March 4, 2025

Submitted electronically via Federal eRulemaking Portal: www.regulations.gov

Docket Management System
Bureau of Industry and Security
U.S. Department of Commerce

Re: Commercial Drone Alliance Comments on the Bureau of Industry and Security, U.S. Department of Commerce Advance Notice of Proposed Rulemaking re: Foreign Adversary ICTS Integral to UAS Technology [Docket No. 241213-0327; RIN 0694-AJ72]

Dear Director Cannon:

The Commercial Drone Alliance ("CDA") appreciates the opportunity to comment on the Bureau of Industry and Security ("BIS"), U.S. Department of Commerce ("DOC") Advance Notice of Proposed Rulemaking ("ANPRM") titled "Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems," which was published in the Federal Register on January 3, 2025.[1]

The CDA is an independent non-profit organization led by key members of the commercial drone industry. The CDA actively participates in legislative, regulatory, and policy efforts to facilitate the safe and secure development and expansion of commercial drone operations. The CDA works with all levels of government to collaborate on policies for industry growth and educates the public on the safe and responsible use of commercial drones to achieve economic benefits and humanitarian gains. 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, newsgathering, filmmaking, and more.[2]

I. Expanding and Enabling the UAS Industry Unlocks Significant Benefits For All Americans

[1] https://www.federalregister.gov/documents/2025/01/03/2024-30209/securing-the-information-and-communications-technology-and-services-supply-chain-unmanned-aircraft

[2] Learn more at www.commercialdronealliance.org

Commercial unmanned aircraft systems ("UAS") provide extraordinary benefits to the American public—enhancing worker and public safety, fighting wildfires, promoting infrastructure resilience, expanding equitable and efficient access to critical supplies, securing our homeland, facilitating emergency response, supporting the U.S. economy, creating jobs, and generating tremendous economic value—all while ensuring America's global leadership in advanced aviation.

If the regulatory framework in the U.S. can keep pace with this rapidly evolving industry, UAS will unlock billions of dollars in economic growth over the next few years. There are many varying estimates of market potential, but the numbers are all large. The size of the commercial drone market—the fastest growing segment—is expected to reach $16 billion by 2025 and $29 billion by 2030.[3] Those figures represent only baseline estimates; other figures estimate a market size of $21 billion and $36 billion by 2025 and 2030, respectively. There also is significant potential for broad economic savings as a result of enterprise UAS operations. For example, the U.S. economy could save up to $920 million annually using drones to inspect energy utility infrastructure.[4] Economic benefits also can flow to local small businesses participating in UAS delivery programs. One study of UAS local delivery programs found that local participating retailers could each experience more than $200,000 a year in increased business opportunities, and local restaurants could generate up to $284,000 in additional sales, by expanding the footprint of serviceable customers.[5]

Drones also offer transformative benefits when used for public safety purposes, including the new paradigm of Drones as a First Responder (DFR), where drones are remotely operated to respond to emergency calls or crises. Public safety drones save lives by reducing emergency response times, providing critical situational awareness, and helping to de-escalate dangerous situations. Notably, several American UAS companies are currently driving innovation and supporting local first responder agencies across the country in this market. New York City, Oklahoma City, San Francisco, Las Vegas, and other large cities are performing DFR operations today using drones and software produced by U.S. companies.

Although these and other efforts are promising, the vast benefits of UAS have not yet been truly realized here in the United States. That is because regulatory uncertainty and the application of legacy crewed aviation rules have prevented scalable UAS operations and limited the integration of UAS into the national airspace system. Despite the best efforts of relevant offices at the Federal Aviation Administration (FAA) and across the Administration, the UAS industry continues to be held back by the application of incongruous approaches designed for crewed aircraft. One of the most important ways the U.S. Government can bolster the domestic UAS supply chain and mitigate risks of foreign adversary technologies is to create a flexible,

---

[3] Levitate Capital White Paper, Enterprise Market 2020 at 28.

[4] *Id.*, at 6.

[5] Sarah Lyon-Hill, et. al., *Measuring the Effects of Drone Delivery in the United States*, Virginia Tech Office of Economic Development and the Grado Department of Industrial & Systems Engineering (Sept. 2020), available at https://www.newswise.com/pdf_docs/160018187481745_Virginia%20Tech%20%20Measuring%20the%20Effects%20of%20Drone%20Delivery%20in%20the%20United%20States_September%202020.pdf (hereafter, Virginia Tech Drone Delivery Study).

performance-based regulatory framework for UAS use that incentivizes domestic and allied development and production of UAS technologies. The UAS Beyond Visual Line-of-Sight (BVLOS) Aviation Rulemaking Committee (ARC) submitted recommendations to the FAA for such a framework three years ago, and to date no proposal has been published by the FAA. Every additional day of continued delay in updating regulations to today's technologies puts the United States further behind our foreign adversaries in domestic technology production and increases the associated vulnerabilities.

