

# AUTOMOTIVE RIGHT TO REPAIR IN MAINE



Representative Amanda Collamore & Representative Tiffany Roberts

## Table of Contents

Maine Citizen’s Guide to the Referendum Election .....	Page 1
Alliance for Automotive Innovation Complaint .....	Page 17
Automotive Right to Repair Working Group Report.....	Page 51
Massachusetts Right to Repair Law.....	Page 72
NHTSA National Traffic and Motor Vehicle Safety Letter .....	Page 80
NHTSA National Traffic and Motor Vehicle Safety Letter 2 .....	Page 82
Automotive Repair Data Sharing Commitment.....	Page 88
Right to Repair MOU.....	Page 93
CRS Access to Motor Vehicle Software and Data .....	Page 101
GAO Vehicle Repair Report .....	Page 131
ITC Investigation Report No. 337-TA-1393 .....	Page 147
Dept. of Commerce Bureau of Security Rulemaking Notice .....	Page 149
Dept. of Commerce Bureau of Security Rulemaking Advance Notice .....	Page 186

*Collated and prepared by Representatives Collamore and Roberts*

# Maine Citizen's Guide to the Referendum Election

Secretary of State's Office

Tuesday, 11/7/2023

Note: To ensure that the appropriate documents are provided, only the title page, letter, Listing of questions, and Questions 4 are included in this portion of the packet.

**Maine Citizen's Guide to the  
Referendum Election**

**Tuesday, November 7, 2023**



**In Accordance with  
the April 7<sup>th</sup>, 2023 Proclamation of the Governor  
and with the Acts Passed by the 131<sup>st</sup> Legislature  
at the First Special Session**

**Shenna Bellows  
Secretary of State**

Appropriation 014 29A 069202



**State of Maine  
Office of the Secretary of State  
Augusta, Maine 04333**

Dear Fellow Citizen,

The information in this booklet is intended to help voters learn about the questions that will appear on the November 7, 2023 Referendum Election ballot. Referendum elections are an important part of the heritage of public participation in Maine.

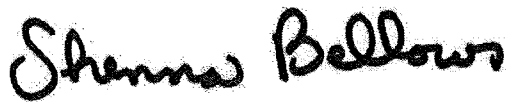
Inside this booklet, you will find:

- ♦ the referendum questions;
- ♦ the legislation each question represents;
- ♦ a summary of the intent and content of the legislation;
- ♦ an explanation of the significance of a “yes” or “no” vote;
- ♦ an estimate of the fiscal impact of each referendum question on state revenues, appropriations and allocations; and
- ♦ public comments filed in support of or in opposition to each ballot measure.

For information about how and where to vote, please contact your local Municipal Clerk or call Maine’s Division of Elections at 207-624-7650. Information is also available online at [www.maine.gov/sos](http://www.maine.gov/sos).

The Department of the Secretary of State, the Attorney General, the State Treasurer and the Office of Fiscal and Program Review have worked together to prepare this booklet of information, and we hope you find it helpful.

Sincerely,

A handwritten signature in black ink that reads "Shenna Bellows". The script is cursive and fluid, with the first name "Shenna" and last name "Bellows" clearly distinguishable.

Shenna Bellows  
Secretary of State

**State of Maine**  
**Referendum Election, November 7, 2023**  
**Listing of Referendum Questions**

**Question 1: Citizen's Initiative**

Do you want to bar some quasi-governmental entities and all consumer-owned electric utilities from taking on more than \$1 billion in debt unless they get statewide voter approval?

**Question 2: Citizen's Initiative**

Do you want to ban foreign governments and entities that they own, control, or influence from making campaign contributions or financing communications for or against candidates or ballot questions?

**Question 3: Citizen's Initiative**

Do you want to create a new power company governed by an elected board to acquire and operate existing for-profit electricity transmission and distribution facilities in Maine?

**Question 4: Citizen's Initiative**

Do you want to require vehicle manufacturers to standardize on-board diagnostic systems and provide remote access to those systems and mechanical data to owners and independent repair facilities?

**Question 5: Constitutional Amendment**

Do you favor amending the Constitution of Maine to change the time period for judicial review of the validity of written petitions from within 100 days from the date of filing to within 100 business days from the date of filing of a written petition in the office of the Secretary of State, with an exception for petitions filed within 30 calendar days before or after a general election?

**Question 6: Constitutional Amendment**

Do you favor amending the Constitution of Maine to require that all of the provisions of the Constitution be included in the official printed copies of the Constitution prepared by the Secretary of State?

**Question 7: Constitutional Amendment**

Do you favor amending the Constitution of Maine to remove a provision requiring a circulator of a citizen's initiative or people's veto petition to be a resident of Maine and a registered voter in Maine, requirements that have been ruled unconstitutional in federal court?

**Question 8: Constitutional Amendment**

Do you favor amending the Constitution of Maine to remove a provision prohibiting a person under guardianship for reasons of mental illness from voting for Governor, Senators and Representatives, which the United States District Court for the District of Maine found violates the United States Constitution and federal law?

---

#### **Question 4: Citizen's Initiative**

*Do you want to require vehicle manufacturers to standardize on-board diagnostic systems and provide remote access to those systems and mechanical data to owners and independent repair facilities?*

---

### **STATE OF MAINE**

#### **“An Act Regarding Automotive Right to Repair”**

**Be it enacted by the People of the State of Maine as follows:**

**Sec. 1. 29-A MRSA §1801, sub-§2-A** is enacted to read:

**2-A. Mechanical data.** "Mechanical data" means any vehicle-specific data, including telematics system data, generated by, stored in or transmitted by a motor vehicle and used in the diagnosis, repair or maintenance of a motor vehicle.

**Sec. 2. 29-A MRSA §1801, sub-§6** is enacted to read:

**6. Telematics system.** "Telematics system" means a system in a motor vehicle that collects information generated by the operation of the vehicle and transmits that information using wireless communications to a remote receiving point where the information is stored or used.

**Sec. 3. 29-A MRSA §1810** is enacted to read:

**§1810. Right to repair**

**1. Access to diagnostic systems.** Access to the vehicle on-board diagnostic systems of all motor vehicles, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, must be standardized and made accessible to owners and independent repair facilities and the access may not require authorization by the manufacturer, directly or indirectly, unless that authorization is standardized across all makes and models of motor vehicles sold in this State and is administered by the independent entity described in subsection 2.

**2. Independent entity.** The Attorney General shall designate an independent entity not controlled by one or more motor vehicle manufacturers to establish and administer access to vehicle-generated data that is available through the on-board diagnostic system or that is transmitted by the standardized access platform authorized under this section. The independent entity must consist of one representative each from a cross section of industry trade groups including but not limited to organizations representing motor vehicle manufacturers, aftermarket parts manufacturers, aftermarket parts distributors and retailers, independent motor vehicle service providers and new car dealers. The independent entity shall manage cyber-secure access to motor vehicle-generated data, including ensuring on an ongoing basis that access to the on-board diagnostic system and standardized access platform is secure based on all applicable United States and international standards. The independent entity shall:

A. Identify and adopt relevant standards for implementation of this section and relevant provisions for accreditation and certification of organizations and for a system for monitoring policy compliance;

B. Monitor and develop policies for the evolving use and availability of data generated by the operations of motor vehicles; and

C. Create policies for compliance with relevant laws, regulations, standards, technologies and best practices related to access to motor vehicle data.

**3. Model year 2002 motor vehicles.** For model year 2002 motor vehicles, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, each manufacturer of motor vehicles sold in this State shall make available for purchase under fair and reasonable terms by owners and independent repair facilities all diagnostic repair tools, parts, software and components incorporating the same diagnostic, functional repair and wireless capabilities that the manufacturer makes available to its authorized repair shops. Each manufacturer shall:

A. Provide diagnostic repair information to each aftermarket scan tool company and each 3rd-party service information provider with whom the manufacturer has appropriate licensing, contractual or confidentiality agreements for the sole purpose of building aftermarket diagnostic tools and 3rd-party service information publications and systems. Once a manufacturer makes information available pursuant to this paragraph, the manufacturer is considered to have satisfied its obligations under this paragraph and thereafter is not responsible for the content and functionality of aftermarket diagnostic tools or service information systems;

B. Make available for purchase by owners of motor vehicles and by independent repair facilities the same diagnostic and repair information, including repair technical updates, that the manufacturer makes available to its authorized repair shops through the manufacturer's Internet-based diagnostic and repair information system; and

C. Provide access to the manufacturer's diagnostic and repair information system for purchase by owners of motor vehicles and independent repair facilities on a daily, monthly and yearly subscription basis and upon fair and reasonable terms.

All parts, tools, software and other components necessary to complete a full repair of the vehicle, as referenced in this subsection, must be included and provided to owners of motor vehicles and authorized independent repair shops.

**4. Model year 2002-2017 motor vehicles.** For model year 2002-2017 motor vehicles, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, access to a vehicle's on-board diagnostic and repair information system must be the same for an owner or an independent repair facility as that provided to a new vehicle dealer.

**5. Model year 2018 and later motor vehicles.** For model year 2018 and later motor vehicles, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, access to the on-board diagnostic and repair information system must be available through use of an off-the-shelf personal computer with sufficient memory, processor speed, connectivity and other capabilities as specified by the vehicle manufacturer and:

A. A nonproprietary vehicle interface device that complies with SAE International standard J2534, SAE International standard J1939, commonly referred to as SAE J2534 and SAE J1939, the International Organization for Standardization standard 22900, commonly referred to as ISO 22900, or any successor to SAE J2534, SAE J1939 or ISO 22900 as may be accepted or published by SAE International or the International Organization for Standardization, as appropriate;

B. An on-board diagnostic and repair information system integrated into and entirely self-contained within the vehicle, including, but not limited to, service information systems integrated into an on-board display; and

C. A system that provides direct access to on-board diagnostic and repair information through a nonproprietary vehicle interface, such as ethernet, universal serial bus or digital versatile disc.

Each manufacturer shall provide access to the same on-board diagnostic and repair information available to their dealers, including technical updates to such on-board systems, through such nonproprietary interfaces as referenced in this subsection. All parts, tools, software and other components necessary to complete a full repair of a vehicle, as referenced in this subsection, must be included and provided to motor vehicle owners and authorized independent repair shops.

**6. Required equipment.** Not later than one year from the effective date of this section, a manufacturer of motor vehicles sold in this State, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, that uses a telematics system is required to equip vehicles sold in this State with an inter-operable, standardized and owner-authorized access platform across all of the manufacturer's makes and models. The platform must be capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform. The platform must be directly accessible by the motor vehicle owner through a mobile-based application and, upon the authorization of the owner, all mechanical data must be directly accessible by an independent repair facility or a licensed dealer as described in section 851, subsections 2 and 9, limited to the time to complete the repair or for a period of time agreed to by the motor vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle. Access must include the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair. All parts, tools, software and other components necessary to complete a full repair of the vehicle, as referenced in this subsection, must be included and provided to motor vehicle owners and authorized independent repair shops.

**7. Exclusions.** Manufacturers of motor vehicles sold in the United States may exclude diagnostic, service and repair information necessary to reset an immobilizer system or security-related electronic modules from information provided to motor vehicle owners and independent repair facilities. If excluded under this subsection, the information necessary to reset an immobilizer system or security-related electronic modules must be made available to motor vehicle owners and independent repair facilities through the secure data release model system as used on the effective date of this section by the National Automotive Service Task Force or other known, reliable and accepted systems.

**8. Enforcement.** If the independent entity described by subsection 2 has reason to believe that a manufacturer has violated any provision of this section, the independent entity shall notify the Attorney General. The Attorney General shall promptly institute any actions or proceedings the Attorney General considers appropriate. The independent entity, through the Attorney General, may apply to the Superior Court of any county of the State to enforce any lawful order made or action taken by the independent entity pursuant to this section.

A motor vehicle owner or independent repair facility authorized by an owner who has been denied access to mechanical data in violation of this section may initiate a civil action seeking any remedies under law. Each denial of access is compensable by an award of treble damages or \$10,000, whichever amount is greater.

