BEFORE THE
DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY
WASHINGTON, D.C.

IN THE MATTER OF

Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems

Docket No. BIS-2024-0058

COMMENTS OF THE SMALL UAV COALITION

Gregory S. Walden
DGA Group Government Relations LLC
1900 K Street NW
Washington, DC 20006
Counsel to the Small UAV Coalition

March 4, 2025

Filed with www.regulations.gov

BEFORE THE
DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY
WASHINGTON, D.C.

IN THE MATTER OF

Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems

Docket No. BIS-2024-0058

COMMENTS OF THE SMALL UAV COALITION

The Small UAV Coalition[1] ("Coalition") is pleased to provide comments in response to the request for comments on the advanced notice of proposed rulemaking ("ANPRM") regarding certain transactions involving information and communications technology and services ("ICTS") integral to unmanned aircraft systems ("UAS" or "drones") that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of certain designated foreign countries in Executive Order 13873 ("Securing the Information and Communications Technology and Services Supply Chain")(84 Fed. Reg. 22689 (May 17, 2019). 90 Fed. Reg. 271 (Jan. 3, 2025). This rulemaking follows the Bureau of Industry and Security ("BIS") final rule "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles," 90 Fed. Reg. 5360 (Jan. 16, 2025) ("BIS Connected Vehicles Rule").

The Coalition appreciates your engagement with industry in the process of delving into this critical issue that not only affects drones, but also the aviation sector more broadly, in addition to many other industries. This input will be important in enabling BIS to strike the appropriate balance of addressing and mitigating specific risks while ensuring that American companies can continue as global leaders in the drone industry.

As described more in the specific comments below, the Coalition believes the prohibited transactions in any BIS final rule should apply only to "fully assembled" drones that includes software that poses the risks of exfiltration or remote access identified in the ANPRM.

---

[1] Members of the Small UAV Coalition are listed at www.smalluavcoalition.org.

Definition of UAS. For simplicity and consistency, the Coalition recommends that BIS adopt the definition of "unmanned aircraft" and "unmanned aircraft systems" Congress included in amendments to the Federal Aviation Act, 49 U.S.C. § 44801(11) and (12):

> *Unmanned aircraft* means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.
>
> *Unmanned aircraft system* means an unmanned aircraft and its associated elements (including communication links and the components that control the unmanned aircraft) that are required for operator to operate safely and efficiently in the national airspace system.

While the Coalition recommends that BIS adopt these definitions, we do not believe the definition BIS uses should be dispositive with respect to any of the prohibitions or requirements of this rulemaking. Each of the definitions set forth in the ANPRM is broader than the sum of the security-related components that are integral to a drone's operation. The reference to "communications links and the components that control the aircraft" in the Federal Aviation Act definition should suffice to cover the components that are "integral to unmanned aircraft systems (UAS)." 90 Fed. Reg. at 271. The Coalition does not agree with BIS that all the UAS "subsystems" listed in the notice are "integral," such as "recording capabilities for receiving live imagery" and "the capability of remote software or firmware updates." 90 Fed. Reg. at 274. There are many drone use cases with regular operations (from delivery operations without live feeds to hobbyist drones without remote update capability) that do not involve the capabilities mentioned above, and therefore should not be considered integral to a drone's operation.

The International Trade Administration (ITA) definition is overly broad as it includes the entirety of a drone's payload, including, for example, items being carried or delivered by a drone but not at all related to its operation, which is the risk vector intended to be addressed in this rulemaking.

Given its verbiage referring to "any aircraft capable of initiating flight and sustaining controlled flight and navigation without any human presence on board", the Export Administration Regulations (EAR) definition (15 C.F.R. 772.1) would not be fitting either. The EAR definition does not recognize these key differences between UAS aircraft and eVTOL or autonomous aircraft transporting large cargo or passengers.

