appropriate mitigations are in place. The Chamber supports creating such a process to accommodate mitigation measures consistent with national security. objectives This should align with agency guidance on threats posed by foreign adversary ICTS such as Department of Homeland Security's *Cybersecurity Guidance: Chinese-Manufactured UAS*, which identifies potential mitigation measures to improve an organization's security.[4]

For example, BIS should examine how compartmentalization can be utilized in the authorization process. Compartmentalization can be used by a manufacturer to protect against third-party interference with UAS operations. If the entities supplying distinct hardware components do not have access to the software running the aircraft itself, a firewall can be created to protect the operations.

---

[2] National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, § 1822 (2024).
[3] *Id*.
[4] CYBERSEC, AND INFRASTRUCTURE SEC. AGENCY AND FED. BUREAU OF INVESTIGATION, CYBERSECURITY GUIDANCE: CHINESE-MANUFACTURED UAS (2024).

III. Provide a Phase-In Period

BIS appropriately recognizes that regulations have the potential to pose significant economic impacts on industry end-users of drones. BIS should take a risk-based approach that phases in restrictions and harmonizations its approach with other similar security frameworks.

BIS should recognize that drones are used on a wide range of industry sectors including transportation (e.g. construction, engineering, rail, manned aviation), retail, delivery services, insurance, security, agriculture (e.g. crop monitoring, irrigation, pest control), energy (electric utilities, oil and gas production and distribution), telecommunications and broadband, media, film production, public safety and law enforcement, and many others. For these users, drones are capital investments to address specific requirements, and time is necessary for the marketplace to change.

To address marketplace realities, Chamber believes that any new ICTS requirements from BIS provide an transition period comparable to that provided in the Connected Vehicles rule. The Connected Vehicles rule provides a two-year transition period for software and three to four years for hardware components from the publication date of the final rule.[5] This will provide a clear market signal for drone and drone component manufacturers to adjust to end-user requirements and for end-users to adjust their supply chains. This will help minimize disruptions to end-user operations and the UAS supply chain while still achieving the objective of the ANPRM.

IV. Ensure Inter-Governmental Coordination and Strategy on UAS Security and Innovation policy

We recognize BIS' focus is to craft an ICTS rule focused on UAS. However, the Department of Commerce and policymakers should be aware that additional actions are necessary to pursue in concert with an ICTS rule to achieve the twin objectives of UAS security and American leadership in UAS innovation. We encourage the U.S. government to coordinate and advance a multi-pronged effort to achieve these objectives.

Restricting the import of untrusted UAS is only one pillar of an effective UAS security regime. Even if untrusted UAS transactions were restricted under an ICTS rule, other drone security risks remain that require action by policymakers. This includes the malicious, careless, and clueless use of drones to critical infrastructure facilities, mass gatherings and sporting events, aviation facilities, and other sensitive sites. To address these risks, the FAA should advance a rulemaking under Section 2209 of the FAA Extension, Safety, Security Act of 2016 to establish a national system of no-fly zones around critical infrastructure.[6] Further, Congress should enact a comprehensive counter-drone framework to protect critical infrastructure, mass gatherings, and aviation facilities from unauthorized UAS operations. At present, only four

[5] 15 CFR 791.300-21.

[6] FAA Extension, Safety, and Security Act of 2016, Pub. Law No: 114-190, § 2209, 130 Stat. 634 (2016).

federal agencies have the legal authority to utilize counter-drone detection and mitigation technologies to protect sensitive facilities and operations. This creates significant security gaps that can only be resolved by legislative action to expanding detection and mitigation authorities to other key federal government agencies and functions that do not possess these authorities, detection authorities for private sector entities, and limited mitigation authority for state and local law enforcement agencies through a pilot program.

As previously discussed, phased-in ICTS UAS restrictions will provide a clear market signal to make the necessary adjustments to the UAS marketplace. However, the U.S. government can augment and ease this adjustment through pro-competitive and affirmative steps to bolster the market for trusted UAS technologies. This includes [establishing a "rip and replace" program for industry end-users impacted by restrictions, pursuing deregulatory actions at the Federal Aviation Administration to enable routine, complex UAS operations, and facilitating market access for UAS products and components with trusted international partners though export promotion, reducing of tariffs and other barriers to trade, and pursuing select practical end effective tools to bolster manufacturing.

Finally, the Chamber seeks clarification from BIS about how this rulemaking will interact with Section 1709 of the Fiscal Year 2025 National Defense Authorization Act.[7] Section 1709 directs the Administration to determine if the drone industry of the People's Republican of China poses an unacceptable risk to the United States, and if no determination is made, the Federal Communications Commission would be directed to add communications equipment from those entities on the FCC's covered list.[8] We expect that there may be overlap between BIS' UAS ICTS process and a potential FCC process. The FCC, Department of Commerce, and other relevant agencies should coordinate to provide a consistent approach, so industry has a clear understanding of any restrictions.

V. Conclusion

The Chamber appreciates the opportunity to provide these comments and welcomes continued engagement with BIS and the U.S. government on these issues to ensure the promotion of trusted US unmanned aviation leadership.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center

[7] Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. Law 118-159, § 1709 (2025).
[8] *Id*.