Sec. 4. 29-A MRSA §1811 is enacted to read:

**§1811. Telematics system notice**

**1. Notice.** The Attorney General shall establish for prospective motor vehicle owners a motor vehicle telematics system notice that includes, but is not limited to, the following features:

A. An explanation of telematics systems and their purposes;

B. A description summarizing the mechanical data collected, stored and transmitted by a telematics system;

C. The prospective motor vehicle owner's ability to access the vehicle's mechanical data through a mobile device; and

D. A motor vehicle owner's right to authorize an independent repair facility to access the vehicle's mechanical data for vehicle diagnostics, repair and maintenance purposes.

**2. Notice form.** The notice form must provide for the prospective motor vehicle owner's signature certifying that the prospective owner has read the telematics system notice under subsection 1.

**3. Provision of notice.** When selling or leasing motor vehicles containing a telematics system, a dealer as defined in section 851, subsection 2 and a new vehicle dealer as defined in section 851, subsection 9 shall provide the telematics system notice under subsection 1 to the prospective owner, obtain the prospective owner's signed certification that the prospective owner has read the notice and provide a copy of the signed notice to the prospective owner. A dealer's failure to comply with the provisions of this subsection is grounds for any action by the licensing authority relative to the dealer's license, up to and including revocation.

**SUMMARY**

This initiated bill requires manufacturers of certain motor vehicles to standardize the vehicle on-board diagnostic systems and make those systems accessible to owners and independent repair facilities. It requires the Attorney General to designate an independent entity to administer the accessibility of vehicle on-board diagnostic systems by adopting standards and developing policies. The initiated bill requires the release of certain diagnostic repair tools, parts, software and components depending on model year of the motor vehicle. It also requires certain motor vehicles to be equipped with a standard access platform and provides exclusions for information otherwise required to be shared with owners or independent repair shops if that information is necessary for immobilizer systems or security-related modules. The initiated bill provides for enforcement by civil action of the provisions related to access and information sharing and provides the available damages. It also requires that the Attorney General establish a notice relating to motor vehicle telematics systems and requires dealers of certain motor vehicles to provide that notice to potential owners of motor vehicles, and it provides for an administrative consequence if a dealer does not comply.

**Intent and Content**  
**Prepared by the Office of the Attorney General**

This citizen-initiated bill is intended to require automakers to take steps, including expanding access to on-board vehicle diagnostic systems, to make it easier for vehicle owners and independent repair shops to diagnose, repair, and maintain motor vehicles.

**Access to On-Board Diagnostic Systems.** The initiated measure would require vehicle manufacturers to standardize and make available to owners and independent repair shops the on-board diagnostic systems of all vehicles, including commercial vehicles and heavy-duty vehicles. Manufacturers could not require authorization for owners and independent repair shops to access these systems, except through a standardized authorization process administered by an independent entity chosen by the Maine Attorney General.

Specific access requirements would depend on the model year of the vehicle:

*Model year 2018 and later.* Vehicles with model years of 2018 and later would be required to have an on-board diagnostic system that could be accessed using an off-the-shelf personal computer. The system would also have to be accessible using certain other technologies. Manufacturers would also need to provide access to all parts, tools, software, and other components necessary to repair the vehicle.

*Model years 2002 to 2017.* Vehicles with model years between 2002 and 2017 would have to provide the same access to on-board diagnostic and repair information systems to owners and independent repair shops as is provided to new vehicle dealers.

*Model year 2002.* For vehicles with a 2002 model year, manufacturers would have to sell, under fair and reasonable terms, diagnostic repair tools, parts, software, and components that have the same capabilities as those the manufacturer makes available to its authorized repair shops. Manufacturers would also have to provide information to certain aftermarket scan tool companies, make available for purchase the same diagnostic repair information that the manufacturer makes available through its Internet-based diagnostic and repair information system, and provide access to the manufacturer's diagnostic and repair information system for purchase on a daily, monthly, and yearly subscription basis. Finally, manufacturers would have to provide access to all parts, tools, software, and other components necessary to repair the vehicle.

*Model years prior to 2002.* The initiated measure has no provisions specifically addressing vehicles older than model year 2002.

**Telematics Access Platform.** The initiated measure would require manufacturers that use telematics systems to equip all new vehicles with a standardized platform to access vehicle information. A telematics system, as defined by the measure, collects information generated by a vehicle's operation and transmits that information using wireless communications to a remote receiving point. The required telematics access platform must be able to securely communicate all vehicle-specific data generated by, stored in or transmitted by the vehicle and used for diagnosis, repair, or maintenance of the vehicle. The platform must be accessible to the owner through a mobile



app and must permit the owner to authorize dealers and independent repair shops to access the data. The platform must also include the ability to send commands to vehicle components if needed for maintenance, diagnosis, or repair.

**Exception for Security Systems.** Vehicle manufacturers would not be required to provide access to information needed to reset a vehicle immobilizer system or security-related electronic modules. However, if such information is withheld, the manufacturers must make such information available through the secure data release model system used by the National Automotive Service Task Force, or some other known, reliable and accepted system.

**Oversight.** The measure requires the Maine Attorney General to designate an independent entity to establish and administer access to vehicle data. The entity must include representatives of various industry trade groups and may not be controlled by vehicle manufacturers. The entity must manage cyber-secure access to vehicle data. It must also ensure that access to vehicles' on-board diagnostic system and standardized access platform is secure under United States and international standards. The entity must identify and adopt various standards and policies relating to data access.

If the independent entity has reason to believe that a manufacturer has violated any provision of the measure, it must notify the Attorney General. The measure directs the Attorney General to promptly institute any actions or proceedings he or she deems appropriate. The Attorney General may also seek court enforcement of any lawful order made or action taken by the independent entity.

The measure also requires the Attorney General to establish a notice for prospective vehicle owners containing certain information, including the owner's ability to access the vehicle's mechanical data through a mobile device and right to authorize an independent repair facility to access the vehicle's mechanical data. Dealers would be required to provide the notice to prospective owners and obtain a signed certification that the prospective owner has read the notice.

**Civil Remedy.** The initiated measure allows a vehicle owner or independent repair shop authorized by an owner to sue a vehicle manufacturer for denying access to mechanical data. For each denial of access, the owner or repair shop is entitled to recover 3 times their actual damages or \$10,000, whichever is greater.

A "YES" vote is to enact the initiated legislation.

A "NO" vote opposes the initiated legislation.

**Fiscal Impact Statement**  
**Prepared by the Office of Fiscal and Program Review**

This citizen initiative proposes to require manufacturers of certain motor vehicles to standardize the vehicle on-board diagnostic systems and to make those systems accessible to motor vehicle owners and independent repair facilities.

Enforcement of this initiative may require the Office of the Attorney General (AG) to take court action. Assuming that this requires one half-time Assistant Attorney General position in the Office of the Attorney General, the ongoing annual costs to pursue and address violations will be approximately \$65,000 annually. In the event the initiative itself becomes the subject of litigation, there may be additional costs to the AG to defend the new law in court. Any additional costs to the AG to establish a notice for prospective motor vehicle owners regarding motor vehicle telematics systems are not expected to be significant.

This initiative may increase the number of civil suits filed in the court system. The additional workload associated with the minimal number of new cases does not require additional funding for the Judicial Department. The collection of additional filing fees will increase General Fund and dedicated revenue by minor amounts.

## Public Comments

### **Public Comment in Support of Question 4**

Comment submitted by:

Tim Winkeler

Maine Automotive Right to Repair

15 Rebecca Way

Falmouth, ME 04105

Maine's automotive right to repair citizen's initiative allows access to owners and independent auto repair shops to the vehicle on-board diagnostic systems, parts, software, and components of all motor vehicles, including commercial motor vehicles and heavy-duty vehicles having a gross vehicle weight rating of more than 14,000 pounds through the following:

- This initiated bill requires manufacturers of certain motor vehicles to standardize the vehicle on-board diagnostic systems and make those systems accessible to owners and independent repair facilities.
- It requires the Attorney General to designate an independent entity to administer the accessibility of vehicle on-board diagnostic systems by adopting standards and developing policies.
- The initiated bill requires the release of certain diagnostic repair tools, parts, software and components and it also requires certain motor vehicles to be equipped with a standard access platform and provides exclusions for information otherwise required to be shared with owners or independent repair shops if that information is necessary for immobilizer systems or security-related modules.
- The initiated bill provides for enforcement by civil action of the provisions related to access and information sharing and provides the available damages. It also requires that the Attorney General establish a notice relating to motor vehicle telematics systems and requires dealers of certain motor vehicles to provide that notice to potential owners of motor vehicles, and it provides for an administrative consequence if a dealer does not comply.

Protect your car repair choice and vote YES on question 4!

The printing of this public comment does not constitute an endorsement by the State of Maine, nor does the State warrant the accuracy or truth of any statements made in the public comment.
--

## Public Comment in Opposition to Question 4

Comment submitted by:  
Robert L. Redding, Jr.  
Washington, D.C. Representative  
Automotive Service Association  
313 Massachusetts Avenue, N.E.  
Washington, D.C. 20002

The Automotive Service Association (ASA) is the oldest and largest national organization committed solely to protecting independent automotive repair shops. Our members own and operate automotive mechanical and collision repair facilities. Independent repair shops are responsible for the majority of all post-warranty repairs and collision repairs in the United States.

Our members are on the front lines of the right-to-repair issue. That is why, over the past several decades, ASA reached agreements with automotive manufacturers to secure the right of vehicle owners to repair their vehicle or bring it to a repair facility of their choosing. In July 2023, ASA, the Society of Collision Repair Shops, and the Alliance for Automotive Innovation (the trade group whose members manufacture 98% of vehicles on the road in the United States) reached a new vehicle data access agreement. Manufacturers committed to provide owners and independent repairers access to the data, systems, and tools needed to diagnose and repair vehicle issues, even if it requires telematics (wireless communication between a vehicle and an external device) access, the vehicle operates on alternative fuel sources, or it is equipped with any other technology. Not only have these agreements endured, but they also have provided direct channels of communication between repairers and manufacturers, enabling quick resolution to instances in which a repairer lacked data access.

Ballot Question 4 is unnecessary because the agreements in place already provide vehicle owners a competitive automotive repair market. However, approving Ballot Question 4 would create new legal obstacles that could impede repairers from working directly with manufacturers to quickly resolve data access issues. Furthermore, it could burden independent repairers with new cybersecurity liabilities based on access to data beyond what is needed to diagnose and repair their customers' vehicles.

ASA urges you to vote NO on Ballot Question 4.

<p>The printing of this public comment does not constitute an endorsement by the State of Maine, nor does the State warrant the accuracy or truth of any statements made in the public comment.</p>
---

## **Public Comment in Opposition to Question 4**

Comment submitted by:  
Wayne Weikel  
Automakers and Repairers for Vehicle Repair Choice  
P.O. Box 4543  
Portland, ME 04112

### **Question 4 is entirely unnecessary.**

Automotive right to repair already exists. Every vehicle owner in Maine today has a choice and the absolute right to get your car fixed anytime, anyplace and anywhere.

In fact, automakers and independent repairers are in total agreement: Maine repairers should be guaranteed access to the same repair information and tools provided to auto dealers.

If you ask repairers, they will say they already have all the necessary repair information.

That's not going to change and why Question 4 isn't necessary.

### **Question 4 is backed by out-of-state, big box retailers.**

The referendum is backed by companies headquartered outside of Maine that really want instant and remote access to the electronic data produced by today's high-tech vehicles.

Like what? Navigation, location information, airbag deployment and crash notifications.

Why? So, they can use your private information to try and sell or market their products directly through your vehicle's computer screen.

### **Question 4 puts your privacy and vehicle security at risk.**

Instant and remote access to your vehicle data puts your personal privacy at risk and presents a security threat to you and other vehicles on the road.

How? The cybersecurity protections that manufacturers currently install in vehicles sold across Maine will need to be disabled if Question 4 passes.

Government car safety authorities have warned this could make your vehicle vulnerable to hacking and cyberattacks.

*(cont'd next pg.)*

The printing of this public comment does not constitute an endorsement by the State of Maine, nor does the State warrant the accuracy or truth of any statements made in the public comment.
--

**Responsible Maine Car Owners should Vote No on Question 4.**

Today's automotive repair market is working just fine. Automotive right to repair already exists.

Car owners have a range of vehicle repair options. Independent repairers have said they have all the information necessary to repair vehicles.

