JOHN MOOLENAAR, MICHIGAN
CHAIRMAN
ROB WITTMAN, VIRGINIA
BLAINE LUETKEMEYER, MISSOURI
ANDY BARR, KENTUCKY
DAN NEWHOUSE, WASHINGTON
DARIN LAHOOD, ILLINOIS
NEAL DUNN, FLORIDA
JIM BANKS, INDIANA
DUSTY JOHNSON, SOUTH DAKOTA
MICHELLE STEEL, CALIFORNIA
ASHLEY HINSON, IOWA
CARLOS GIMENEZ, FLORIDA

RAJA KRISHNAMOORTHI, ILLINOIS
RANKING MEMBER
KATHY CASTOR, FLORIDA
ANDRÉ CARSON, INDIANA
SETH MOULTON, MASSACHUSSETTS
RO KHANNA, CALIFORNIA
ANDY KIM, NEW JERSEY
MIKIE SHERRILL, NEW JERSEY
HALEY STEVENS, MICHIGAN
JAKE AUCHINCLOSS, MASSACHUSSETTS
RITCHIE TORRES, NEW YORK
SHONTEL BROWN, OHIO

Congress of the United States
House of Representatives
SELECT COMMITTEE ON THE CHINESE COMMUNIST PARTY

June 13, 2024

The Honorable Gina Raimondo
Secretary
Department of Commerce
1401 Constitution Avenue, NW
Washington, D.C. 20230

Dear Secretary Raimondo:

Thank you for your ongoing work to develop regulations to secure and safeguard the Information and Communications Technology and Services (ICTS) supply chain.[1] This initiative is critical to our national security. As part of such effort, in March, the U.S. Department of Commerce (Commerce) issued an advance notice of proposed rulemaking (Proposed Rulemaking) requesting input regarding the regulation of connected vehicles in the context of draft regulations for ICTS transactions.[2] Under Executive Order 13873, Commerce has authority to regulate ICTS transactions that pose a critical national security threat if the relevant technology is owned by, controlled by, or subject to the jurisdiction or direction of foreign adversary governments and persons. As Commerce advances additional rulemaking, we write to request that you expand the proposed definition of a connected vehicle to include unmanned aerial vehicles (UAV). Otherwise, we request that you launch a new ICTS inquiry into the national security risks posed by UAVs.

The Proposed Rulemaking currently appears to focus on vehicles in the automotive industry. We encourage Commerce to also consider risks related to UAVs. UAV companies headquartered in the People's Republic of China (PRC) control 90 percent of the U.S. consumer market for drones and 70 percent of the global drone market.[3] With UAVs' connected software and hardware posing similar national security threats to those of other identified connected vehicles, such transactions present undue and unacceptable risks to U.S. national security.

---

[1] Press Release, U.S. Department of Commerce, Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles (Feb. 29, 2024), https://www.commerce.gov/news/press-releases/2024/02/citing-national-security-concerns-biden-harris-administration-announces.

[2] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15,066 (Mar. 1, 2024), https://www.federalregister.gov/documents/2024/03/01/2024-04382/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles (EO 13873 CV Advanced Notice of Proposed Rulemaking).

[3] Thomas Black, *The US Can't Let China Dominate the Small-Drone Market*, BLOOMBERG (Apr. 1, 2024), https://www.bloomberg.com/opinion/articles/2024-04-01/the-us-can-t-let-china-dominate-the-small-drone-market; *The Chinese Drone Market Report 2019-2024*, DRONE IND. INSIGHTS, https://droneii.com/product/chinese-drone-market-report (last accessed May 5, 2024).

There is broad bipartisan agreement among Congress and the Executive Branch that PRC UAVs pose serious national security risks. Congress passed, and the President signed, the American Security Drone Act in 2023, which prohibits federal procurement and use of UAVs manufactured or assembled by certain foreign entities, including the PRC, with limited exceptions. This law and additional bills before Congress consider PRC UAVs to pose serious national security risks, a fact with which the Executive Branch concurs. In January 2024, the Cybersecurity and Infrastructure Security Agency, in coordination with the Federal Bureau of Investigation, released a Cybersecurity Guidance memorandum related to PRC-manufactured UAVs, which specifically notes that "while any [UAV] could have vulnerabilities that enable data theft or facilitate network compromises, the [PRC] has enacted laws that provide the government with expanded legal grounds for accessing and controlling data held by firms in China."[4] The Agency released a similar industry alert five years ago, in which it explained that PRC UAVs collect sensitive data, have access to critical systems, and can be required by the PRC Government to hand over data, including to support national intelligence operations.[5] Clearly, PRC UAVs represent a serious risk to national security.

