Articles + Publications | January 9, 2025

Drone Alert! BIS Seeks Comments From Industry on How to Secure the Unmanned Aircraft Systems Supply Chain

WRITTEN BY

Peter E. Jeydel | Ryan Last

The U.S. Department of Commerce’s Bureau of Industry and Security (BIS) issued an Advance Notice of Proposed Rulemaking (ANPRM) on January 3, 2025, seeking public input to inform the potential development of a rule to secure the information and communication technology and services (ICTS) supply chain for unmanned aircraft systems (UAS), commonly known as drones.

Stakeholders with any exposure to the UAS supply chain, including research organizations, manufacturers of components or larger systems, distributors, users, and others, should follow these developments and consider submitting comments.

Background and Purpose

The rapid development of advanced technology has made UAS commonplace across the U.S., but their proliferation and increasingly sophisticated capabilities have also raised national security concerns. BIS warns that foreign adversaries, particularly the People’s Republic of China (PRC), may exploit vulnerabilities in the UAS ICTS supply chain for malign purposes such as espionage or sabotage. The concerns include adversaries’ ability to gain remote access to or manipulate drones, potentially exposing sensitive U.S. data or compromising critical infrastructure.

This outreach by BIS on the potential regulation of UAS supply chain security is the latest in a string of recent rulemakings under the agency’s still relatively new ICTS authority. This authority was actually initiated under the first Trump administration, pursuant to Executive Order (EO) 13873, “Securing the Information and Communications Technology and Services Supply Chain.” However, it was only during the middle of the Biden administration that BIS assumed this mission, and the office director was only appointed last year.

Now that the ICTS office at BIS is fully up and running, the pace of its regulatory activity is accelerating, and one can expect an aggressive approach in this area under the coming Trump administration.

Key Details

The ANPRM outlines several areas where BIS seeks public feedback, including:

- <u>Definitions</u>: Feedback is sought on how UAS and related components should be defined to ensure clarity and precision in the expected regulations. For example, commenters could propose appropriate definitions for flight control systems, communication modules, or data storage devices, along with whether/how to exclude off-the-shelf parts or those that otherwise do not pose a significant security risk.

- Risk Assessment: BIS invites stakeholders to highlight scenarios in which UAS technology could present security risks, such as by enabling unauthorized access to U.S. critical infrastructure or sensitive data, or outline specific high-risk use cases, such as drones employed in military or law enforcement operations.

- Foreign Adversary Evaluation: Comments are requested on the risks posed by specific foreign adversaries. For instance, industry participants could provide evidence of supply chain dependencies on manufacturers in high-risk jurisdictions or offer perspectives on how the risk profiles of adversaries like the PRC differ from those of other countries.

- Approval Processes: BIS seeks feedback on potential mechanisms for requesting approval to engage in otherwise restricted ICTS transactions. A licensing and advisory opinion procedure was left out of BIS's recent final rule establishing the ICTS regulatory regime. Commenters might propose a fast-track review process for low-risk transactions, such as those involving academic research, or suggest criteria for exceptions, including the use of secure, independent audit trails for data access.

- Economic Impact: BIS is interested in understanding the potential economic implications of the proposed UAS regulations on different stakeholders. For example, drone manufacturers might detail the cost burden of shifting supply chains to avoid foreign adversary-linked components, while small businesses could discuss how compliance costs might affect their ability to remain competitive.

- Mitigation Measures: The agency is exploring feasible risk mitigation strategies to reduce vulnerabilities while avoiding outright prohibitions. Suggestions might include implementing robust encryption standards for data transmission, requiring firmware updates to be sourced from trusted suppliers, or mandating audits for suppliers in foreign jurisdictions.

Public Participation and Next Steps

BIS encourages stakeholders to provide comments by March 4. Comments can be submitted through the Federal eRulemaking Portal at https://www.regulations.gov under docket number BIS-2024-0058, or via email to UnmannedAircraftSystems@bis.doc.gov (include "RIN 0694-AJ72" in the subject line).

Conclusion

BIS is still at a relatively early stage in considering how to regulate the UAS sector for national security purposes and would welcome useful comments on any aspect of this expected rulemaking. Stakeholders should give serious consideration to engaging now, as it will become increasingly difficult to influence the process after it moves forward.

By engaging with BIS in a timely and thoughtful manner, industry participants can contribute to a balanced approach that mitigates security risks while supporting economic growth and technological innovation.

To learn more about the potential impacts of this expected rulemaking on your organization, or how to engage with BIS, please ?reach out to Pete Jeydel or Ryan Last.

RELATED INDUSTRIES + PRACTICES

- Corporate
- Sanctions + Trade Controls
- White Collar Litigation + Investigations