Question 4 will undo what already works and put your privacy – and the security of vehicles on the road – at risk.

Vote NO on Question 4.

The printing of this public comment does not constitute an endorsement by the State of Maine, nor does the State warrant the accuracy or truth of any statements made in the public comment.

# Alliance for Automotive Innovation Complaint

Against Aaron Frey, Attorney General of the State of Maine  
in his official capacity

Files 1/31/2025

Case 1:25-cv-00041-LEW

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MAINE**

ALLIANCE FOR AUTOMOTIVE  
INNOVATION

Plaintiff,

vs.

AARON FREY, ATTORNEY GENERAL OF  
THE STATE OF MAINE in his official  
capacity,

Defendant.

C.A. No. \_\_\_\_.

**COMPLAINT**

Plaintiff Alliance for Automotive Innovation (Auto Innovators) brings this complaint against Defendant, the Attorney General of the State of Maine, for declaratory and injunctive relief, and alleges as follows:

**INTRODUCTION**

1. This action challenges the threatened and actual enforcement of 29-A M.R.S. § 1810 (the “Data Law”). An express and critical prerequisite for compliance with the Data Law—an “independent entity” to develop and administer data access to vehicles—does not exist. Because compliance with the Data Law is impossible and the Data Law is unconstitutionally vague, the Data Law violates due process and harms vehicle manufacturers. Moreover, any means of compliance with the law that does not ensure cybersecurity, including any compliance strategies without the establishment of the “independent entity,” is preempted by federal law.

2. The nation’s leading car and light truck manufacturers—the members of Auto Innovators—take seriously their role as careful stewards of sensitive vehicle data. Each member



recognizes that unauthorized access to that data, and to the secured vehicle systems that generate that data, could, in the wrong hands, spell disaster.

3. To that end, vehicle manufacturers have developed and implemented hardware- and software-based security measures in their vehicles to ensure the integrity of their vehicle systems and the data contained on them. These security measures are intended to ensure that, *inter alia*, nefarious actors cannot remotely access or alter vehicle systems and data that control safety-critical functions, such as acceleration, braking, steering, and airbag deployment. However, access to vehicle systems and the accompanying security for that access is not subject to any particular or precise standard currently existing, and generally is administered by vehicle manufacturers themselves.

4. Despite the risks of providing external access to vehicle data, subsection 6 of Maine's new Data Law ("Subsection 6") states that, beginning no later than January 5, 2025, vehicle manufacturers must provide access "through a mobile-based application" to an "inter-operable, standardized and owner-authorized access platform across all of the manufacturer's makes and models." 29-A M.R.S. § 1810(6). The Data Law states this "platform must be capable of *securely* communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform." *Id.* (emphasis added).

5. Subsection 2 of the Data Law ("Subsection 2") requires that the Defendant, the Attorney General of the State of Maine, "designate an independent entity . . . to establish and administer access to vehicle-generated data . . . that is transmitted by [that] standardized access platform . . . ." *Id.* § 1810(2). The Data Law mandates that such entity "shall manage cyber-secure access to motor vehicle-generated data, including by ensuring on an ongoing basis that access to the . . . standardized access platform is secure" based on U.S. and international standards. *Id.* The

Data Law further mandates that such entity must, *inter alia*, adopt relevant standards and create policies for compliance with laws, regulations, standards, technologies, and best practices related to the access of motor vehicle data. *Id.*

6. Similarly, subsection 1 of the Data Law (“Subsection 1”) mandates that access to vehicles’ on-board diagnostic (“OBD”) systems “may not require authorization by the manufacturer, directly or indirectly,” unless that authorization “is administered by the independent entity described in [S]ubsection 2.” *Id.* § 1810(1). The Data Law does not permit any other form of “authorization” for access to OBD systems.

7. Thus, for Auto Innovators’ members to even attempt to comply with the Data Law’s “access” requirements, or to authorize only legitimate actors to access OBD systems, several steps must have occurred: (a) the Attorney General must have designated the relevant “independent entity”; (b) that independent entity must have established and begun to administer access to vehicles through the “standardized access” platform that the Data Law contemplates, having adopted standards and policies to ensure that such access would be consistent with laws, regulations, standards, and best practices regarding access for motor vehicle data; and (c) Auto Innovators’ members must have had the opportunity to implement that “standardized access” platform in their vehicles.

8. None of these steps has occurred—not even the Attorney General’s designation of the independent entity that is the precursor to establishment of the “standardized access” platform that the Data Law contemplates. Accordingly, Auto Innovators’ members have no ability even to start to comply with the Data Law.

9. Though they have no means of complying with the Data Law, vehicle manufacturers’ purported failure to comply would subject them to substantial fines, amounting to

\$10,000 per violation—several times the manufacturers’ profit margin on a given vehicle. Moreover, a violation of the Data Law can constitute criminal liability, as such violations constitute Class E crimes that are punishable by up to \$500 per violation, imprisonment of not more than 30 days, or both.

10. Further, the Attorney General recently has taken the position that the Data Law is immediately enforceable against Auto Innovators’ members. In particular, the Attorney General has taken the position that the requirement for a “standardized and owner-authorized access platform” in Subsection 6 of the Data Law is effective and enforceable against Auto Innovators’ members as of January 5, 2025. Given that the Attorney General has not designated the independent entity necessary to administer access to the “platform” referenced in Subsection 2 of the Data Law, his position concerning the immediate enforceability of Subsection 6 must mean, *a fortiori*, that the “platform” specified in Subsection 6 is different from the “platform” referenced in Subsection 2 of the Data Law; otherwise, compliance with Subsection 6 is rendered impossible due to the Attorney General’s own inaction. Such a construction, however, would render the Data Law unconstitutionally vague because the same key but undefined term would have alternative meanings.

11. Acting on his view of the Data Law’s effectiveness, the Attorney General has issued a notice to Maine dealerships stating that as of January 5, 2025, vehicles sold in Maine would need to be equipped with the “platform” that Subsection 6 mandates (but that no “independent entity” has created). The notice also stated that the platform would need to communicate data securely through a direct data connection to the platform—even though Subsection 2 states that the “independent entity” (which does not exist) must establish and administer access to that data. Thus, the foundational premise of that notice does not yet exist. Nevertheless, the Attorney General has

mandated that dealers must deliver that notice to prospective owners of motor vehicles, ensure that those owners have read the notice, and obtain their signature.

12. Following the Attorney General's lead, proponents of the Data Law have begun advertising to Maine residents that they should contact the Attorney General with complaints about manufacturers' purported failure to provide access to repair data under the terms of the Data Law, even though manufacturers have no ability to do so. Notably, those proponents have advocated immediate lawsuits and enforcement actions against Auto Innovators' members even though manufacturers already provide independent repair facilities with the same secure access to vehicle, maintenance, and repair data that dealerships enjoy.

13. Vehicle manufacturers cannot even begin to attempt to comply with requirements that have not yet been established by an entity that does not yet exist. Thus, the threatened enforcement of the Data Law is unconstitutional and unlawful, and/or the Data Law itself is unconstitutionally vague.

14. **First**, because compliance with Subsection 6 is impossible, holding vehicle manufacturers liable for violations of Subsection 6 would violate their due process rights. Further, if vehicle manufacturers have any obligation to comply with Subsection 6 before the creation of the relevant "independent entity" and before that entity establishes and begins to administer access to vehicles through a "standardized access" "platform" that may have different meanings across the Data Law, Subsection 6 and other provisions are hopelessly vague and fail to provide Auto Innovators' members fair notice of what they are required to do to comply with the Data Law—which also violates their due process rights.

15. Likewise, if vehicle manufacturers are required to comply with Subsection 6 before these steps occur, the Data Law directly conflicts with the requirements, purposes, and objectives

of the National Traffic and Motor Vehicle Safety Act (the “Vehicle Safety Act”), 49 U.S.C. § 30101, *et seq.*, and its regulations. If the Data Law forces vehicle manufacturers to provide an “inter-operable” and “owner-authorized access platform” before the “standardized” means of “securely communicating” data to and from that data exist, the Vehicle Safety Act and its accompanying regulations preempt that law.

16. **Second**, because the “independent entity” that is supposed to manage authorization for access to OBD systems does not exist, it is impossible for vehicle manufacturers to comply with Subsection 1 without permitting *any* person to fully access vehicles’ OBD systems. Manufacturers cannot comply with Subsection 1 while ensuring that legitimate users (like vehicle repair personnel) may access OBD systems and illegitimate users (like hackers) cannot. Thus, the effect of immediate enforcement of Subsection 1 is to require manufacturers to remove vehicles’ cybersecurity protections, which they cannot do consistent with their obligations under the Vehicle Safety Act and its regulations, thereby preempting immediate enforcement.

17. **Third**, the Attorney General has failed to comply with his obligations under the Data Law to designate the “independent entity” that the Data Law requires, yet simultaneously seeks to hold vehicle manufacturers liable for the consequences of not complying with the Data Law because of his failure to designate such an entity. This constitutes a “failure or refusal of an agency to act” and “refusal or failure to adopt a rule where the adoption of a rule is required by law[]” for which Auto Innovators and its members are entitled to relief pursuant to Maine’s Administrative Procedures Act. 5 M.R.S. §§ 8058, 11001.

18. Accordingly, by this action, Auto Innovators seeks a declaration that compliance with the Data Law is impossible, that the Data Law is unconstitutionally vague, and that the Attorney General cannot currently enforce the Data Law. Auto Innovators further seeks an

injunction prohibiting the Attorney General from enforcing the Data Law until he has designated the relevant “independent entity,” that entity has established and begun to administer access to vehicles through the “standard access” platform that the Data Law contemplates, and Auto Innovators’ members have had the opportunity to implement that “standardized access” platform.

### **THE PARTIES**

19. Plaintiff Alliance for Automotive Innovation (Auto Innovators) is a nonprofit trade association with its corporate headquarters and principal place of business in Washington, D.C. Its members include BMW of North America, LLC; FCA US, LLC; Ford Motor Co.; General Motors Co.; Honda North America, Inc.; Hyundai Motor America; Jaguar-Land Rover North America, LLC; Kia Motors America, Inc.; Mazda North America; Mercedes-Benz USA, LLC; Mitsubishi Motors of North America, Inc.; Nissan North America, Inc.; Porsche Cars North America, Inc.; Subaru of America, Inc.; Toyota Motor North America, Inc.; Volkswagen Group of America; and Volvo Cars USA.

20. Auto Innovators is the leading advocacy group for the auto industry. It was formed in 2020 from the combination of the country’s two largest industry trade associations, the Alliance of Automobile Manufacturers and the Association of Global Automakers, to provide a single, unified voice for the auto industry. Auto Innovators’ members are the country’s leading auto manufacturers. Together, the group’s members produce nearly 99 percent of the cars and light trucks sold in the United States today. Vehicles manufactured by those members are sold throughout the country, including in Maine, both through dealership sales and aftermarket used sales.

21. Defendant is the Attorney General of the State of Maine. In that position, he is the State’s chief law enforcement officer, he is responsible for enforcing the Data Law, and he is

responsible for “designat[ing] an independent entity” as described in Subsection 2. The Attorney General is sued in his official capacity only.

### **JURISDICTION AND VENUE**

22. This Court has subject matter jurisdiction over Auto Innovators’ claims pursuant to 28 U.S.C. §§ 1331, 1367(a), and 2201(a). There is federal question jurisdiction under 28 U.S.C. § 1331 because Auto Innovators alleges violations of the federal Constitution and federal law, and the Court has supplemental jurisdiction over Auto Innovators’ third cause of action under 28 U.S.C. § 1367(a). Auto Innovators, on behalf of its members, seeks a declaration of its rights pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, over which there is an actual controversy after the enactment of the Data Law and the Attorney General’s actions following the enactment of the Data Law.

23. This Court has personal jurisdiction over Defendant because (a) he is located in the District in which this action was filed; and (b) many of the actions giving rise to these claims occurred in and/or were directed from this District.

24. Venue in this District is proper pursuant to 28 U.S.C. §§ 1391(b) and (c).

### **FACTUAL ALLEGATIONS**

#### **A. Background on Motor Vehicles**

25. Modern vehicles have changed a great deal since the advent of the automobile. Vehicles sold in the United States today are often as much marvels of technology as they are of mechanics. At tremendous expense, Auto Innovators’ members have developed electronic systems for the vehicles in their production lineup to provide the functionality of the vehicles they sell in the increasingly high-tech new automobile market demanded by consumers.