Regardless of the definition BIS adopts in a proposed rule, BIS should explain that there are components of a drone that are not "integral to the operation" of the drone and/or do not pose the exfiltration and remote access risks BIS seeks to reduce in this rulemaking; e.g., package load, battery management, propellers, carbon fiber frames, and motors.

In response to question 2, the Coalition recommends that BIS focus this rulemaking on the systems and components that are deemed security-critical in terms of posing the risks BIS identifies in the ANPRM. We understand this definition excludes the term "cameras," as BIS did in the BIS

Connected Vehicles Rule, 90 Fed. Reg. at 5390, as a camera is not integral to the operation of a drone, it is not a communications link and does not control the drone.

In scoping how broadly any restrictions should apply, the Coalition believes that the fundamental question relates to directly linking the restrictions to the capabilities of the aircraft. Capabilities of a drone that implicate whether or not it presents a security risk include: the ability to fly beyond the visual line of sight; direct and precise control of the drone by the operator; presence of a live video feed to the operator or other navigational tools that allow the operator to understand the location of the drone and where it is going; and a communications and control ("C2") link that is susceptible to interference or tampering. Without all of these characteristics – particularly when the hardware and software are designed and integrated by U.S. or allied countries – a drone presents very little risk to the primary concerns BIS has identified in this ANRPM Also critical is the operation to be performed. Inspection of pipelines and other critical infrastructure poses more risk than other drone operations.

Concerning specific components of the list of ICTS components that BIS has "preliminarily identified as integral to the UAS platform," listed below, (8) local and external data storage devices and services may be relevant to privacy concerns, but the Coalition does not believe it is integral to the drone's operation in the national airspace system.

(1) onboard computers for processing data and controlling UAV flight
(2) communication systems including, but not limited to, flight controllers, transceiver/receiver equipment, proximity links such as GNSS sensors and flight termination equipment
(3) flight control systems responsible for takeoff, landing, and navigation, including but not limited to, exteroceptive and proprioceptive sensors
(4) GCS or systems including, but not limited to, handheld flight controllers
(5) operating software, including but not limited to, network management software
(6) mission planning software
(7) intelligent battery power systems
(8) local and external data storage devices and services
(9) AI software or applications

Some of these components functionally overlap, such as (1), (2), (3), and (4). The key concepts in the UAS definition are control and communications. These components can be listed as examples of what is used for control and communications.

With respect to hardware, the Coalition believes hardware components pose little if any exfiltration or remote access control risk. These risks reside in the software stack that controls hardware components, because the hardware is inert without the software to control it. Excluding hardware as a general matter would align this rulemaking with the BIS Connected Vehicles Rule, see 90 Fed. Reg. at 5373-75.

Risks associated with UAS. The Coalition agrees that the two primary areas of security risks associated with transactions involving foreign adversary ICTS are exfiltration and remote access

control. These risks exist for UAS technology but are not unique to such technology. In fact, these risks are common to all supply chain technologies, including connected vehicles.

Threat posed by foreign adversaries. The Coalition acknowledges the threats that have been identified by the Department of Homeland Security, Department of Defense, and FBI, as discussed in the BIS ANPRM at pages 275-276. However, the Coalition does not agree that "forced updates that disable UAS in predefined zones" are necessarily "malicious." These restrictions are commonly imposed for safety and security purposes. Preventing a drone from entering prohibited or restricted airspace is a good thing. Like many technologies such as connected vehicles, remote control of drones carries risks. But it also carries significant safety benefits.

Prohibited transactions. The prohibited transactions in the BIS Connected Vehicles Rule apply to "completed" connected vehicles that incorporate VCS hardware or covered software. The Coalition urges BIS to adopt a similar provision and apply the prohibitions to fully assembled drones. The prohibited transactions also include VCS hardware, 15 C.F.R. 791.302, defined as "software- enabled or programmable components if they directly enable the function of and are directly connected to Vehicle Connectivity Systems, or are part of an item that directly enables the function of Vehicle Connectivity Systems." 15 C.F.R. 791.301, 90 Fed. Reg. at 5416.

