FOR IMMEDIATE RELEASE
January 14, 2024

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs https://bis.gov
Media Contact: OCPA@bis.doc.gov

Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats

Washington, D.C. – Today, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) announced a final rule prohibiting certain transactions involving the sale or import of connected vehicles integrating specific pieces of hardware and software, or those components sold separately, with a sufficient nexus to the People's Republic of China (PRC) or Russia.

BIS and its Office of Information and Communications Technology and Services (OICTS) have found that certain technologies originating from the PRC or Russia present an undue and unacceptable risk to U.S. national security. Today's action represents the culmination of a months-long regulatory process to design, seek public input on, and ultimately finalize a measure to protect drivers and passengers on American roads.

"Cars today aren't just steel on wheels – they're computers. They have cameras, microphones, GPS tracking, and other technologies that are connected to the internet. Through this rule, the Commerce Department is taking a necessary step to safeguard U.S. national security and protect Americans' privacy by keeping foreign adversaries from manipulating these technologies to access sensitive or personal information," said **U.S. Secretary of Commerce Gina Raimondo.** "This is a targeted approach to ensure we keep PRC and Russian-manufactured technologies off American roads and protect our nation's connected vehicle supply chains."

"Connected vehicles yield many benefits, but software and hardware sources from the PRC and other countries of concern pose grave national security risks. Today, we are taking strong action to protect Americans against these national security risks by safeguarding our critical infrastructure and automotive supply chain. President Biden has been clear: we will not hesitate to take needed action to protect the safety of the American people," **said National Security Advisor Jake Sullivan.**

"China is trying to dominate the future of the auto industry, but connected vehicles with software and hardware systems linked to foreign adversaries could expose the American people to risks of misuse of their sensitive data or interference by malicious actors," said **National Economic Advisor Lael Brainard. "**Today's rule will prohibit Chinese and Russian software and hardware

from being used in connected vehicles on American roads, protecting consumers and ensuring a more secure American auto industry."

"Today's action is the final step in a comprehensive process to protect America's connected vehicle supply chains from foreign threats. I am confident the work of OICTS, and BIS more broadly, will safeguard the U.S. automotive ecosystem and our national security now and in many years to come," said **Under Secretary of Commerce for Industry and Security Alan F. Estevez**.

"Since publishing our Advance Notice of Proposed Rulemaking in March 2024, OICTS has engaged deeply with industry, civil society, and international partners – including through a robust public comment process – to better understand the connected vehicle supply chain," said **OICTS Executive Director Elizabeth Cannon**. "This final rule reflects significant stakeholder feedback and protects our national security while reducing unintended impacts. We look forward to working with all relevant parties to facilitate compliance as the rule comes into effect."

The final rule establishes that hardware and software integrated into the Vehicle Connectivity System (VCS) and software integrated into the Automated Driving System (ADS), the systems in vehicles that allow for external connectivity and autonomous driving capabilities, present an undue and unacceptable risk to national security when designed, developed, manufactured, or supplied by persons with a sufficient nexus to the PRC or Russia. Malicious access to these critical supply chains could allow our foreign adversaries to extract sensitive data, including personal information about vehicle drivers or owners, and remotely manipulate vehicles.

At this time, given the complexity of the commercial vehicle supply chain, the final rule applies only to passenger vehicles (defined as those under 10,001 pounds). BIS recognizes the acute national security threat presented by foreign adversary involvement in the commercial vehicle supply chain and intends to issue a separate rulemaking addressing the technologies present in connected commercial vehicles – including in trucks and buses – in the near future.

Today's final rule prohibits the import of VCS hardware or connected vehicles containing such hardware, and the import and sale of vehicles containing VCS or ADS software, with a sufficient nexus to the PRC or Russia. VCS is defined as the set of systems that allow the vehicle to communicate externally, including telematics control units, Bluetooth, cellular, satellite, and Wi-Fi modules. ADS includes the components that collectively allow a highly autonomous vehicle to operate without a driver.

The rule also prohibits manufacturers with a sufficient nexus to the PRC or Russia from selling new connected vehicles that incorporate VCS hardware or software or ADS software in the United States, even if the vehicle was made in the United States.

The software-related prohibitions will take effect for Model Year 2027. The hardware-related prohibitions will take effect for Model Year 2030, or January 1, 2029, for units without a model year. Prohibitions on the sale of connected vehicles by manufacturers with a sufficient nexus to the PRC or Russia, even if manufactured in the United States, take effect for Model Year 2027.

The rule requires certain importers and manufacturers to submit annual Declarations of Conformity to certify their compliance with the prohibitions. The final rule allows Commerce to issue General Authorizations for certain types of transactions posing lower risk. It also allows regulated parties to seek Specific Authorizations permitting them to engage in otherwise prohibited transactions, as well as advisory opinions to ask BIS for a determination if a prospective transaction may fall within the scope of the rule.

The final rule follows a Notice of Proposed Rulemaking (NPRM) published by BIS on September 26, 2024, and an Advance Notice of Proposed Rulemaking (ANPRM) published by BIS on March 1, 2024.

The final rule is implemented under BIS's ICTS authorities, as provided for under Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain." EO 13873 allows the Department of Commerce to issue regulations that establish criteria by which particular technologies may be included in EO 13873's prohibitions when transactions involving those technologies (1) pose an undue or unacceptable risk of sabotage to or subversion of ICTS in the United States; (2) pose an undue risk of catastrophic effects on the security or resiliency of U.S. critical infrastructure or the digital economy of the United States; or (3) otherwise pose an unacceptable risk to the national security of the United States or the security and safety of U.S. persons.

Additional Information:

The text of the final rule is available on the Federal Register's website here. The final rule will become effective 60 days after publication, on March 17, 2025. Regulated entities may contact the OICTS Compliance and Adjudication Division for questions related to this final rule at CV-intake@bis.doc.gov.