In its Proposed Rulemaking for connected vehicles, the Bureau of Industry and Security (BIS) describes the risks associated with the types of technologies it is considering regulating. It implicitly limits its scope to the automotive industry. Specifically, the Proposed Rulemaking points to "significant data collection not only about the vehicle and its myriad components, but also . . . the vehicle's surroundings, and nearby infrastructure" as principal risks present in connected vehicles.[6] For connected vehicles that BIS anticipates regulating, these risks are particularly acute when the collected data relate to critical infrastructure and public safety systems. Foreign adversaries, as the Proposed Rulemaking correctly notes, are often able to access such data, remotely access the connected vehicles, and push software, firmware, and hardware updates to the vehicle without the user's knowledge. BIS recognizes the novel threat posed by the PRC as it relates to connected vehicles, stating that hundreds of automakers that operate in the PRC are "legally obligated to transmit real-time vehicle data, including geolocation information, to government monitoring centers," and that the issue "is indicative of a broader approach [of the CCP] co-opting private companies" to exploit ICTS vulnerabilities in the United States.[7]

These risks are also presented by PRC-manufactured or controlled UAVs. Much like the connected vehicles in the automotive industry currently considered by the Proposed Rulemaking, UAVs are outfitted with multiple means of data collection and transfer. There are real concerns that data recorded and processed by these systems may be regularly shared with software and hardware teams, including those located in the PRC, to enable real-time determinations of the operator's location and activities, and to provide software updates unbeknownst to the operator.

---

[4] *Cybersecurity Guidance: Chinese-Manufactured UAS*, CYBERSECURITY& INFRASTRUCTURE SEC. AGENCY (Jan. 17, 2024), https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf.
[5] *Industry Alert: Chinese Manufactured Unmanned Aircraft Systems*, CYBERSECURITY& INFRASTRUCTURE SEC. AGENCY (Jun. 3, 2020), https://content.govdelivery.com/attachments/USDHS/2020/06/03/file_attachments/1465486/Industry%20Alert%20-%20Chinese%20Manufactured%20UAS%20%2820%20May%202019%29.pdf.
[6] EO 13873 CV Advanced Notice of Proposed Rulemaking.
[7] *Id.*

The data transmission concerns inherent in connected vehicles currently considered by the Proposed Rulemaking are also present in UAVs. In a March 19, 2024 letter, we wrote to you, the Secretary of the U.S. Department of Homeland Security, and the U.S. Trade Representative, and described the data security issues present in PRC UAVs.[8] We noted that "security flaws [in PRC UAVs] . . . risk putting U.S. persons' data in the hands of the PRC's military and intelligence services," and we further highlighted that "[PRC UAVs] can transmit their GPS location, as well as the coordinates of their operators" back to the PRC, likely to the People's Liberation Army (PLA) as the final end-user.[9] U.S. law enforcement, certain government agencies, and utility companies prolifically use PRC UAVs, which is unsurprising given such UAVs' current dominance of the market. However, this means the PLA and other components of the PRC's national security apparatus can map, analyze, and exploit critical U.S. national security infrastructure.

As mentioned, BIS's Proposed Rulemaking currently defines connected vehicles in a manner that addresses risk in the context of the automotive industry, which is an important and necessary measure. However, because vehicles such as UAVs can pose similar risks to cybersecurity, data privacy, and public safety, Commerce should consider expanding its rulemaking on connected vehicles to include UAVs and other non-automotive vehicles, or otherwise initiate an additional rulemaking for UAVs. While Congress advances bipartisan legislation to address certain threats posed by foreign adversary-made drones, including DJI,[10] these measures are targeted, and comprehensive action from the Executive Branch under existing authorities is worthy of consideration as well. PRC-made UAVs pose national security concerns and should be appropriately controlled by the U.S. Government. Addressing these risks through Commerce's ICTS authorities would be an important step to that end.

Accordingly, we request that BIS consider expanding its definition of connected vehicles to include UAVs in future rulemaking. If it does not, we further request that BIS launch a new investigation into the risks posed by PRC UAVs. Additionally, we request the opportunity to speak with appropriate representatives of Commerce by July 15, 2024 to discuss these matters, including your consideration of UAVs with respect to future regulatory action under your ICTS authorities.

---

[8] Letter to Gina Raimondo, Sec'y Commerce, et al. from Mike Gallagher et al. (Mar. 19, 2024), https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/3.19.24%20Letter%20to%20Raimondo%20Mayorkas%20and%20Tai%20-%20PRC%20UAVs.pdf.

[9] *Id.*

[10] The Countering CCP Drones Act (H.R. 2864) would include DJI on the FCC's Covered List, and the American Security Drone Act recently imposed restrictions on the federal procurement and use of PRC-controlled drones.

We appreciate your attention to this important matter. Thank you for your ongoing work to protect our national security.

Sincerely,

John Moolenaar
Chairman
House Select Committee on the CCP

Raja Krishnamoorthi
Ranking Member
House Select Committee on the CCP

CC: Alan F. Estevez, Under Secretary of Commerce for Industry and Security, U.S. Department of Commerce
Elizabeth Cannon, Executive Director for Information and Communications Technology and Services, U.S. Department of Commerce