As BIS explained in the preamble to the BIS Connected Vehicles Rule:

> BIS confirms that transactions involving covered software and VCS hardware that are not integrated into a connected vehicle are not subject to this regulation. VCS hardware importers and connected vehicle manufacturers executing covered software and VCS hardware transactions that are intended to be incorporated into a connected vehicle, as defined in the final rule, are subject to this regulation.

90 Fed. Reg. at 5375.

Prohibitions and requirements should be tailored to the security risks of exfiltration and remote access. Any new regulations should be tailored to the risk profile and take great care in the process of determining which components constitute an undue or unacceptable threat or should otherwise be prohibited. Any new regulations should also consider if there can be sufficient manufacturing process or operational mitigations to address undue or unacceptable threats posed by such components that could be utilized when there is no reasonable alternative supplier of such components. Even small changes from foreign to domestically manufactured components could cause significant disruptions.

What components should be carved out? There are many components of a drone that are not integral to the control or communications of a drone, such as a camera, propeller, wing, motor, battery, lighting, wiring, harness, molded foam, and the drone-equivalent of a fuselage. More broadly, hardware components should be excluded from the prohibitions, as components at this stage of the manufacturing process do not pose the risk of data exfiltration or remote access control, the two risks BIS proposes to address in this rulemaking. The Coalition recommends that BIS propose to exclude hardware from the final rule as a general matter and provide a list of any

hardware or software components that are included so that the industry has clarity on how to approach potential supply chain adjustments.

Also, the components of a drone as well as the completed drone used exclusively for experimental, research and development purposes should be excluded from the prohibitions to allow for innovation, recognizing that the finally assembled drone used for other than R&D purposes would be subject to the otherwise applicable prohibition(s). Because these drones will not be sold to consumers, they would pose only limited risks, while testing and research will help U.S. companies advance drone capabilities.

In the ANPRM, BIS anticipates carving out a clear exception for open-source code that foreign adversaries have developed in the past. The NPRM should explicitly address scenarios involving purchased or licensed source code, similar to existing provisions for modified open-source code with a view to the least-restrictive regulation in this low-risk area. When a U.S. entity purchases code, creates a new repository with significant updates, and hosts it domestically without any post-purchase foreign involvement, this represents a much lower-risk profile than would continuous foreign control. In the NPRM, BIS should propose for comment specific criteria for when it would consider such "branched" code sufficiently independent from its foreign origin. Such criteria could include factors such as: percentage of code modified; hosting location; update control; and elimination of foreign access to the new codebase.

Sensors without connection capabilities should also be excluded from the prohibitions. Such sensors do not pose the types of risk BIS seeks to address in this rulemaking. We refer to the BIS Connected Vehicle Rule, which exempted "items that are . . for the purpose of distancing position or imaging only . . . (e.g., . . . sensors including LiDAR and radar). 90 Fed. Reg. at 5390. BIS should similarly exclude drone sensors that perform only distancing or imaging.

Legacy, "pre-rule" components. The Coalition notes that the BIS Connected Vehicles Rule included a legacy software provision due to the "burden of determining the provenance of software subcomponents for legacy code bases." 90 Fed. Reg. at 5377. BIS should similarly exclude legacy software in this rulemaking, with the goal of reducing the regulatory burden on U.S. companies and allowing regulated entities to comply with the compliance deadlines in the eventual final rule.

Temporary authorizations. BIS asks in Question 42 whether there are "instances in which granting a temporary authorization to engage in otherwise prohibited . . . transactions would be necessary to avoid supply chain disruptions or otherwise unintended consequences and in the interests of the United States. The Coalition agreed there are such instances. In recognition of this concern, BIS should allow for a three-year ramp for domestic U.S. manufacturers to minimize supply chain disruption. BIS should also implement a structured validation process for potential partners in countries of concern.

