Association for Uncrewed Vehicle Systems International (AUVSI) Comment on Federal Register Notice and Request for Comments: Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

Printed version: PDF	**Document Citation:** 89 FR 15066
Publication Date: 03/01/2024	**Page:** 15066-15072 (7 pages)
Agencies: Department of Commerce Bureau of Industry and Security	**CFR:** 15 CFR 7
Dates: Comments must be received on or before April 30, 2024.	**Agency/Docket Number:** Docket No. 240227-0060
Comments Close: 04/30/2024	**RIN:** 0694-AJ56
Document Type: Proposed Rule	**Document Number:** 2024-04382

AUVSI appreciates the Department of Commerce (DOC), Bureau of Industry and Security (BIS), and Office of Information and Communications Technology and Services' (OICTS) interest in furthering the understanding of the definition of a Connected Vehicle (CV). Given DOC and BIS' experience in regulating information security, the Association for Uncrewed Vehicle Systems International (AUVSI) believes these agencies are well positioned to leverage their expertise to appropriately promulgate and fairly administer rules that protect our national security, while also fostering a competitive industry and avoiding unintended consequences.

As the world's largest non-profit organization dedicated to the advancement of uncrewed systems, autonomy, and robotics, we would expect to be included among the conversations associated with the Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles Advance Notice of Proposed Rulemaking (ANPRM).[1] AUVSI represents corporations and professionals from more than 60 countries that are involved in industry, government, and academia. AUVSI's primary markets span the defense, civil, and commercial industries. Our membership also includes many of the leading companies in the Advanced Air Mobility (AAM) industry, including Original Equipment Manufacturers (OEMs), components suppliers, and supporting vertiport/infrastructure companies. Uncrewed systems of all sizes and missions represent an expansive market within the transportation system, and it is our mission to ensure all types of uncrewed systems, autonomy, and robotics companies that work with us have access to the resources they need to be successful in such a highly competitive industry.

[1] https://www.federalregister.gov/documents/2024/03/01/2024-04382/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles

Additionally, AUVSI recently created the Partnership for Drone Competitiveness, a coalition of U.S. drone and drone component manufacturers and enterprise users who are committed to strengthening the U.S. drone industry. The Partnership is built on a simple premise: that stronger U.S. leadership in this industry is better for everyone. For more information on the challenges facing the drone industry and recommendations for U.S. lawmakers and regulators, see our white paper here.[2]

The Securing the Information and Communications Technology and Services Supply Chain Executive Order, which prompted this ANPRM, does not mention drones.[3] However, we provide the following comments in case DOC/BIS is contemplating including them in the scope of the ANPRM.

Drones/Uncrewed Aircraft Systems (UAS) and CVs (mostly described as automotive CVs in the ANPRM) are not completely alike in their operations. AUVSI would be concerned about any efforts to regulate these different types of vehicles as if they were a single category, whether in the context of this ANPRM, an eventual Notice of Proposed Rulemaking (NPRM)/Final Rule, or otherwise. Drones do not generally use vehicle-to-vehicle communication. Automotive CVs, by contrast, do use vehicle-to-vehicle communication, which links them to transportation networks and critical infrastructure (the networks that a prospective NPRM/Final Rule would seek to secure). Regulating these technologies together could unintentionally set a precedent for drones to be categorized as CVs in future regulatory proceedings across federal agencies. If drones are included, they should instead be considered as a separate sub-class.

AUVSI recognizes that the Chinese Communist Party (CCP) has a history of engaging in espionage and the risk that this nefarious activity poses to our national security. It is of critical importance to guard against these cybersecurity threats, and other government bodies also have sought to provide safeguards to address this harmful and illicit activity targeting companies connected to Foreign Adversaries.[4] For instance, the American Security Drone Act (ASDA), which was enacted in December as part of the Fiscal Year 2024 National Defense Authorization Act (NDAA), delineates what constitutes a covered component and what would be subject to prohibition.[5] These provisions that are being implemented involve the Consolidated Screening List, to which the DOC contributes. Additionally, the world's largest drone manufacturer, DJI, was recently listed as a "Chinese Military Company" due to its direct support of the People's Liberation Army (PLA).[6] A warning was also issued by the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) to all public and private sector critical infrastructure operators concerning the risks posed by the use of People's Republic of China (PRC)-made UAS, including serving as a vector for a cyberattack.[7]

Given supply chain limitations in terms of alternative sources of components, BIS should allow standards, such as National Institute of Standards and Technology (NIST), Security Technical Implementation Guide (STIG), and International Organization for Standardization (ISO) compliance, to serve as mitigation measures to permit prohibited transactions from entities that are considered CVs.

---

[2] https://www.auvsi.org/sites/default/files/AUVSI-Partnership-for-Drone-Competitiveness-White-Paper.pdf
[3] https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain
[4] https://www.ecfr.gov/current/title-15/subtitle-A/part-7/subpart-A/section-7.4
[5] Public Law 118-31 - https://www.congress.gov/bill/118th-congress/house-bill/2670/text
[6] https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF
[7] https://www.cisa.gov/news-events/news/release-cybersecurity-guidance-chinese-manufactured-uas-critical-infrastructure-owners-and-operators

This approach would enable continued growth of beneficial technology while ensuring that appropriate safeguards are in place to prevent malicious cybersecurity attacks from adversaries.

Should DOC and BIS decide to include drones in the CV definition for the purposes of this rulemaking, certain principles should be taken into consideration:

- The CV definition should be precisely and narrowly tailored to address the threats posed by the use of drones from countries listed as foreign adversaries while avoiding unintended consequences that could hurt domestic companies.
    - Subclasses of drones have different risk profiles that should be considered, as well as adoption levels, which would make changes more or less disruptive.
- The Regulatory Impact Analysis must consider both costs and benefits of the proposed rule, including as it relates overall to vehicular safety.
    - Should DOC and BIS decide to include drones in its definition of CVs, the regulatory analysis should consider the costs and availability of alternative sources for security critical components or subcomponents in relation to the security threat posed.
- Efforts at definitions around covered equipment/components or other requirements should align wherever possible with existing law or build on existing efforts.
    - For example, use the same definitions as covered UAS categories in the recently-enacted ASDA.
    - DOC and BIS should consider whether existing rules would sufficiently safeguard against the risk discussed in this ANPRM, and if BIS decides to still promulgate a new regulation, it should build upon this precedent.
- The proposed process for determining covered equipment and components, as well as any available waivers that could be granted, should involve significant stakeholder input.
    - Even small changes from foreign to domestically manufactured components could change type certification processes with the Federal Aviation Administration (FAA) and cause significant disruptions.
- The process the ANPRM, and potentially an NPRM/Final Rule, proposes for determining covered equipment to be prohibited should allow for risk mitigation solutions to be considered, particularly with respect to non-security sensitive components.
- Any forthcoming requirements or restrictions should provide sufficient lead-time/runway for operators and industry to transition to secure solutions and make adjustments to the supply chain.

Again, we are thankful for the opportunity to provide input about proposed definitions for CVs across multiple domains. The potential risks, and costs of mitigating those risks, in addition to the opportunities presented by CVs argue against regulating them. If the NPRM/Final Rule includes drones, it must do so with a separate set of proposed rules and associated regulatory impact analysis.

Respectfully,

Max Rosen

Max Rosen
Director, Government Affairs, Association for Uncrewed Vehicle Systems International (AUVSI)