II. Bolstering the UAS Supply Chain in Response to Potential Risks Posed by Foreign Adversaries without Introducing Overly Burdensome Unintended Consequences for the UAS Industry

The CDA supports BIS's interest in determining the technologies and market participants that may be most appropriate for regulation for undue risk pursuant to Executive Order 13873 titled ''Securing the Information and Communications Technology and Services Supply Chain" in order to protect U.S. national security interests. We understand that BIS is using this comment period to better understand and evaluate information and communications technology and services ("ICTS") that are "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries," as defined in the ANPRM.[6]

CDA supports responsible efforts to mitigate national security risks posed by UAS manufactured in adversarial nations, including the People's Republic of China (PRC). Congress, DOD, FBI, DHS, and others have expressed continued concern regarding risks associated with adversarial systems. We also recognize the realities of global supply chains, the complexity of transitioning sourcing strategies, and the need to ensure that any regulatory framework allows for the continued growth and competitiveness of the U.S. commercial drone operations industry and drone and component manufacturing. We urge any BIS regulation to balance these priorities and concerns in a way that strengthens national security without stifling domestic innovation.

Maintaining a strong and secure domestic UAS industry promotes competitiveness and protects national security. For this reason, the CDA has long advocated for enhanced support for domestic UAS manufacturing capabilities and supported efforts to ensure a robust and secure UAS supply chain. The federal government's actions must not only be punitive; the government must also take positive steps to support the domestic drone marketplace.

Finally, in addressing any identified risks we urge BIS to avoid unintended consequences for American and allied UAS companies that pose additional regulatory and policy hurdles that prevent scalable, safe, and secure commercial UAS operations in the United States.

III. Key UAS-Related Considerations for BIS as It Develops a Proposed Rule

This section addresses ANPRM questions 1, 3, and 5.

[6] https://www.federalregister.gov/documents/2025/01/03/2024-30209/securing-the-information-and-communications-technology-and-services-supply-chain-unmanned-aircraft.

First, any proposed rule should build on existing laws, including use of precise and narrowly defined terms and definitions. Definitions in the proposed rule should, to the greatest extent possible, be consistent with how those same terms have been previously defined in other Acts and regulations. For example, drafters should seek to align with existing definitions in the American Security Drone Act, which in turn relies on existing definitions in the U.S. Code to prohibit the federal government from procuring "covered unmanned aircraft systems" that are manufactured or assembled by "covered foreign entities."[7] Where existing categories are insufficient or overly broad, we recommend creating narrowly tailored categories in order to address undue risk.

The definition of unmanned aircraft system in 49 U.S.C. §44801(12) broadly includes both the unmanned aircraft (as defined in 49 U.S.C. §44801(11)) and "any associated elements that are required for the operator to operate safely and efficiently in the national airspace system." The "associated elements" of the UAS that are required for safe and efficient operations would include flight controllers, ground control stations and docking systems, global navigation satellite systems (GNSS) modules, communication devices, navigation devices, and sensors with control systems.

Ultimately the appropriate definition will be dependent on the focus and scope of the regulation. In crafting a definition and determining applicability, BIS should either not include or very clearly distinguish between "smart" and "dumb" aspects of the system. "Dumb" components, such as package load, vehicle movement and staging, battery management, propellers, carbon fiber frames, charging infrastructure, foam air frames, wiring harnesses, and motors, do not contribute to the risks BIS has identified as the subject of this potential regulation.

The "smart" software stack that operates the ICTS hardware is the source of risks BIS seeks to address with this proposed rulemaking; without operating software, hardware parts are inert and akin to "dumb" components. Focusing the proposed rule on software would support BIS's objective to mitigate the risks associated with ICTS without imposing undue burden on domestic drone companies.

Additionally, BIS should consult existing standards promulgated by DOC's National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO"), and the Defense Information System Agency ("DISA")'s Security Technical Implementation Guide ("STIG") in securing connected vehicles. Furthermore, both ASTM International and the Radio Technical Commission for Aeronautics ("RTCA") have published standards that may also be instructive to the BIS.[8] Leveraging existing standards will provide clarity and guidance for industry when issuing the proposed rule.