Special authorization process. The ANPRM contemplates the creation of a special authorization process where a manufacturer may mitigate an undue or unacceptable risk and not be prohibited from engaging in a transaction. The BIS Connected Vehicles Rule also established a *general* authorization process where mitigating factors reduce risks to an acceptable level. The Coalition recommends that BIS similarly propose a general authorization process for drones. BIS should

also consider a general or specific authorization for trusted U.S. manufacturers and distributors that might have some parts of their supply chain located in China.

The potential risk drones pose can be mitigated in two ways: through the practice of compartmentalization and/or through US- or allied country-based vertically integrated manufacturers and operators (VIMOs) that employ controls on hardware and software and their integration.

Compartmentalization (a practice long proven to work to secure information) is an effective mitigation a manufacturer can use 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. US-based vertically integrated manufacturers and operators represent a limited subset of the drone sector composed of entities that are subject to stringent federal regulations. VIMOs have quality assurance and controls for hardware, tightly control data pipelines, limit external access, employ encryption, and implement controls that achieve effective compartmentalization and make unauthorized control or data exfiltration highly unlikely. Further, the software used by VIMOs – how the airplane receives, processes, and transmits data – is developed in-house and only loaded onto the aircraft in the US for operations in the US.

Taken together, the practices around hardware assurance, stringent software controls, compartmentalization, and controlled data pipelines work together to greatly reduce or eliminate the risks as stated in the ANPRM.

For these reasons, we urge BIS to adopt 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 US- (or allied country-) based VIMOs from this proceeding or provide for a general authorization process with presumption of approval for these VIMOs given their distinct security posture.

Mitigation mechanisms.
The Coalition agrees that there are mitigations in design, manufacture, and operation that address the otherwise undue or unacceptable risk. Encryption and authentication are important means of attempting to secure drones from these threats. As the ANPRM recognizes, these mitigations may be in design requirements, machine learning control, implementation standards and protocols, cybersecurity firmware and/or software inputs, and manufacturing integrity protection systems and procedures. U.S. manufacturers and operators have the ability to mitigate potential risks from ICTS hardware components by developing software, including firmware, and implementing other controls and redundancies.

BIS recognizes that companies may be reluctant to provide answers in the public docket that would reveal "confidential business information." BIS invites such companies to provide answers to BIS separately and provide a summary in the public docket. Members of the Coalition would be reluctant even to provide a summary in the docket and request the opportunity to brief BIS officials in person. Beyond traditional commercial proprietary concerns, the Coalition is concerned that

answering many questions in the ANPRM (i.e., questions 15-41) regarding specific type and models of drones would reveal vulnerabilities and provide a roadmap for malicious actors. The Coalition recommends that BIS consult with all relevant actors in the supply chain, including end users of drones.

Standards and guidelines. There are a number of existing standards covering cybersecurity and risk management best practices and standards for both the hardware and software supply chain, which the Coalition suggests BIS should leverage to inform this rulemaking, and which may be useful for companies to reference and incorporate into their practices to meet a requirement in the final rule. In addressing the supply chain aspect as well as cybersecurity, our members should have the option of developing internal processes to execute due diligence on their suppliers. This process could take inspiration from the North American Transmission Forum ("NATF") Supply Chain Security Criteria by having suppliers answer these questions from NATF, which could then enable companies to make a risk-based assessment.

Economic impact. At the ANPRM stage, it is not possible to understand or estimate the economic impact to the UAS industry from prohibitions and other requirements BIS may eventually impose in a final rule. At this point, it may safely be stated that even small changes from foreign to domestically manufactured components in drones could cause significant costs and delays, depending on the status of the supply chain for such components. Replacing components may also substantially delay the FAA's certification and other approval processes. In addition to the near-term impact of increased costs, it also runs the risk of severely limiting the availability of certain products, such as batteries, motors, and rare earth minerals. Finally, action contemplated by BIS could also result in retaliatory action taken by other countries, further exacerbating supply chain disruptions and potentially cutting off availability of critical components. While the market is shifting, forcing changes could also result in significant impact or product quality and availability.