26. But high-tech automobiles necessarily present cybersecurity challenges. As the FBI has observed, as a result of increasing Internet-connectivity, the “automotive industry will face a

wide range of cyber threats and malicious activity in the near future,” with vehicles “a highly valued target for nation-state and financially motivated actors.” Josh Campbell, CNN, *FBI Says Hackers Are Targeting US Auto Industry* (Nov. 20, 2019), <https://www.cnn.com/2019/11/20/politics/fbi-us-auto-industry-hackers/index.html>. In recent years, there have been hundreds of incidents in which hackers have targeted vehicles and the auto industry. *See, e.g.*, Jim Motavalli, Auto Week, *As Cyberattacks Ramp Up, Electric Vehicles Are Vulnerable* (Feb. 19, 2024), <https://www.autoweek.com/news/a46857624/cyberattacks-on-electric-vehicles-and-chargers/>; Patrick George, The Atlantic, *Car Hackers Are Out for Blood* (Sep. 11, 2023), <https://www.theatlantic.com/technology/archive/2023/09/electric-car-hacking-digital-features-cyberattacks/675284/>.

27. To address this threat, Auto Innovators’ members have made substantial investments to design and put in place access controls that guard the security and performance of vehicle systems, including safety-critical functions like acceleration, braking, steering, and airbag deployment. In many cases, these controls limit access to the secure parts of those systems (and the data they protect) to those authorized by the manufacturers. For instance, to conduct certain diagnostics and repairs to vehicles, it is necessary for repair personnel to send software commands to vehicle systems and/or modify the software that governs vehicle systems. To avoid nefarious actors from inappropriately altering vehicle systems and software, vehicle manufacturers limit authorization to access those features—including through such technical features as secure gateways, electronic control unit (ECU) authentication, and message authentication.

28. The development and implementation of these access and security controls are necessary to keep hackers and other unauthorized parties out of vehicle systems and to ensure the safe operation of members’ vehicles in accordance with industry standards and federal law.



29. Most modern vehicles also have a telematics system that allows a vehicle to communicate remotely, enabling features such as GPS, emergency response, and remote start. Vehicle manufacturers generally separate vehicles' telematics function from other, safety-critical functions of vehicles by using secure gateways and other hardware and software features.

30. Telematics systems can also allow manufacturers to communicate recall information to consumers and deliver firmware-over-the-air updates, including to safety-related vehicle systems which allow for quicker and more comprehensive patching than traditional in-the-shop vehicle recalls. Indeed, the National Highway Traffic Safety Administration (NHTSA) strongly encourages the implementation and use of telematics systems for precisely these reasons.

#### **B. The Data Law**

31. For at least a decade, residents of Maine—like every other U.S. state—have had the ability to have their vehicles diagnosed, maintained, and repaired by repair personnel of their choice. All vehicle manufacturers who are current members of Auto Innovators agreed to a 2014 memorandum of understanding (MOU) that ensured that independent repair facilities would have a right equal to that of any dealerships to access vehicle data necessary for vehicle diagnosis, maintenance, or repair. The MOU established a dispute resolution system for access to diagnostic, repair, and maintenance data. In the decade since the MOU has been in place, no one has ever had to sue over data access or even see a dispute resolution through to completion.

32. Nevertheless, the proponents of Maine's Data Law sought and obtained its passage based upon the pretense that it would provide Maine residents with a "right to repair" their vehicles. Though framed as a "right to repair" statute, the Data Law has the effect of stripping vehicle manufacturers of their ability to secure access to the data within motor vehicles, except as established and administered by an "independent entity."

33. Specifically, Subsection 2 of the Data Law states that the Attorney General must “designate an independent entity . . . to establish and administer access to vehicle-generated data that is available through the on-board diagnostic system or that is transmitted by the **standardized access platform** authorized under this section,” *i.e.*, the Data Law. 29-A M.R.S. § 1810(2) (emphasis added). That independent entity “must consist of one representative each from a cross section of industry trade groups including but not limited to organizations representing motor vehicle manufacturers, aftermarket parts manufacturers, aftermarket parts distributors and retailers, independent motor vehicle service providers and new car dealers.” *Id.*

34. Subsection 2 further states that “[t]he independent entity shall manage cyber-secure access to motor vehicle-generated data, including ensuring on an ongoing basis that access to the on-board diagnostic system and **standardized access platform** is secure based on all applicable United States and international standards.” *Id.* (emphasis added).

35. Lastly, Subsection 2 mandates that the “independent entity” will “[i]dentify and adopt relevant standards for implementation of [the Data Law] and relevant provisions for accreditation and certification of organizations and for a system for monitoring policy compliance;” “[m]onitor and develop policies for the evolving use and availability of data generated by the operations of motor vehicles;” and “[c]reate policies for compliance with relevant laws, regulations, standards, technologies and best practices related to access to motor vehicle data.” *Id.*

36. Two of the Data Law’s other major provisions—Subsections 1 and 6—both rely upon the existence of the “independent entity” described in Subsection 2.

37. First, Subsection 1 states that “[a]ccess to the vehicle [OBD] systems of all motor vehicles . . . must be standardized and made accessible to owners and independent repair facilities

and the access may not require authorization by the manufacturer, directly or indirectly, unless that authorization is standardized across all makes and models of motor vehicles sold in this State and is *administered by the independent entity described in [S]ubsection 2.*” 29-A M.R.S. § 1810(1) (emphasis added).

38. Thus, the Data Law mandates that the Attorney General designate an independent entity that will establish and administer access to OBD systems.

39. Second, under Subsection 6, as of January 5, 2025, a manufacturer using telematics “is required to equip vehicles sold in this State with an inter-operable, *standardized* and owner-authorized *access platform* across all of the manufacturer’s makes and models.” 29-A M.R.S. § 1810(6) (emphasis added). “Th[at] *platform* must be capable of securely communicating all mechanical data<sup>1</sup> emanating directly from the motor vehicle via direct data connection to the *platform.*” *Id.* (emphasis added). Further, that “*platform* must be directly accessible by the motor vehicle owner through a mobile-based application and, upon the authorization of the owner, all mechanical data must be directly accessible by an independent repair facility or a licensed dealer . . .” *Id.* (emphasis added).

40. Subsection 6 is the only portion of the Data Law (*i.e.*, Section 1810 of chapter 15 of the Maine Revised Statutes) that authorizes a standardized access platform. Indeed, other than Subsection 2, Subsection 6 is the only portion of the Data Law that even references such a “platform.” Thus, the “platform” mandated and authorized in Subsection 6 is the same “platform authorized under this section [*i.e.*, section 1810]” referenced in Subsection 2. That is consistent with the original language of the ballot initiative that the Data Law’s proponents presented to the

---

<sup>1</sup> “Mechanical data” is defined as “any vehicle-specific data, including telematics system data, generated by, stored in or transmitted by a motor vehicle and used in the diagnosis, repair or maintenance of a motor vehicle.” 29-A M.R.S. § 1801(2-A).

Maine Secretary of State, which referred to a single “standardized access platform authorized by this law,” *i.e.*, the Data Law.<sup>2</sup>

41. Indeed, since the passage of the Data Law, the Maine government has passed legislation acknowledging that the “platform” authorized in Subsection 6 is the “platform” referenced in Subsection 2. In particular, in April 2024, the Maine legislature passed—and Maine’s Governor signed—as resolution “to Establish an Automotive Right to Repair Working Group.” 2024 Me. Legis. Serv. Resolves c. 171 (S.P. 1002) (L.D. 2289). That resolution created a working group for the development of the “entity” described in the Data Law—whose responsibilities would include, among other things, “adopt[ing] standards governing access to motor vehicle telematics systems and to otherwise implement and enforce the requirements of the [Data Law].” *Id.*; *see also id.* § 2 (“The working group shall develop recommendations . . . to establish an entity to ensure cyber-secure access to motor vehicle-generated data . . . for maintenance, diagnostic and repair purposes,” and those recommendations must include the development of “standards relating to access to vehicle telematics systems” and the adoption of “rules necessary for implementation and enforcement of [the Data Law] consistent with those rules.”).

42. Subsection 8 of the Data Law (“Subsection 8”) authorizes the Attorney General to “institute any actions or proceedings” to enforce the Data Law. 29-A M.R.S. § 1810(8). For instance, under 29-A M.R.S. § 1770, any “violation of this chapter” (*i.e.*, chapter 15 of Title 29-A of the Maine Revised Statutes, which includes the Data Law) is “a Class E crime, punishable by a fine of not less than \$25 nor more than \$500 or by imprisonment for not more than 30 days, or by

---

<sup>2</sup> The Secretary of State revised “this law” to “this Section,” *i.e.*, section 1810, pursuant to its obligations to revise ballot initiative language for conformance with drafting conventions and the statutory numbering system, without changing the substance of the draft initiative. 21-A M.R.S. § 901(3-A).

both.” Thus, the Attorney General could seek to fine or otherwise criminally penalize vehicle manufacturers who purportedly violate the Data Law.

43. Subsection 8 also authorizes “[a] motor vehicle owner or independent repair facility authorized by an owner who has been denied access to mechanical data in violation of this section” to “initiate a civil action seeking any remedies under law,” including “an award of treble damages or \$10,000, whichever amount is greater,” for “[e]ach denial of access.” 29-A M.R.S. § 1810(8).

**C. Attorney General’s Plan to Enforce the Data Law Despite the Non-Existence of an Independent Entity**

44. Though Subsections 1 and 6 hinge upon the designation of an “independent entity” that will administer access to data transmitted through each vehicle’s OBD system and “standardized access platform,” the Attorney General has not designated such an independent entity. Indeed, to Auto Innovators’ knowledge, no such independent entity even exists.

45. Because the Attorney General has not designated such an entity and no such entity even exists, that entity has not even begun to “establish and administer access” to data transmitted through each vehicle’s OBD system and “standardized access platform.” 29-A M.R.S. § 1810(2). No entity has begun to “manage cyber-secure access to motor vehicle-generated data, including ensuring on an ongoing basis that access to the [OBD] system and standardized access platform is secure based on all applicable United States and international standards.” *Id.* Nor has any entity “[i]dentif[ied] and adopted relevant standards for implementation of [the Data Law],” created “policies for compliance with relevant laws, regulations, standards, technologies and best practices,” or complied with any of its other obligations under the Data Law. *Id.*

46. Even if that entity existed and had undertaken those steps, vehicle manufacturers still could not comply with or implement the precise “access” (and accompanying policies and standards) established by that entity without being given significant time to do so. Vehicle

manufacturers generally “lock in” the design of a production model three to five years before it is actually released, so they have sufficient time to test and build vehicles consistent with that design. Thus, vehicle manufacturers need years of “lead time” to implement changes to their vehicles.

47. Though the Attorney General has not designated the relevant “independent entity”—which does not yet exist, much less undertaken its obligations under the Data Law—the Attorney General has taken the position that the Data Law is immediately enforceable against Auto Innovators’ members.

48. The Attorney General has informed Auto Innovators of his view that the requirements set forth in Subsection 6 (which was the provision of the Data Law scheduled to take effect) are now effective, and that he may pursue purported violations of the Data Law.

49. The Attorney General has taken the position that the “platform” specified in Subsection 6 of the Data Law might be different from the “platform” referenced in Subsection 2 of the Data Law—even though Subsection 2 refers to the “platform authorized under this section” and the “platform” described in Subsection 6 is the only “platform authorized under this section.”

50. Consistent with his view, on January 2, 2025, the Attorney General issued the notice to Maine automotive dealers that is attached hereto as **Exhibit A**. That notice stated that, as of January 5, 2025, vehicles sold in Maine would need to be equipped with the “platform” that Subsection 6 mandates. The Attorney General’s notice to dealers included an accompanying “Maine Vehicle Telematics System Notice,” which stated, among other things, that the “platform” would need to communicate data securely through a direct data connection to the platform, even though Subsection 2 states that the “independent entity” (which does not exist) must establish and administer access to that data. The Attorney General’s notice to dealers mandated that they deliver the Maine Vehicle Telematics System Notice to prospective owners of motor vehicles, ensure that

those owners have read that notice, and obtain their signature—even though that notice is based upon the false premise that vehicle manufacturers have any ability to provide the “access” that the Data Law requires.