---

[7] The American Security Drone Act refers to a preexisting definition of "unmanned aircraft systems" in 49 U.S.C. sec. 44801

[8] For additional information regarding existing standards that could be leveraged in this rulemaking, see the discussion of cybersecurity considerations in the UAS Beyond Visual Line of Sight ("BVLOS") Operations Aviation Rulemaking Committee ("ARC") Final Report, (March 10, 2022) at pp. 59-60, 149150, 283-284, available at: https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS_BVLOS_ARC_FINAL_REPORT_03102022.pdf.

Prior to publishing the proposed rule, BIS should engage with the full range of stakeholders to determine the definition of covered components and assess the cost and availability of sourcing components and subcomponents. For example, in considering whether to broadly define "UAS" and any related subcomponents, BIS should assess whether certain components pose an individual risk of data exfiltration and remote access control. Our view is that BIS should consider focusing the proposed rule on only those parts and components susceptible to these risks. In addition, the rule should recognize that in certain circumstances even these parts and/or components may continue in use if acceptable mitigations to the risk are in place.

This section addresses ANPRM questions 4 and 6.

The CDA believes data exfiltration and remote access control represent the two primary areas of risk associated with foreign adversary ICTS integral to UAS technology. Our view is that BIS should consider focusing the proposed rule on those parts and components that are vulnerable to these risks. These risks are clearest when a UAS is both capable of operating BVLOS (automated flight and waypoint flight planning capability) and of performing some form of intelligence, surveillance, and reconnaissance (ISR). Therefore, UAS with those capabilities versus aircraft without these capabilities (e.g., small radio-controlled toys with no cameras, or balsa wood model aircraft) should be a critical point of distinction for BIS to consider in its rulemaking. Furthermore, BIS should account for the fact that risks associated with aircraft with BVLOS and ISR capabilities can be mitigated.

Supply chain reliance on foreign adversary-produced aircraft, components, and subcomponents is an additional consideration. Companies are generally in the best position to manage this supply chain risk based on their knowledge of their aircraft and/or operations, and this should not necessarily be a primary consideration for BIS's potential regulations. The U.S. commercial drone industry shares the common goals of seeing this industry succeed here in the U.S., boosting domestic manufacturing capabilities, and addressing legitimate national security concerns.

This section addresses ANPRM question 13.

The CDA represents a wide range of organizations within the commercial drone marketplace, that vary by size, structure, and organization. Our goal is ultimately to enable American and Allied organizations to bring the benefits of drone technology to communities across the United States at scale. Companies and organizations in this marketplace range from small businesses with less than five employees to multinational corporations with complex international relationships. There is also significant variation in how companies build, buy, and use drones:

For **Operators**, this variation ranges from vertically integrated manufacturers/operators[9] to operators that buy commercial-off-the-shelf (COTS) systems and fly them right out of the box with no customization. Between these two extremes, there are myriad 'integrator' companies who leverage combinations of COTS hardware with third party sensors or software, including cloud-storage and processing and autoflight systems, or who build systems with varying degrees of customized hardware and COTS software solutions.[10]

For **Manufacturers**, this variation ranges from manufacturers who build an entire UAS, complete with all associated elements, and produce thousands of systems a month for commercial and public safety customers,[11] to manufacturers who develop and/or build various components and subcomponents of a UAS, including flight data service providers, spectrum providers, and autoflight software developers.[12]

It is critical that BIS takes into account the entire commercial drone ecosystem, including but not limited to manufacturers, vertically integrated organizations, component and software developers, and ultimate end users of drone technology. These different entities may also have varying degrees of capability to mitigate risks associated with foreign adversary produced UAS and components. BIS should also consider the ease, difficulty, and cost of implementing BIS regulations for these various entities.

The CDA represents a variety of stakeholders with competing views. A majority of CDA members urge BIS to consider that there are multiple methods of mitigating the risks associated with foreign adversary-produced UAS and components. Any BIS regulation should clearly identify such risks and provide flexibility for companies to mitigate those risks in a performance-based way. For example, compartmentalization (a practice long proven to work for securing information) is one type of mitigation a manufacturer can use to protect against third party interference with UAS operations whereby the entities supplying distinct hardware components do not have access to the software running the aircraft itself.

