wiley

ALERT

Commerce Considers Regulating Connected Vehicles to Protect Against Foreign Adversaries

March 8, 2024

On March 1, 2024, at the direction of President Biden, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) published an Advanced Notice of Proposed Rulemaking (ANPRM) seeking public comment on the proposed regulation of transactions involving Information and Communications Technology and Services (ICTS) that are integral for connected vehicles (CVs). Specifically, BIS is probing the vulnerabilities and threats that could arise if entities owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries (*see* 15 C.F.R. § 7.4(a)) gained access to CV systems or data. Comments on the ANPRM are due Tuesday, April 30, 2024. This new effort continues a trend by the Administration to expand the regulation and security of ICTS across the economy. It should be closely followed by the auto and telecommunication sectors as well as more broadly in the ICTS supply chain because it signals increasing scrutiny of vulnerabilities arising from certain geopolitical adversaries.

What does Executive Order 13873 do?

This ANPRM stems from Executive Order (EO) 13873, "Securing the Information and Communications Technology and Services Supply Chain" (May 15, 2019), which declared a national emergency regarding the ICTS supply chain. In the EO, the President found that a lack of regulation and oversight of the use and acquisition of information and communications technology and services in connected vehicles creates a risk that foreign adversaries can "create and exploit vulnerabilities in information and communications technology or services with potentially catastrophic effects." The EO

Authors

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Paul J. Coyle
Associate
202.719.3446
pcoyle@wiley.law

Practice Areas

Connected & Autonomous Vehicles
International Trade
National Security
Privacy, Cyber & Data Governance
Strategic Competition & Supply Chain
Telecom, Media & Technology
Trade Policy and Trade Negotiations

concludes that this is "an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."

To address these risks, EO 13873 granted to the Secretary of Commerce, in consultation with other agency heads, the broad authority to review and, if necessary, impose mitigation measures on or prohibit any ICTS transaction. Notably, transactions that are subject to review and potential government action include an acquisition, importation, transfer, installation, dealing in, or use of any ICTS by any person, or with respect to any property, subject to United States jurisdiction, when the transaction involves any property in which a foreign country or national has any interest.

The 2019 EO defined a foreign adversary as "any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of the United States" and poses undue or "unacceptable" risks to the national security of the United States or security and safety of U.S. persons. EO 13873 was followed by an Interim Final Rule in January 19, 2021, and a limited-scope final rule (connected software applications) issued on June 16, 2023, in response to a notice of proposed rulemaking on November 26, 2021.

What is BIS concerned about with connected vehicles?

According to the new CV-specific ANPRM, the incorporation by foreign adversaries of ICTS products and services into CVs in the United States could offer such adversaries a direct entry point to sensitive U.S. technologies and data, and it expects that foreign adversaries can bypass measures intended to protect such information. BIS states that adversaries presently are able to engage in malicious cyber activities that harm U.S. persons and critical infrastructure and pose threats to U.S. national security.

A White House fact sheet released with the ANPRM further elaborates how CVs using technology and data systems from foreign adversaries are vulnerable to exploitation. In particular, "[c]onnected vehicles collect large amounts of sensitive data on their drivers and passengers; regularly use their cameras and sensors to record detailed information on U.S. infrastructure; interact directly with critical infrastructure; and can be piloted or disabled remotely." Further, "[c]onnected autos that rely on technology and data systems from countries of concern, including the People's Republic of China, could be exploited in ways that threaten national security." The ANPRM recognizes that these threats are especially concerning in light of the rising market share of Chinese automakers, the use of Chinese parts in new cars, and the Chinese government's ability to access any data at any time from private companies.

What is BIS proposing to do?

Currently, the ANPRM's purpose is to gather information to support the potential development of rules to regulate risks to CVs. The ANPRM therefore requests comment on whether to create a regulatory process by which to permit, regulate, and prohibit specific transactions. Specifically, BIS is seeking input from interested stakeholders to broadly discern the vulnerabilities of CVs, including definitions and analyses of how foreign adversary interference in CV-related ICTS could pose undue or unacceptable risks to U.S. national security. This information gathering will inform next steps in potential regulation. BIS inquires into, among other topics:

- The definition of CVs within the context of transactions involving ICTS incorporated into such vehicles, and potentially also alternative terminology including "networked vehicles," "intelligent connected vehicles," "software-defined vehicles," or "connected autonomous vehicles";
- Information to enhance BIS's understanding of the role that foreign adversaries play in the supply chain for CVs and the leverage that these entities might be able to exert as a result;
- Details of the ICTS supply chain, including software and hardware, and categories of ICTS that are integral to CVs, as well as the market leaders for each phase of the supply chain responsible for those components;
- The geographic locations where software, hardware, and other components are designed, developed, manufactured, or supplied;
- The technological advantage(s) that foreign adversaries have over U.S. and other foreign counterparts in the ICTS market;
- The types of disruptions that may result from ICTS interference by a foreign adversary and risks posed by aftermarket ICTS items;
- Capabilities of CVs including data collection and broad connectivity, types of access or control original equipment manufacturers (OEMs) might have over their CVs, relationships between OEMS and cloud service providers, OEM verification of bill of materials (hardware or software) and ability to authenticate vendors/suppliers, cybersecurity concerns arising from sensors in CVs, and connections to the U.S. charging infrastructure;
- The best practices and industry norms on cybersecurity standards relating to ICTS CVs;
- The specific ICTS in CVs that pose the greatest risks to national security;
- The potential means to narrowly address the involvement of foreign adversaries in CVs and methods to authorize transactions while mitigating national security risks; and
- The economic impact of new regulations on U.S. businesses (including small businesses) and the public, and any anticompetitive effects that could result.

We suggest that clients closely track the issuance of draft rules and regulations and avail themselves of the opportunity to comment either individually or through a trade association. Parties can submit confidential business information within a comment submission without making that information public.

This ANPRM is part of a broader effort by the Biden Administration to strengthen U.S. supply chains and prevent disruption to those supply chains foreign adversaries. On February 28, 2024, President Biden issued EO 14117 entitled, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." The U.S. Department of Justice then issued an ANPRM seeking comment on the regulatory program it is proposing to establish to protect this data by restricting or prohibiting certain transactions with "countries of concern" to protect national security. In February 2024, the Biden Administration issued EO 14116 to bolster the security of critical infrastructure at the nation's ports. In December 2023, Wiley highlighted new restrictions on the U.S. Government procurement of sensitive software and equipment from foreign adversaries and expansion of cybersecurity programs, among other initiatives,

included in the 2024 National Defense Authorization Act (NDAA).

For more information about the ANPRM, please contact one of the attorneys listed on the alert. Wiley has a robust Supply Chain practice, as well as unparalleled experience and expertise in International Trade, National Security, Telecom, Media & Technology, Privacy, Cyber & Data Governance, Government Contracts, and Trade Analytics, and can help clients navigate evolving supply chain developments. Wiley's multidisciplinary team has been helping companies with shifting export controls, entity listings, ICTS supply chain regulations, the Federal Acquisition Security Council, Federal Communications Commission (FCC) supply chain activities, procurement restrictions such as Section 889 and new NDAA restrictions, various regulatory efforts targeting connected vehicles, and work at NIST on cybersecurity, AI, and more. NIST has several workstreams on connected vehicles that may inform this ANPRM and future regulation.

Kurt Gmunder, a Practice Assistant at Wiley Rein LLP, contributed to this alert.