51. Following the Attorney General’s lead, proponents of the Data Law have begun advertising to Maine residents that they should contact the Attorney General with complaints about manufacturers’ purported failure to provide access to vehicle data under the terms of the Data Law, even though manufacturers have no ability to do so.

**D. Provision of Access to OBD Systems Without Cybersecurity Protections Compromises Vehicle Safety**

52. The Data Law’s mandate that an “independent entity” ensure cyber-secure access to motor vehicles and that the relevant “platform” be “secure based on all applicable United States and international standards” is a recognition of the safety risks that would arise without adequately secured vehicle systems.

53. Currently, motor vehicle manufacturers perform that function. While manufacturers make some vehicle systems accessible without any authorization, they place controls and limitations on access to certain aspects of OBD-accessible systems.

54. Many modern vehicles’ functions are controlled by computers and software—not mechanical functions. Thus, repairing vehicles today frequently requires repair personnel to alter vehicle software. For instance, technicians may send diagnostic commands, referred to as “writing,” that cause the vehicle to execute a certain function, such as causing the car to accelerate. Technicians often must alter the software that makes vehicle components work. These include vehicle components that govern critical safety functions, such as acceleration, braking, steering, and airbag deployment.

55. In order to protect core safety functions and other vehicle components, manufacturers have developed and implemented various cybersecurity protections—such as by using challenge-and-response protocols, message authentication, encryption keys, unique identifiers for vehicle components, password protections, secure communication channels between OBD systems and offboard computer servers, secure gateways, intrusion detection and prevention systems, software authenticity and integrity checks, challenge-and-response protocols, rationality checks, secure storage controls, and firewalls.

56. Many of these cybersecurity protections are forms of “authorization” that manufacturers have imposed to protect OBD systems. For instance:

(a) *Challenge-and-response protocols.* “Challenge-and-response” protocols ensure that an appropriate person is accessing an OBD system. In a challenge-and-response protocol, when a diagnostic tool requests access to protected vehicle data or functions, a “challenge” is issued. The tool then has to give the correct “response” before the component will “unlock” the requested data or function. To give the correct response, the tool either must be programmed with a response from a manufacturer or communicate with the manufacturer’s “back office,” which sends the answer to the tool. This protocol, which is akin to a two-factor authentication procedure (*e.g.*, providing the answer to a “secret” question or the number sent to the user’s mobile phone), ensures that only authorized users and devices are accessing vehicle systems for diagnosis, maintenance, and repair.

(b) *Message authentication.* Message authentication prevents threat actors from transmitting malware or other unauthorized communications that may affect a vehicle’s core functions. Vehicle manufacturers program a vehicle’s electronic control unit (ECU) to receive only messages with a secure key evidencing that the message is authorized and not malicious.



(c) *Segmentation and the secure gateway.* Vehicle manufacturers may segment vehicle systems through physical isolation (using separate processors for different functions) and logical isolation (preventing direct communication between different features). This segmentation divides the “dirty” side of the vehicle (*e.g.*, telematics systems and other functions with external connectivity) and the “clean” side of the vehicle (*e.g.*, safety-critical systems), while limiting external actors’ access to the “clean” side.

(d) *Firmware encryption.* Vehicle manufacturers use asymmetric encryption techniques, termed a vehicle public key infrastructure (PKI), to secure the software that makes up an ECU. Asymmetric encryption involves both a public and private key when the firmware is installed on a vehicle. The public key allows third parties to verify that the software is authentic but still restricts access to the software, while the private key is maintained by the manufacturer on secure servers and is required to alter the firmware—thereby preventing third parties from modifying the firmware on ECUs in ways that could cause safety issues.

57. Auto Innovators’ members have good reasons for maintaining these sorts of controls over access to OBD systems. Without adequate cybersecurity controls, a hacker could, for instance, cause a vehicle to accelerate without application of the accelerator pedal, or prevent the brakes from working when the vehicle exceeds a certain speed. A sophisticated hacker could even install software with delayed activation, such as disabling the brake system one month after repair is performed—making it virtually impossible to identify the malevolent actor or hold him accountable for the harm. Whatever form they take, the consequences of such an event due to compromised or non-existent access controls could be disastrous. Threats to cybersecurity are an ever-present danger today—and require constant vigilance from manufacturers to stave off.

58. It remains to be seen what the designated “independent entity” will do to ensure that access to OBD systems is sufficiently secure. However, by disregarding the mandate that an independent entity be responsible for ensuring such cyber-secure access, while simultaneously failing to designate such an entity, the Attorney General has stymied vehicle manufacturers’ ability to maintain vehicle safety while complying with the Data Law.

**E. The Vehicle Safety Act and NHTSA**

59. The maintenance of cybersecurity controls on vehicle systems, including OBD systems, implicates the federal National Traffic and Motor Vehicle Safety Act, 49 U.S.C. § 30101, *et seq.*

60. Under the authority of the Vehicle Safety Act, the Secretary of Transportation, acting through NHTSA, acts to safeguard the public through education, research, safety standards, and enforcement.

61. NHTSA has the statutory authority to order recalls to address unreasonable risks to vehicle safety. Of the hundreds of vehicle recalls issued each year, vehicle manufacturers issue the overwhelming majority without any prompting from NHTSA. When a problem arises, NHTSA addresses safety-related concerns via direct discussions with vehicle manufacturers, often leading to manufacturers issuing a “voluntary” recall. Moreover, vehicle manufacturers have an affirmative obligation to certify compliance of their vehicles with safety standards and recall a vehicle if they become aware of a safety-related defect. Thus, the Vehicle Safety Act requires vehicle manufacturers to act regardless of whether NHTSA does so.

62. As part of its supervisory authority to promote vehicle safety, NHTSA has developed guidance to address safety problems proactively before recalls are necessary. In particular, NHTSA has advised vehicle manufacturers to implement the types of cybersecurity controls described above. As NHTSA has explained, “[v]ehicles are cyber-physical systems and

cybersecurity vulnerabilities could impact safety”—citing examples such as manipulation of vehicle sensors, braking, steering, propulsion, and power. Nat’l Highway Traffic Safety Admin., *Cybersecurity Best Practices for the Safety of Modern Vehicles*, at 1, 5, 15 (2022), available at <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf>. Thus, NHTSA has advised vehicles manufacturer that they should:

- Limit access to vehicle ECUs’ software;
- Employ “cryptographic techniques” and credentialing of users, including through passwords, PKI certificates, and encryption keys;
- Control diagnostic tools’ “access to vehicle systems that can perform diagnostic operations”;
- Treat “all networks and systems external to a vehicle’s wireless interfaces as untrusted”;
- Employ “[n]etwork segmentation and isolation techniques” and “[g]ateways with strong boundary controls”;
- Employ “encryption and authentication methods in any operational communication between external servers and the vehicle”; and
- Otherwise “limit[] an attacker’s ability to modify firmware.”

*Id.* at 12-17.

## **FIRST CLAIM FOR RELIEF**

### **Declaratory Judgment**

#### **(Unenforceability of Subsection 6 Due to Violation of Due Process and Federal Preemption)**

63. Paragraphs 1–62 above are incorporated herein by reference.

64. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court’s inherent equitable authority, and seeks a declaration that Subsection 6 of the Data Law currently is unenforceable because it violates Auto Innovators’ members’ right to due process and, alternatively, it is preempted by the Vehicle Safety Act.

65. As explained, Subsection 6 requires vehicle manufacturers using telematics—including all of Auto Innovators’ members—to use a “platform” created by the independent entity called for by Section 2 that allows for **“inter-operable, standardized and owner-authorized access [to mechanical data] . . . across all of the manufacturer's makes and models.”** 29-A M.R.S. § 1810(6) (emphasis added). In turn, Subsection 2 describes how the “standardized . . . access platform” referenced in Subsection 6 will be created and administered by an “independent entity” designated by the Attorney General, as well as that independent entity’s other responsibilities. *Id.* § 1810(2).

66. Thus, compliance with Subsection 6 requires using a “standardized access platform” in vehicles, and access through that platform must be “establish[ed] and administer[ed]” through the independent entity designated by the Attorney General. *Id.* §§ 1810(2), (6). In addition, Subsection 6 requires that access through the platform must be “secure,” and it is the responsibility of the independent entity to ensure the security of the standardized access platform. *Id.* § 1810(6).

67. Providing such access currently is not possible because (a) the Attorney General has not designated an independent entity; (b) that independent entity has not established, much less started administering, the relevant access; and (c) vehicle manufacturers have not had time to adapt their vehicles to provide such access in accordance with the independent entity’s instructions.

68. Because it is impossible for Auto Innovators' members to comply with Subsection 6, it would deprive them of due process to hold them liable. *See, e.g., Doe v. Snyder*, 101 F. Supp. 3d 722, 724 (E.D. Mich. 2015) ("Holding an individual criminally liable for failing to comply with a duty imposed by statute, with which it is legally impossible to comply, deprives that person of his due process rights.").

69. Similarly, because the Attorney General has not designated the "independent entity" which in turn has not established or administered the relevant "access," Subsection 6 is hopelessly vague and violates Auto Innovators' members' due process rights for that additional reason. *See, e.g., Frese v. Formella*, 53 F.4th 1, 6 (1st Cir. 2022) ("A statute is impermissibly vague if it 'fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.'") (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)).

70. Alternatively, to the extent the Attorney General interprets Subsection 6 to permit compliance by providing an "access platform" *without* the "cyber-secure" access that the independent entity is supposed to establish and administer, the Vehicle Safety Act and its implementing regulations preempt that interpretation.

71. The Supremacy Clause of the United States Constitution, U.S. Const. art. VI, provides that "the laws of the United States . . . shall be the supreme law of the land." State laws that conflict with federal law are preempted by operation of the Supremacy Clause. Preemption may arise in a variety of contexts, including when the state law conflicts with, or poses an obstacle to, the purposes sought to be achieved by the federal law.

72. A failure to maintain adequate cybersecurity controls would give rise to a safety-related defect, and the Vehicle Safety Act requires manufacturers to issue recalls and remediate

safety-related defects. Therefore, providing non-secure access would conflict with the purposes and objectives of the Vehicle Safety Act.

73. The Data Law is similar to, and largely based upon, a ballot initiative passed in Massachusetts in 2020, which is codified at Chapter 93K of the Massachusetts General Laws (the “Massachusetts Data Access Law”). NHTSA has recognized that if the Massachusetts Data Access Law’s access requirements would create safety issues, then the Vehicle Safety Act would require motor vehicle manufacturers to recall and stop selling new vehicles compliant with that requirement. Thus, in June 2023, NHTSA specifically instructed Auto Innovators’ members that “the [Massachusetts] Data Access Law conflicts with and therefore is preempted by the [Vehicle] Safety Act.”

74. Nevertheless, as explained, the Attorney General has taken the position that the Data Law is immediately enforceable and effective and that Auto Innovators’ members can be held liable under the Data Law. Therefore, an actual controversy exists between the parties regarding the enforceability and effectiveness of Subsection 6 of the Data Law.

75. Accordingly, Auto Innovators is entitled to a declaration that Subsection 6 currently is unenforceable because it violates Auto Innovators’ members’ right to due process or, alternatively, is preempted by federal law.<sup>3</sup>

---

<sup>3</sup> Auto Innovators reserves its right to advance further claims and/or arguments, including regarding preemption of the Data Law, based upon any particular interpretation of the Data Law that the Attorney General asserts, and/or the standards and regulations that the “independent entity” adopts following its creation and designation by the Attorney General.

## SECOND CLAIM FOR RELIEF

### Declaratory Judgment

#### (Unenforceability of Subsection 1 Due to Violation of Due Process and Federal Preemption)

76. Paragraphs 1–75 above are incorporated herein by reference.

77. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, and this Court’s inherent equitable authority, and seeks a declaration that Subsection 1 of the Data Law currently is unenforceable because it either violates Auto Innovators’ members’ right to due process or is preempted by the Vehicle Safety Act.