While not the prevailing CDA view, other members believe there to be unique risk associated with UAS that are wholly built by a company subject to foreign adversarial control, meaning hardware, software, and all integration thereof is designed and built by the foreign adversary-owned company, These stakeholders would urge BIS to consider restrictions on entire platforms, rather than using third party software, cybersecurity standards, component restrictions, or other methods to mitigate risk.

Accounting for the ability of various stakeholders to ultimately mitigate such risks at an appropriate scale is critical to the viability of the industry as a whole. We strongly encourage BIS

[9] These companies manufacture their own drones, develop and integrate their own software, and then operate the drones they build for commercial services. Examples include Wing, Amazon Prime Air, Zipline, Percepto, and Ondas.

[10] These include companies like Florida Power and Light, Southern Company, NUAIR, and Choctaw Nation.

[11] These include companies like Skydio.

[12] These include companies like Skysafe, Hidden Level, and Honeywell.

to engage with a variety of operators, manufacturers, service providers, and end users to inform any potential proposed regulation.

Vertically Integrated Manufacturers/Operators

U.S.-based vertically integrated manufacturers/operators represent a subset of the drone sector composed of entities that are already subject to stringent federal regulations. These entities employ controls on hardware and software, as well as the integration of hardware and software in the aircraft they design, build, and operate; they have quality assurance programs and controls for hardware, tightly control data pipelines, limit external access to systems, employ encryption, and implement other controls that achieve effective compartmentalization and make unauthorized control or data exfiltration highly unlikely. Further, the software used by these entities – which dictates how the aircraft receives, processes, and transmits data – is developed by the U.S. or allied countries and loaded onto the aircraft within the U.S. or allied country of origin.

Taken together, the practices around hardware assurance, stringent software controls, compartmentalization, and controlled data pipelines work together to greatly reduce or eliminate the risks identified in the ANPRM. BIS should therefore consider adopting an approach that excludes appropriately certified domestic and allied-country drone operators who design and manufacture their own drones and develop and integrate their own software from restrictive measures, given their critical role in advancing the domestic UAS sector. BIS should either exclude U.S.- (or allied country-) based vertically integrated manufacturers/operators from this proceeding or provide for a general authorization process with presumption of approval for these entities given their distinct security posture.

This section addresses ANPRM questions 15, 16, 18, 19, and 20.

Data collection capabilities of UAS are largely dependent on sensor quality. Those sensors typically capture imagery (also called RGB), thermal/IR, LIDAR, or optical gas "visual data." That visual data also comes with EXIF metadata that would show the geo-positioning of the image, and sometimes, the azimuth angle the drone was facing, the angle of the camera, and the distance from the object taken.

Typically, the operator or end customer owns the data. Sometimes a software company that helps process that data may have the right to do algorithmic / anonymized derivative products from that data. Generally, broad-based UAS data is not sold into data markets in the same way as satellite and airplane data. Given the point-to-point nature and low altitude flight of drones, there is no clear resale market, as the data is generally based on the owner of an asset asking for drone use. A company may maintain the right to build derivative algorithmic products, but particularly given contractual obligations, would not sell competitors' data to each other as normal practice.

Typically, U.S. customer data is stored at a U.S.-based cloud service provider. This is completely customer or operator driven – the only time data would be stored outside of the U.S. is when a non-U.S. customer asks that their data be stored in the equivalent system in another

country. Additionally, given the growth of drones used for public safety and other governmental purposes, data captured by a UAS can also be stored locally by state and local public agencies.

Generally, software companies in the UAS space utilize end-to-end encryption of customer data and adhere to SOC / SOC-2 security protocols. Software tools like field uploaders provide another layer of obfuscation that enable data to be wiped, stored, and processed away from the end system operator.

This section addresses ANPRM question 23.

Typically, sensors are imagery (RGB), thermal/IR, LIDAR, and Optical Gas. In each case, these are heavy data products that are downloaded onto a Software Development Kit card and are only available locally. Typically, a video downlink connecting the drone to the controller is the only 'over the air' transmission of imagery or video, which is not stored/saved, but is critical to the safety of flight for UAS.

Regardless of their use in any particular industry, BIS should consider excluding sensors without connection capabilities from the scope of the regulation as such sensors do not pose the types of risk that BIS seeks to reduce in this rulemaking. The BIS Connected Vehicles Rule, which exempted "items that are … for the purpose of distancing positioning or imaging only… (e.g., …. Sensors including LiDAR and Radar)" should serve as a guide for regulation of sensors in the current rulemaking. In this rule, BIS determined that these types of sensors do not pose significant risks. It should follow that path and exclude from regulation UAS sensors that perform distancing positioning or imaging only and other sensors without connection capabilities.

