DEBBIE DINGELL
6TH DISTRICT, MICHIGAN

102 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225–4071

HOUSE COMMITTEE ON
ENERGY AND COMMERCE
SUBCOMMITTEES ON
HEALTH
INNOVATION, DATA, AND COMMERCE
COMMUNICATIONS AND TECHNOLOGY

HOUSE COMMITTEE ON
NATURAL RESOURCES
SUBCOMMITTEES ON
WATER, WILDLIFE, AND FISHERIES
ENERGY AND MINERAL RESOURCES

OVERSIGHT AND ACCOUNTABILITY
SELECT SUBCOMMITTEE ON
THE CORONAVIRUS PANDEMIC

Congress of the United States
House of Representatives
Washington, DC 20515

DISTRICT OFFICES:

2006 HOGBACK ROAD
SUITE 7
ANN ARBOR, MI 48105
(734) 481–1100

WOODHAVEN CITY HALL
21869 WEST ROAD
WOODHAVEN, MI 48183
(313) 278–2936

WEBSITE: DEBBIEDINGELL.HOUSE.GOV

October 16, 2024

The Honorable Gina Raimondo
Secretary
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Dear Secretary Raimondo:

I am writing to express my strong support for the Department of Commerce Bureau of Industry and Security's (BIS) Notice of Proposed Rulemaking (NPRM) aimed at prohibiting the sale and import of connected vehicles incorporating specific hardware and software components with a sufficient nexus to the People's Republic of China (PRC) or Russia. As our vehicles become smarter and more connected, it is crucial that we address the national security risks posed by these components. This initiative directly addresses significant national security concerns stemming from the increasing prevalence of Chinese Original Equipment Manufacturers (OEMs) in the global automotive market.

China's emergence as the second largest vehicle exporter in 2023 underscores the urgency of this matter. The Chinese Communist Party's (CCP) pervasive control and broad legal framework over its industries raises serious concerns about the potential for data exploitation and the weaponization of technology embedded within Chinese-made vehicles. As you know, the CCP requires companies to share data with the government upon request.

This inherent vulnerability extends to data from connected vehicles, presenting a clear and present danger to the United States. It is well-documented that Chinese OEMs are deploying autonomous vehicles (AVs) in the U.S. These vehicles' sophisticated suites of sensors and cameras can gather precise and detailed data about the vehicles' surroundings. Taken together, the result will reveal massive amounts of real-time information about our nation's roadways and critical infrastructure, as well as the location of the occupants of those vehicles and of the vehicles and people in the vehicle's proximity. The CCP can access the vast amounts of data from connected cars with Chinese hardware and software components, raising real and serious national security concerns. This risk extends not just to Chinese OEMs, but to many Chinese-

made components incorporated into other connected cars. These Chinese-made components may also pose an immediate threat to vehicle safety, and these systems could be exploited by malicious actors to remotely control vehicles on our roads.

Nearly 70% of vehicles on American roads are now connected — they rely on internet-enabled services and advanced software to manage functions such as navigation, vehicle diagnostics, and even autonomous driving features. The data these connected vehicles and their technologies generate also include highly sensitive information. When this technology is manufactured or controlled by companies with close ties to the CCP, our data becomes vulnerable to foreign access and exploitation.

I commend BIS for proactively addressing these risks through this NPRM. The proposed restrictions on hardware and software designed, developed, manufactured, or supplied by Chinese or Russian-controlled entities represent a critical step toward safeguarding our national security. It will also prevent foreign adversaries from accessing our most sensitive infrastructure and consumer data.

Given the gravity of these implications, I ask if the Department would provide a briefing to the relevant Congressional caucuses, such as the Auto Caucus and the Autonomous Vehicle (AV) Caucus on the NPRM, its implementation strategy, and the ongoing assessment of risks posed by Chinese and Russian-controlled components in connected vehicles. This briefing would allow Members of Congress to better understand the nuances of the rule and offer any potential assistance.

I also strongly encourage the Department to finalize this rulemaking process without delay, given the urgency of the threat posed by these technologies. The potential threats require a swift response, and I am ready to assist in any way possible to streamline the process and ensure its effective enforcement. Should any legislative support be required to strengthen or clarify the rule's provisions, I am committed to working collaboratively with both parties in both chambers of Congress to ensure its success.

Thank you for your leadership on this issue, and I look forward to your response and to continuing to work together to keep Americans safe.

Sincerely,

Debbie Dingell

Debbie Dingell
Member of Congress