78. As explained, Subsection 1 states that “[a]ccess to the vehicle on-board diagnostic systems of all motor vehicles . . . may not require authorization by the manufacturer, directly or indirectly, unless that authorization is standardized across all makes and models of motor vehicles sold in this State and is administered by the independent entity described in [S]ubsection 2.” 29-A M.R.S. § 1810(1). In turn, Subsection 2 states that the relevant independent entity will “establish and administer access to vehicle-generated data that is available through the on-board diagnostic system . . . .” *Id.* § 1810(2).

79. Thus, manufacturers may not “require authorization” to access OBD systems unless that authorization is administered by the “independent entity” that does not yet exist. Holding manufacturers liable for imposing authorization that is not administered by that independent entity—when such entity does not exist and has not established and begun administering the relevant standards—would violate their due process rights. *E.g., Snyder*, 101 F. Supp. 3d at 724; *Frese*, 53 F.4th at 6.

80. The only alternative, theoretical means of compliance under Subsection 1 is to provide access without any authorization by the manufacturer. But existing cybersecurity protections (which are not administered by the independent, third-party entity) necessarily require

manufacturers to impose limits on access to OBD systems, which encompasses the vehicle's internal system that monitors and reports vehicle performance issues. Thus, removal of that authorization would require removal of cybersecurity protections that would give rise to a safety-related defect.

81. Nevertheless, as explained, the Attorney General has taken the position that the Data Law is immediately enforceable and effective and that Auto Innovators' members can be held liable under the Data Law. Therefore, an actual controversy exists between the parties regarding the enforceability and effectiveness of Subsection 1 of the Data Law.

82. Accordingly, Auto Innovators is entitled to a declaration that Subsection 1 currently is unenforceable because it violates Auto Innovators' members' right to due process and/or is preempted by federal law.

### **THIRD CLAIM FOR RELIEF**

#### **Declaratory Judgment**

#### **(Relief under Maine Administrative Procedures Act for Attorney General's Failure to Designate Independent Entity)**

83. Paragraphs 1–82 above are incorporated herein by reference.

84. This claim is brought under the Maine Administrative Procedure Act ("Maine APA"), 5 M.R.S. § 8001 *et seq.*; 28 U.S.C. § 1367(a); and this Court's inherent equitable authority, and seeks a declaration that Subsections 1 and 6 of the Data Law currently are unenforceable because the Attorney General has failed to designate the "independent entity" that the Data Law mandates.

85. The Maine APA permits "[a]ny person aggrieved by the failure or refusal of an agency to act" to seek "judicial review" of that failure or refusal. 5 M.R.S. § 11001. Likewise, "any person who is aggrieved" by "an agency's refusal or failure to adopt a rule where the adoption



of a rule is required by law[]” is entitled to “[j]udicial review” of that refusal or failure, and the court may “issue such orders as are necessary and appropriate to remedy such failure.” *Id.* § 8058.

86. The Attorney General is an “agency” as defined in the Maine APA. *See id.* § 8002(2) (“[a]gency’ means any body of State Government authorized by law to adopt rules, to issue licenses or to take final action in adjudicatory proceedings, including, but not limited to, every . . . officer of the State Government so authorized,” subject to certain exceptions not applicable here).

87. The Attorney General’s designation of an “independent entity” under Subsection 2 is the adoption of a “rule” as defined in the Maine APA. *See id.* § 8002(9) (“Rule” encompasses any “regulation, standard, code, statement of policy, or other agency guideline or statement of general applicability” that “is intended to be judicially enforceable and implements, interprets or makes specific the law administered by the agency.”). Alternatively, it is a final agency action. *Id.* § 8002(4).

88. The Attorney General has not designated an “independent entity” under the Data Law, which is a “failure or refusal . . . to act” and a “refusal or failure to adopt a rule” that was required by law. *Id.* §§ 8058, 11001. Nevertheless, as explained, the Attorney General has taken the position that the Data Law is immediately enforceable and effective and that Auto Innovators’ members can be held liable under the Data Law. An actual controversy exists between the parties regarding the enforceability and effectiveness of the Data Law in the absence of the Attorney General’s designation of the “independent entity.”

89. Auto Innovators and each of its members are “person[s] . . . aggrieved” by that conduct. 5 M.R.S. §§ 8058, 11001. The Data Law specifically contemplated that vehicle manufacturers would be able to comply with the Data Law—purportedly while maintaining cyber-

secure vehicle systems—by relying upon an independent entity, designated by the Attorney General, that would include industry representatives (including organizations representing motor vehicle manufacturers) that would establish and administer access to vehicle data. As a result of the Attorney General’s failure to designate an entity and the resulting failure of any entity even to begin to establish or administer data access, Auto Innovators’ members face crippling financial liability from civil actions and potential criminal liability.

90. Accordingly, Auto Innovators is entitled to a declaration that Subsections 1 and 6 of the Data Law currently are unenforceable because the Attorney General has failed to designate the “independent entity” that the Data Law mandates.

#### **FOURTH CLAIM FOR RELIEF**

##### **Injunctive Relief**

91. Paragraphs 1–90 above are incorporated herein by reference.

92. This claim is brought under 28 U.S.C. § 2201, 42 U.S.C. § 1983, the Maine APA, and this Court’s inherent equitable authority, and seeks an injunction prohibiting enforcement of Subsections 1 and 6 until the Attorney General has designated the relevant independent entity, that independent entity has undertaken its obligations under Subsection 2, and vehicle manufacturers have had an opportunity to comply with the access requirements that the independent entity has established and administered.

93. Absent an injunction, Auto Innovators’ members would face civil and criminal liability from premature enforcement of the Data Law. Further, any attempts at compliance before the relevant “independent entity” has created and begun to administer cyber-secure access to vehicle mechanical data could undermine the integrity of motor vehicle systems and the safe operation of consumer vehicles. Premature enforcement or attempts at compliance could harm manufacturers’ business reputations, result in exposure to claims by customers, and/or result in the

considerable costs of conducting recalls mandated by NHTSA, which includes the mandatory “stop sale” of all vehicles containing the safety-related defects leading to the recalls.

94. Defendant and third parties would not be harmed by an injunction, which would preserve the status quo, in which Maine consumers enjoy complete mechanical data access (to the extent any such data is necessary for vehicle diagnosis, repair, and maintenance) to have their vehicles repaired at any facility they choose or to enable the repair themselves. Further, an injunction would serve the interest of the public, which has a strong interest in halting the enforcement of unconstitutional laws and state laws that directly conflict with federal law, as well as the protection of consumer safety.

#### **PRAYER FOR RELIEF**

Plaintiff respectfully requests that the Court enter judgment:

- A. Declaring that Subsections 1 and 6 currently are unenforceable because they violate Auto Innovators’ members’ right to due process and/or are preempted by federal law;
- B. Declaring the Data Law unconstitutionally vague;
- C. Temporarily and permanently enjoining enforcement of Subsections 1 and 6 until the Attorney General has designated the relevant independent entity, that independent entity has undertaken its obligations under Subsection 2, and vehicle manufacturers have had an opportunity to comply with the access requirements that the independent entity has established and administered;
- D. Awarding Plaintiff its costs and litigation expenses, including attorneys’ fees and costs, pursuant to 42 U.S.C. § 1988; and
- E. Awarding Plaintiff such other and further relief as the Court deems just, proper, and equitable.

Dated: January 31, 2025

Respectfully submitted,

ALLIANCE FOR AUTOMOTIVE INNOVATION

By its attorneys,

/s/ Joshua D. Dunlap

Joshua D. Dunlap  
Shannon Linnehan  
PIERCE ATWOOD LLP  
254 Commercial Street  
Merrill's Wharf  
Portland, ME 04101  
Tel: (207) 791-1100  
jdunlap@pierceatwood.com  
slinnehan@pierceatwood.com

John Nadolenco (*pro hac vice* pending)  
Erika Z. Jones (*pro hac vice* pending)  
Daniel D. Queen (*pro hac vice* pending)  
Eric A. White (*pro hac vice* pending)  
MAYER BROWN LLP  
1999 K Street, NW  
Washington, DC 20006  
Tel: (202) 263-3000  
jnadolenco@mayerbrown.com  
ejones@mayerbrown.com  
dqueen@mayerbrown.com  
eawhite@mayerbrown.com

Charles H. Haake (*pro hac vice* pending)  
Jessica L. Simmons (*pro hac vice* pending)  
ALLIANCE FOR AUTOMOTIVE INNOVATION  
1050 K Street, NW  
Suite 650  
Washington, DC 20001  
Tel: (202) 326-5500  
chaake@autosinnovate.org  
jsimmons@autosinnovate.org

**Exhibit A**

AARON M. FREY  
ATTORNEY GENERAL



TEL: (207) 626-8800  
TTY USERS CALL MAINE RELAY 711

STATE OF MAINE  
OFFICE OF THE ATTORNEY GENERAL  
6 STATE HOUSE STATION  
AUGUSTA, MAINE 04333-0006

REGIONAL OFFICES  
84 HARLOW ST. 2ND FLOOR  
BANGOR, MAINE 04401  
TEL: (207) 941-3070  
FAX: (207) 941-3075

125 PRESUMPSHOT ST., STE. 26  
PORTLAND, MAINE 04103  
TEL: (207) 822-0260  
FAX: (207) 822-0259

14 ACCESS HIGHWAY, STE. 1  
CARIBOU, MAINE 04736  
TEL: (207) 496-3792  
FAX: (207) 496-3291

## NOTICE TO MAINE DEALERS

Under Maine law, 29-A M.R.S.A. § 1810, vehicle owners have the right to access their vehicle's mechanical data through a mobile device and to authorize an independent repair facility to access the vehicle's mechanical data to diagnose, repair, and maintain the vehicle. As of January 5, 2025, manufacturers of motor vehicles sold in Maine, including commercial motor vehicles and heavy-duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, that use a telematics system, are required to equip vehicles sold in Maine with an inter-operable, standardized and owner-authorized access platform across all of the manufacturer's makes and models.

As required by Maine law (29-A M.R.S.A. § 1811), the Attorney General has established for prospective motor vehicle owners the accompanying Maine Motor Vehicle Telematics System Notice. Please note that the notice form provides for the prospective motor vehicle owner's signature certifying that the prospective owner has read the telematics system notice.

**DEALER OBLIGATIONS:** When selling or leasing motor vehicles containing a telematics system, a dealer as defined in Title 29-A, section 851, subsection 2 and a new vehicle dealer as defined in section 851, subsection 9 shall provide the telematics system notice under subsection 1 to the prospective owner, obtain the prospective owner's signed certification that the prospective owner has read the notice and provide a copy of the signed notice to the prospective owner.

### Maine Vehicle Telematics System Notice

This vehicle includes a “telematics system” as defined under Maine Revised Statutes, Title 29-A, section 1801(6). Under Maine law, you have the right to access the vehicle's mechanical data through a mobile device and to authorize an independent repair facility to access the vehicle's mechanical data to diagnose, repair, and maintain your vehicle.

A vehicle’s telematics system collects information generated by the operation of the vehicle and transmits that information using wireless communications to a remote receiving point where the information is stored or used.

As of January 5, 2025, manufacturers of motor vehicles sold in Maine, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, that use a telematics system, are required to equip vehicles sold in Maine with an inter-operable, standardized and owner-authorized access platform across all of the manufacturer's makes and models. The platform must be capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform. The platform must be directly accessible by the motor vehicle owner through a mobile-based application and, upon the authorization of the owner, all mechanical data must be directly accessible by an independent repair facility or a licensed dealer limited to the time to complete the repair or for a period of time agreed to by the motor vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle.

“Mechanical data” refers to vehicle-specific data, including telematics system data, generated by, stored in, or transmitted by a motor vehicle and used in the diagnosis, repair, or maintenance of the vehicle. The type of mechanical data available through telematics will vary depending on the vehicle, but can come from sensors on many vehicle parts, such as the airbags, battery, engine and/or motor, transmission, brakes, or tires.

### Certification of Notice

#### Prospective Owner 1

I hereby certify that I have been provided with and read the Maine Vehicle Telematics System Notice on this \_\_\_\_ day of \_\_\_\_\_, \_\_\_\_\_.

\_\_\_\_\_  
Name (Printed)

\_\_\_\_\_  
Signature

#### Prospective Owner 2

I hereby certify that I have been provided with and read the Maine Vehicle Telematics System Notice on this \_\_\_\_ day of \_\_\_\_\_, \_\_\_\_\_.