This section addresses ANPRM question 50.

Mitigating Economic Impacts

In the event that the proposed rule restricts or prohibits certain foreign-produced components, the rule should also provide sufficient time to allow U.S. companies to source adequate substitutes for alternative components. Depending on the components covered in a proposed rule, this process could take several years. Similarly, the proposed rule should consider the different levels of investment and regulatory burdens associated with having to make software and hardware changes within the industry. For example, vertically integrated drone manufacturers/operators must engage in costly and time-consuming design, test, validation, and approval processes for any hardware or software change on their UAS. Therefore, the proposed rule should provide either a phased implementation or a temporary exemption or reporting requirement that allows the industry sufficient time to adjust its supply chain. In the event that BIS determines there is not an adequate alternative source outside of a "foreign adversary" as defined in 15 C.F.R. § 7.4, the proposed rule should explicitly enable a streamlined process for exemptions such as the license exemptions BIS maintains under the Export Administration Regulations ("EAR").

For example, the "Notified Advanced Computing (NAC) and Advancing Computing Authorized (ACA)" license exception at section 740.8 of the EAR allows use of certain components twenty-five days after (1) exporters submit a report to BIS notifying it of the use of those components and (2) BIS confirms use within that twenty-five day window. A similar reporting mechanism could be considered wherein manufacturers could notify BIS of the use of certain components subject to the proposed rule from countries of concern and BIS could authorize such use during a waiting period. Depending on what restrictions BIS ultimately proposes, a longer transition period may be warranted.

Bolstering Domestic Manufacturing and Supply Chain

The CDA also strongly encourages the government to provide manufacturing and production incentives to aid in strengthening the domestic or allied supply chain in support of a proposed rule by BIS. The development of both hardware and software domestically each warrant distinct consideration, given the differences in development and production timelines.

It is also important to note that parts of the drone industry currently rely on many of the same components and supply chains as the cellphone and consumer electronics industry at large. Changes to or relocations of existing production facilities rely on decisions made by suppliers that deal with millions of units for cellphone and other smart device components, in addition to the thousands of units for drone components. Imposing specific and unique restrictions on the drone industry when it overlaps so significantly with the broader consumer electronics supply chains (without the same restrictions) risks the health and success of the domestic drone industry.

Software Considerations

In the event that BIS proposes to regulate software developed by foreign adversaries, we encourage BIS to explicitly address scenarios around purchased or licensed source code, in addition to carving out a clear exception for open-source code that foreign adversaries have developed in the past. As BIS is aware, when a U.S. entity purchases code, creates a new repository with significant updates, and hosts it domestically without ongoing foreign involvement, this represents a lower risk profile than does continuous foreign control. Additionally, both the NPRM and final rule should consider a legacy software period to reduce regulatory burden and increase compliance with final rule timelines, akin to the Connected Vehicles Rule.

BIS should also consider excluding or providing an authorization process for ICTS hardware if the operating software has been exclusively built, developed, and tested by domestic or non-adversary companies. There is significant market potential for U.S.- and allied country-developed software solutions that support broad commercial UAS applications, and we hope that BIS gives consideration to enabling this market potential in its regulatory proposal.

Testing Considerations

BIS should consider an exemption or general authorization for UAS hardware and software that will only be used for testing and research purposes, which will help the U.S.

advance its development capabilities and also continue to support counter-UAS testing and research needs. This will not represent a significant risk since these types of UAS hardware and software would not be available for consumers.

Strengthening Regulatory Predictability

Finally, the long-overdue finalization of an FAA rule to deregulate scalable commercial drone operations beyond visual line of sight would provide the domestic drone industry with increased ability to conduct business at scale in the U.S.

The CDA recognizes the Administration's commitment to advancing U.S. innovation, reducing bureaucratic red tape, and creating American jobs. We encourage BIS to take a holistic view and work with other departments and agencies to accelerate American leadership in the drone industry while addressing risks in a responsible manner.

IV. Conclusion

The CDA appreciates this opportunity to comment on the BIS's ANPRM regarding UAS and we hope that the BIS will continue to take into account the diverse perspectives of the UAS industry. The CDA looks forward to continuing to work with the BIS to ensure a safe and secure supply chain while simultaneously working to accelerate the safe and secure integration of commercial drones into the National Airspace System, which will unlock the benefits of commercial drone operations for the American people.

Respectfully submitted,

Liz Forro

Liz Forro
Policy Director
Commercial Drone Alliance