It is worth also noting the significant economic benefits that scaled utilization of drones flying beyond the operator's visual line of sight will bring to the U.S. economy. An Accenture report from 2021 identifies myriad economic and societal benefits from a thriving U.S. drone industry.[2] Any adverse effect that limits this vision from becoming a reality ought to be weighed in the scoping and development of a BIS NPRM on drones.

Anticompetitive effects. In response to Question 47, lithium-ion batteries used in drones, which are today primarily sources from China, remain the core energy supply with drone systems including those otherwise wholly or primarily produced in the United States. These lithium-ion batteries are critical to the development of strong LI cell / pouch production in the United States and vital to maintaining and developing government and private UAS operations. The BIS Connected Vehicles Rule explicitly excluded from its scope "a hardware or software item that exclusively… supplies or manages power for the VCS." 90 Fed. Reg. at 5391. BIS's rationale for this exclusion in that rulemaking was due to the "low-risk use cases and [to] provide the industry with greater flexibility." 90 Fed. Reg. at 5390. That reasoning equally applies here.

---

[2] 'Faster, Safer and Greener: The Potential Impact of Delivery Drones in the Dallas-Fort Worth Metroplex' (February 2021), Report by Accenture, p 5. Available: https://storage.googleapis.com/wing-static-us/us/Dallas%20Impact%20Report.pdf

Depending on particulars in a final rule, this rulemaking threatens to have anti-competitive effects on the U.S. market. Specifically, U.S. domestic drone production often depends on hardware components from the Asia-Pacific region, with many sub-tier components produced by companies with links to Chinese government ownership. The types of regulation of transactions involving foreign adversary ICTS contemplated in this ANPRM, if made final, would require U.S. companies that depend on these sources to establish alternative, competitive, manufacturing of these elements in other geographic locations and without ties to foreign adversary-linked companies. Few alternative manufacturing capabilities exist today. Those that exist are not adequate to serve the current market, much less the future needs of the rapidly-growing industry that promises benefits to public safety, healthcare, and U.S. consumers. Establishing such facilities and know-how is a multi-year process under the most optimistic estimates. Especially without a multi-year compliance period in the final rule, regulation of transactions involving foreign adversary ICTS integral to UAS will delay U.S. production timelines for some drones and result in increased costs on some U.S. producers, although there are some U.S. producers today that only minimally rely on foreign adversary ICTS.

Governmental support. Overly restrictive and broad regulation could hamstring innovation for American companies by making the drone industry less equipped to compete strongly on a global scale. If BIS moves forward with this rulemaking, the Coalition recommends coordination across agencies for a whole-of-government approach to minimize costs to the drone industry. For instance, the drone industry would greatly benefit from financial incentives and resources available for alternative manufacturing and building domestic capabilities. Without such assistance to offset change to supply chain regulations, American innovation, economic growth and global competitiveness in the global drone industry will suffer.

Timeline for compliance. To minimize supply chain disruptions and spread out the economic costs in the BIS Connected Vehicles Rule, BIS agreed to delay imposition on the prohibitions on both VCS hardware and on connected vehicles manufacturers, granting an exemption from the VCS hardware prohibitions until model year 2030 and an exemption from the connected vehicle manufacturer prohibitions until model year 2027. Likewise for drone manufacturers, to minimize supply chain disruptions, avoid the anticompetitive effects described above, and spread out the economic costs of a final rule on drones, the Coalition recommends a timeline for compliance at least equivalent to that provided for connected vehicles (or otherwise justified as appropriate after consultation with U.S. manufacturers of UAS subject to the requirements of a scoped NPRM) within the terms of the final rule.

Respectfully submitted,

Gregory S. Walden
DGA Group Government Relations LLC
1900 K Street NW
Washington, DC 20006
gregory.walden@dgagroup.com
202-403-9904
Counsel to the Small UAV Coalition

March 4, 2025