\_\_\_\_\_  
Name (Printed)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Make

\_\_\_\_\_  
Model and Model Year

\_\_\_\_\_  
Seller Name

\_\_\_\_\_  
VIN

\_\_\_\_\_  
Seller Address



# Automotive Right to Repair Working Group

Report Pursuant to Resolves 2023, ch. 171 –  
Submitted by the Office of the Attorney General of Maine

2/24/2025



**Automotive Right to Repair Working Group  
Report Pursuant to Resolves 2023, ch. 171  
February 24, 2025**

## Maine's Automotive Right to Repair Law

In November 2023, Maine voters approved Initiated Bill 3 (LD 1677), An Act Regarding Automotive Right to Repair. The law requires motor vehicle manufacturers to make access to on-board diagnostic and repair information the same for owners and independent repair facilities as it is for new vehicle dealers and/or manufacturer-authorized repair facilities. 29-A M.R.S. § 1810. For 2002 models through the present, the law requires access through methods that require physical access to the vehicle. 29-A M.R.S. § 1810(3)-(5). Starting on January 5, 2025, however, vehicles sold in the state that use telematics systems must be equipped "with an interoperable, standardized and owner-authorized access platform across all of the manufacturer's makes and models." 29-A M.R.S. § 1810(6). A "telematics system" is a "system in a motor vehicle that collects information generated by the operation of the vehicle and transmits that information using wireless communications to a remote receiving point where the information is stored or used." 29-A M.R.S. § 1801(6). This means that diagnostic and repair information generated by the vehicle, with owner-authorization, could be accessed remotely and without the physical presence of the vehicle.

The vehicle access platform "must be capable of securely communicating all mechanical data<sup>1</sup> emanating directly from the motor vehicle via direct data connection to the platform" and "must be directly accessible by the motor vehicle owner through a mobile-based application." 29-A M.R.S. § 1810(6). Additionally, "upon the authorization of the owner," the data "must be directly accessible by an independent repair facility or a licensed dealer . . . limited to the time to complete the repair or for a period of time agreed to by the motor vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle." *Id.*

The law also requires the Attorney General to "designate an independent entity not controlled by one or more motor vehicle manufacturers to establish and administer access to vehicle-generated data that is available through the on-board diagnostic system or that is transmitted by the standardized access platform authorized under this section." 29-A M.R.S. § 1810(2). This "independent entity" shall:

- A. Identify and adopt relevant standards for implementation of this section and relevant provisions for accreditation and certification of organizations and for a system for monitoring policy compliance;
- B. Monitor and develop policies for the evolving use and availability of data generated by the operations of motor vehicles; and
- C. Create policies for compliance with relevant laws, regulations, standards, technologies and best practices related to access to motor vehicle data.

---

<sup>1</sup> "Mechanical data" is "any vehicle-specific data, including telematics system data, generated by, stored in or transmitted by a motor vehicle and used in the diagnosis, repair or maintenance of a motor vehicle." 29-A M.R.S. § 1801(2-A).

## Automotive Right to Repair Working Group

Subsequently, during its Second Regular Session, the 131st Legislature enacted LD 2289, Resolve, to Establish an Automotive Right to Repair Working Group. This Resolve directed the Attorney General to “convene a working group to develop recommendations for legislation to establish an entity with rule-making and enforcement authority to adopt standards governing access to motor vehicle telematics systems and to otherwise implement and enforce the requirements” of Section 1810. The working group was charged with “develop[ing] recommendations for legislation to establish an entity to ensure cyber-secure access to motor vehicle-generated data to owners and owner-authorized independent repair facilities for maintenance, diagnostic and repair purposes.” The recommendations must address the entity’s ability to:

- A. Identify and adopt relevant standards for implementing the requirements of Title 29-A, Section 1810, including standards relating to access to vehicle telematics systems;
- B. Monitor motor vehicle manufacturer compliance with standards adopted by the entity;
- C. Develop and monitor policies for the evolving use and availability of data generated by the operations of motor vehicles;
- D. Create policies for compliance with relevant laws, regulations, standards, technologies and best practices related to motor vehicle data, with consideration given to privacy and cybersecurity concerns; and
- E. Adopt rules necessary for implementation and enforcement of Title 29-A, Section 1810 and to enforce the requirements of that law consistent with those rules.

The Resolve directed the Attorney General to submit a report by February 28, 2025 “to the joint standing committee of the Legislature having jurisdiction over innovation, development, economic advancement and business matters a report containing the findings and recommendations of the working group.” The committee may then report out legislation relating to the report to the 132<sup>nd</sup> Legislature in 2025.<sup>2</sup>

---

<sup>2</sup> Given the benefits resulting from the working group’s consideration of the powers, duties, and authority of the independent entity, the Attorney General decide to await conclusion of the working group’s work before designating an independent entity pursuant to Initiated Bill 3. See letter attached hereto as Exhibit A.

## Formation of the Working Group

The Resolve directed the Attorney General or the Attorney General's designee to participate in the working group and to invite the following additional members:

- A. The Secretary of State or the Secretary of State's designee;
- B. Two members representing motor vehicle manufacturers, at least one of whom must represent an organization of motor vehicle manufacturers;
- C. One member representing aftermarket parts manufacturers;
- D. One member representing aftermarket parts distributors and retailers;
- E. Two members representing independent repair facilities, at least one of whom is an owner or operator of a facility;
- F. One member representing new motor vehicle dealers;
- G. One member representing a consumer advocacy organization; and
- H. One member representing a data privacy advocacy organization.

The Attorney General designated Chief Deputy Attorney General Christopher Taub and Assistant Attorney General and Chief of the Consumer Protection Division Christina Moylan as his designees to participate in the working group. During the summer of 2024, DAG Taub and AAG Moylan reached out to the designated stakeholders to identify persons interested in serving on the working group. Ultimately, the following persons agreed to serve on the working group:

- A. Lynne Gardner, Esq., Director of Legal Affairs, Adjudications & Hearings for the Bureau of Motor Vehicles (serving as the Secretary of State's designee)
- B. Elizabeth Frazier, Esq. of Pierce Atwood LLP (representing the Alliance for Automotive Innovation, an organization of motor vehicle manufacturers)
- C. Brian Boggs, Director of Service Engineering at Tesla, Inc. (representing motor vehicle manufacturers)
- D. Eric Luftig, Senior Vice President of Product, Engineering, Manufacturing & Quality of Dorman Products (representing aftermarket parts manufacturers)
- E. Jeffrey Groves, General Counsel for O'Reilly Automotive, Inc., retired (representing aftermarket retailers and distributors)
- 6. Tommy Hickey of Brian S. Hickey & Associates and Executive Director of the Maine Automotive Right to Repair Coalition (representing independent repair facilities)
- 7. Tim Winkeler, President and CEO of VIP Tires & Service (representing independent repair facilities)
- 8. Jack Quirk, President of Quirk Auto Group (representing new motor vehicle dealers)

9. Meagan Sway, Policy Director for the ACLU of Maine (representing a consumer advocacy organization)<sup>3</sup>
10. Caitriona Fitzgerald, Deputy Director of the Electronic Privacy Information Center (representing a data privacy advocacy organization)

## Working Group Meetings

The working group met ten times: August 29, 2024, September 11, 2024, September 26, 2024, October 16, 2024, October 30, 2024, November 18, 2024, December 2, 2024, December 20, 2024, January 17, 2025, and February 12, 2025.

At the working group's first meeting on August 29, there was a general discussion of the working group's goals and expectations for future meetings. The working group also adopted a remote meeting policy, pursuant to which in-person participation by members was expected unless a member determined that their physical presence would not be practical. At its meetings on September 11 and September 26, the working group heard technical and other presentations from stakeholders and others with relevant expertise who members had previously invited to the meetings. At its October 16 meeting, the working group held a public hearing and heard from members of the public who wished to present information, recommendations, or other matters to the group.

At its meetings on October 30 and November 18, members of the working group engaged in discussions regarding recommendations to be made for legislation establishing an entity to implement and enforce the requirements of the automotive right to repair law (29-A M.R.S. § 1810). The discussions covered a number of topics, including: 1) the nature of the entity (*e.g.*, an independent board or commission, a quasi-governmental entity, or a state regulatory agency); 2) whether the entity would maintain, provide access to, or otherwise exercise control over vehicle data; 3) whether the entity would determine who, and on what terms, individuals would have access to vehicle data (*e.g.*, a credentialing or verification process for independent repair facilities); 4) whether the entity would establish a standardized process by which all motor vehicle manufacturers would provide access to vehicle data; 5) whether the entity would need rulemaking authority; 6) whether the entity would need enforcement authority; 7) whether the entity would need staff; and 8) whether the entity would need funding and if so, the manner by which it should be funded.

After the November 18 meeting, and based on the discussions at that meeting and the one on October 30, the working group members representing the Office of the Attorney General prepared a draft of the working group's report to the legislative committee, along with a draft of

---

<sup>3</sup> Michael Kebede, the ACLU of Maine's current Policy Director, later served on the working group in place of Ms. Sway.

proposed revisions to 29-A M.R.S. § 1810. These documents were circulated to working group members and posted on the working group's website.<sup>4</sup>

At its meeting on December 2, 2024, members of the working group reviewed and discussed the previously circulated draft report and draft revisions to 29-A M.R.S. § 1810. Some members proposed additional revisions to both documents before and after the meeting.

On December 6, 2024, working group members representing the Office of the Attorney General circulated to members and posted on the working group's website revised drafts of both the report and proposed revisions to 29-A M.R.S. § 1810, reflecting revisions proposed by working group members.

On December 20, 2024, the working group discussed the draft report and the proposed revisions to 29-A M.R.S. § 1810. Some members of the working group suggested further additions to the report, and it was decided that such suggestions should be submitted in writing to the members representing the Office of the Attorney General in advance of the working group's next meeting. Also at the December 20, 2024 meeting, the working group held a hearing for members of the public to comment on the two documents. The working group allowed members of the public to submit written comments through December 30, 2024, and this deadline was subsequently extended to January 3, 2025. Copies of all comments submitted to the working group are available on the working group's website.

On January 14, 2025, the members representing the Office of the Attorney General circulated a revised version of the report reflecting discussions at the December 20 meeting, public comments, and written submissions from working group members.

On January 17, 2025, the working group met to discuss the revised version of the report. Some additional revisions were discussed and agreed upon.

On February 7, 2025, the members representing the Office of the Attorney General circulated a revised version of the report reflecting the revisions agreed upon at the January 17 meeting.

On February 12, 2025, the working group met to review and discuss the revised version of the report. All members present voted to approve the revised version and authorized the members representing the Office of the Attorney General to submit the report to the Joint Standing Committee on Housing and Economic Development.

## Working Group's Conclusions and Recommendations

The working group focused on the role of the entity with respect to access to vehicle data accessed remotely via telematics systems. Both members of the group and members of the public expressed concerns regarding privacy and cyber-security in allowing third parties to access this data. This led to extensive discussions among group members regarding the extent to which

---

<sup>4</sup> See <https://www.maine.gov/ag/automotive-right-to-repair/index.html>.

the entity should maintain, provide access to, or otherwise exercise control over vehicle data. Ultimately, there was a unanimous consensus that the entity should not maintain, provide access to, or otherwise exercise control over vehicle data. Rather, all vehicle data should be directly accessible by owners and (upon authorization by owners) independent repair facilities to the extent required by 29-A M.R.S. § 1810. As is the case now, manufacturers would remain responsible for addressing potential privacy and cyber-security issues in making data available pursuant to 29-A M.R.S. § 1810.

*after market parts*

Section 1810 can be interpreted as requiring the entity to administer access to vehicle data. For example, the statute states that the independent entity shall "establish and administer access to vehicle-generated data" and "manage cyber-secure access to motor vehicle-generated data." The working group recommends that the statute be amended to make clear that the entity will not maintain, provide access to, or otherwise exercise control over vehicle data. Proposed amended statutory language addressing this recommendation and several other recommendations is attached to this report as Exhibit B.

