FOR IMMEDIATE RELEASE **BUREAU OF INDUSTRY AND SECURITY**
February 29, 2024
https://bis.doc.gov
OCPA@bis.doc.gov

Office of Congressional and Public Affairs
Media Contact:

Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles with ICTS Components and Systems From Foreign Adversaries

U.S. Department of Commerce Begins Regulatory Process to Consider National Security Risks Posed by ICTS Integral to Connected Vehicles

The Advance Notice of Proposed Rulemaking Seeks Information Regarding the Security of Connected Vehicles with PRC Technology in the U.S.

WASHINGTON, D.C. – Today, the U.S. Department of Commerce issued an advance notice of proposed rulemaking (ANPRM) seeking public comment to inform the potential development of regulations to secure and safeguard the Information and Communications Technology and Services (ICTS) supply chain for connected vehicles (CVs).

"It doesn't take a lot of imagination to think of how foreign government with access to connected vehicles could pose a serious risk to both our national security and the personal privacy of U.S. citizens," **said U.S. Secretary of Commerce Gina Raimondo.** "To assess these national security concerns, we are issuing an Advance Notice of Proposed Rulemaking to investigate the national security risks of connected vehicles, specifically PRC-manufactured technology in the vehicles. We need to understand the extent of the technology in these cars that can capture wide swaths of data or remotely disable or manipulate connected vehicles, so we are soliciting information to determine whether to take action under our ICTS authorities."

"While we benefit greatly from the shift to a more digital and connected world, those connections create new avenues for espionage and sabotage. We must remain vigilant in identifying and securing those vulnerabilities, including potential vulnerabilities present in connected vehicles," **said Under Secretary for Industry and Security Alan Estevez**. "Today's action demonstrates that we are taking thoughtful, deliberative, proactive steps to address concerns that connected vehicles may present for U.S. national security."

The ANPRM explains how the incorporation of foreign adversary ICTS in CVs can create risks, for example, by offering a direct entry point to sensitive U.S. technology and data or by bypassing measures intended to protect U.S. persons' safety and security. In such cases, ICTS provided by persons or entities owned, controlled, or subject to the jurisdiction or direction of a foreign adversary may pose undue risks to critical infrastructure in the United States and unacceptable risks to national security. The People's Republic of China presents a particularly acute and persistent threat to the U.S. ICTS supply chain related to CVs.

This ANPRM demonstrates the Biden-Harris Administration's proactive efforts to address the potential national security risks associated with the ICTS integral to CVs and is a significant step in advancing the ICTS mission.

In this ANPRM, the Department seeks feedback on a number of issues, including: definitions; how potential classes of ICTS transactions integral to CVs may present undue or unacceptable risks to U.S. national security; implementation mechanisms to address these risks through potential prohibitions or, where feasible, mitigation measures; and whether to create a process for the public to request approval to engage in an otherwise prohibited transaction by demonstrating that the risk to U.S. national security is sufficiently mitigated in the context of a particular transaction.

The text of the ANPRM is available online at: https://public-inspection.federalregister.gov/2024-04382.pdf. Comments must be received within 60 days of publication in the Federal Register.

About the Office of Information and Communications Technology and Services (OICTS):

Today's ANPRM is being issued pursuant to the authorities established under Executive Order (E.O.) 13873, "Securing the Information and Communications Technology and Services Supply Chain" (May 15, 2019). E.O. 13873 delegates to the Secretary of Commerce (Secretary) authority to prohibit or impose mitigation measures on any ICTS transaction subject to United States jurisdiction that poses undue or unacceptable risks to U.S. national security or to U.S. persons.
The ICTS program became a mission of BIS in 2022. OICTS is charged with implementing a series of E.O.s under the International Emergency Economic Powers Act (IEEPA) focused on protecting domestic information and communications systems from threats posed by foreign adversaries.

For more information, visit www.bis.doc.gov.

##