There was also unanimous consensus that at least initially, the entity should serve a purely advisory role and have no rulemaking or enforcement authority. In this advisory role, the entity would have four major responsibilities: 1) monitoring and assessing implementation of the right to repair law, including manufacturers' compliance with the law's requirements; 2) attempting to informally resolve any complaints from owners and independent repair facilities alleging a manufacturer's non-compliance with the law, and, if a complaint cannot be resolved, considering whether to refer the matter to the Attorney General for enforcement action; 3) designating one or more technical experts with whom the Attorney General may consult in assessing enforcement referrals and maintaining enforcement actions, and 4) making an annual report to the legislative committee of jurisdiction, the Governor, and the Attorney General describing the entity's activities during the preceding year, identifying any implementation or compliance issues that it encountered, and recommending any amendments to the statute, including amendments providing the entity with additional authority, or additional legislation, to address any implementation or compliance issues. Given the recommendation that the entity have no rulemaking or enforcement authority, at least initially, the working group did not develop recommendations for establishing compliance standards. The working group expects that the entity will itself assess its need for authority to develop specific standards for compliance as part of its report addressing compliance issues.

There was consensus that the entity should not be a state agency but instead should be an independent commission. The Governor should appoint commission members as follows:

- A. Three members representing motor vehicle manufacturers, at least one of whom represents an organization of motor vehicle manufacturers, and at least one of whom represents a heavy duty vehicle manufacturer;
- B. One member representing aftermarket parts manufacturers;



- C. One member representing diagnostic tool manufacturers;
- D. One member representing aftermarket parts distributors and retailers;
- E. Three members representing Maine independent repair facilities, at least one of whom is an owner or operator of an independent repair facility specializing in automobiles, and at least one of whom is an owner or operator of an independent repair facility specializing in heavy duty vehicles;
- F. One member representing Maine new motor vehicle dealers;
- G. One member with expertise in automotive cyber-security matters; and
- H. One member representing the public who is a resident of Maine.

The working group recommends including at least one member representing a heavy duty vehicle manufacturer and at least one member who is an owner or operator of an independent repair facility specializing in heavy duty vehicles. This is because the working group received information indicating that heavy duty vehicles differ from automobiles with respect to how they are manufactured and assembled, used, owned, and repaired.

The member representing the public should serve as the commission's chair. Each member should serve a term of three years, with some initial appointees having shorter terms in order to stagger the terms. Members should not receive compensation but should be reimbursed for expenses for attendance at meetings. The commission should meet at least quarterly but should be allowed to meet more frequently at the chair's discretion.

One basis for the working group's recommendation that the commission be advisory is the working group's consensus that, at least initially, motor vehicle manufacturers should decide for themselves the manner in which they will provide access to all mechanical data emanating directly from the vehicle in compliance with the statute.

The working group recognized that depending on how manufacturers implement the telematics requirements of the law, it may become necessary to provide at least some level of standardization across all manufacturers. If the commission determines that access to vehicle data should be standardized, it could recommend in its annual report that it be given the necessary authority to adopt and implement appropriate standardization requirements. The commission can also consider issuing, solely as non-binding recommendations, "best practices" for manufacturers to use in providing access to vehicle data.

Once consensus was reached that the commission would not maintain, provide access to, or otherwise exercise control over vehicle data, and that it would initially serve a purely advisory role, the working group readily reached consensus on several other issues. The working group determined that the commission would not act as a "gatekeeper" between owners/independent repair facilities and vehicle manufacturers. There was discussion of whether manufacturers should be required to use "third-party authenticators" to manage access to vehicle data. The consensus was that while this should not be required initially, the commission may want to

consider imposing such a requirement if evidence suggests owners/independent repair facilities are experiencing obstacles in obtaining appropriate access to vehicle information. Similarly, while there was consensus that the commission initially should not impose a credentialing or other process to ensure that only properly authorized individuals receive access to vehicle information, the commission may want to consider whether such a process would be useful.

There was consensus that an automaker would not send a command to a vehicle in an unsafe manner. There was consensus that some commands sent to vehicles for maintenance, diagnosis, and repairs when physically present at a vehicle could pose safety risks when sent to the vehicle remotely. The commission may want to consider whether amendments to the law are necessary to mitigate these risks. By way of example only, auto makers have determined that certain commands should not be sent to a vehicle while the vehicle is in motion.

Because the commission will initially be only advisory, there was consensus among working group members that the entity will not immediately need rulemaking or enforcement authority. With respect to enforcement, the statute already authorizes the entity to refer matters to the Attorney General for enforcement. There is some ambiguity regarding whether the Attorney General can bring an enforcement action without a referral from the entity (for example, if the Attorney General receives a complaint directly from an owner or independent repair facility). There was consensus that the statute should be amended to make clear that a referral from the entity is not a prerequisite for enforcement action. If the commission determines that it needs its own enforcement authority, it can so recommend in its annual report.

The working group determined that at least initially, the commission will not need staff, although it may need some administrative support to assist in scheduling meetings, maintaining a website, arranging for remote access, and other administrative matters. The Office of the Attorney General may be able to provide at least some of that support. The working group does not expect that the commission will need funding beyond that necessary to compensate members for expenses.

The working group recognizes that the role it recommends that the commission play may not be entirely consistent with the role that the right to repair law seems to contemplate for the independent entity. That said, there was unanimous consensus that the role outlined above makes the most sense during the initial implementation of the law, with the understanding that the commission may well determine it should be given increased authority and responsibilities if issues are encountered with compliance during the law's implementation.

Attached as Exhibit B are recommended changes to the right to repair law. Primarily, the suggested changes set forth the process for appointing persons to the commission and redefine the entity's responsibilities, as discussed above. During the course of its work, the working group identified some additional provisions in the law that it determined should be clarified or corrected, and the attached reflects the working group's recommendations for those clarifications and corrections.

## Other Recommendations

Some working group members had additional recommendations. While there was not consensus on these recommendations, the working group decided to include these recommendations in the report to the extent they may be helpful as the Legislature considers further actions.

Some members of the working group recommend that the commission consider hearing from stakeholders with relevant and necessary expertise, including consumer and privacy advocates. Because any person who has access to vehicle data could potentially misuse that data to obtain information regarding a vehicle's operator, and because such misuse by a perpetrator of domestic abuse could pose safety concerns, the commission should also consider hearing from advocates for survivors of domestic abuse.

Notwithstanding, working group members representing the aftermarket parts distributors and retailers, the independent repair facilities, and the aftermarket parts manufacturers would seek to clarify that the working group is not suggesting that 29-A M.R.S. § 1810 or diagnostic repair data presents an additional risk of domestic violence to that which existed prior to the statute.

The Alliance for Automotive Innovation recommends that the term "standardized access platform," which is referenced in 29-A M.R.S. § 1810(2) and (6), be defined.

The Alliance also recommends that Section 1810(6) be amended and/or clarified such that compliance with the section is not contingent upon implementation of a specific technological solution. The Alliance recommends that the section be "technologically neutral" with respect to compliance, such that compliance would be determined based not on whether a specific technology is implemented, but on whether data is provided as required by the law.

Both the Alliance and Tesla recommend that implementation of Section 1810(6) (the telematics provision) be postponed. While this provision does not expressly reference the entity, the Alliance and Tesla interpret that provision, in conjunction with 29-A M.R.S. § 1810(2), as requiring motor vehicle manufacturers to provide access to telematics data utilizing specific standards to be defined by the independent entity and integrating with and equipping their vehicles with a standardized access platform to be created and administered by the independent entity. As noted above, motor vehicle manufacturers must begin complying with the requirements of Section 1810(6) no later than January 5, 2025. The Alliance and Tesla contend that until Section 1810(2) is amended to clarify that the entity will not maintain, provide access to, or otherwise exercise control over vehicle data, it is uncertain what vehicle manufacturers must do to comply with Section 1810(6). The Alliance and Tesla recommend that implementation of Section 1810(6) be delayed until one year after any amendments to Section 1810.

Working group members representing the aftermarket parts distributors and retailers, the independent repair facilities, and the aftermarket parts manufacturers oppose postponing implementation of Section 1810(6). They contend that automobile manufacturers had ample opportunity to have discussions with the Maine Attorney General's office and stakeholders to

discuss any perceived uncertainties regarding what manufacturers must do to comply with the law. They also contend that manufacturers are currently technologically capable of complying with the law. Finally, they note that approximately 84% of Maine voters approved the citizen-initiated bill in November 2023.

Tesla recommends that the Legislature consider amending Section 1810 to exclude from its coverage commercial and heavy duty motor vehicles. Tesla notes that during the public hearing on October 16, 2024, information was presented that medium and heavy duty vehicles differ from automobiles with respect to their manufacture, usage, ownership, and repair. Tesla recommends that in light of these differences, the Legislature should consider the extent to which Section 1810 should apply to commercial motor vehicles and heavy duty vehicles.

Working group members representing the aftermarket parts distributors and retailers, the independent repair facilities, and the aftermarket parts manufacturers maintain that commercial and heavy duty motor vehicles should remain subject to the law. They point out that there was testimony that owners and independent repair facilities would benefit from access to diagnostic and repair information and that the working group has recommended that a representative of a heavy duty vehicle manufacturer and an owner or operator of a heavy duty vehicle independent repair facility be appointed to the commission to address any issues unique to heavy duty vehicles.

Tesla recommends that the Legislature consider amending Section 1810 as follows:

“Access must include the ability to receive data and send commands to in vehicle components if needed for purposes of maintenance, diagnostics, and repair and that the manufacturer makes available to its authorized repair shops.”

Tesla contends that this will mitigate potential risks posed by remotely sending commands to vehicles and will ensure a level playing field for all types of repair facilities.

Working group members representing the aftermarket parts distributors and retailers, the independent repair facilities, and the aftermarket parts manufacturers believe this proposed language is ambiguous and would caution the Legislature in making any such amendment without fully understanding the implications regarding owners having access to maintenance, diagnostic, and repair data.

The member representing new motor vehicle dealers recommends that the provision in Section 1810 directing the independent entity to “[c]reate policies for compliance with relevant laws, regulations, standards, technologies and best practices related to access to motor vehicle data” be retained and that Section 1810 be amended to direct the independent entity to consider potential cyber-security and privacy concerns relating to telematics data and rules or other measures that could be implemented to address such concerns.

# **EXHIBIT A**

AARON M. FREY  
ATTORNEY GENERAL



STATE OF MAINE  
OFFICE OF THE ATTORNEY GENERAL  
6 STATE HOUSE STATION  
AUGUSTA, MAINE 04333-0006

TEL: (207) 626-8800  
TTY USERS CALL MAINE RELAY 711

REGIONAL OFFICES  
84 HARLOW ST. 2ND FLOOR  
BANGOR, MAINE 04401  
TEL: (207) 941-3070  
FAX: (207) 941-3075

125 PRESUMPSHOT ST., SUITE 26  
PORTLAND, MAINE 04103  
TEL: (207) 822-0260  
FAX: (207) 822-0259

14 ACCESS HIGHWAY, STE. 1  
CARIBOU, MAINE 04736  
TEL: (207) 496-3792  
FAX: (207) 496-3291

July 3, 2024

The Honorable Chip Curry  
The Honorable Tiffany Roberts  
Committee on Innovation, Development,  
Economic Advancement and Business  
100 State House Station  
Augusta, ME 04333

Re: *Automotive Right to Repair Legislation*

Dear Senator Curry and Representative Roberts:

Last November, Maine voters approved Initiated Bill 3 (LD 1677), *An Act Regarding Automotive Right to Repair*. The law took effect on January 5, 2024 and requires manufacturers of certain motor vehicles to make on-board diagnostic and repair information systems accessible to owners and independent repair facilities.<sup>1</sup> One provision in particular requires the Attorney General to "designate an independent entity not controlled by one or more motor vehicle manufacturers to establish and administer access to vehicle-generated data that is available through the on-board diagnostic system or that is transmitted by the standardized access platform authorized under this section."<sup>2</sup> This "independent entity" shall:

- A. Identify and adopt relevant standards for implementation of this section and relevant provisions for accreditation and certification of organizations and for a system for monitoring policy compliance;
- B. Monitor and develop policies for the evolving use and availability of data generated by the operations of motor vehicles; and

---

<sup>1</sup> 29-A M.R.S. § 1810

<sup>2</sup> 29-A M.R.S. § 1810(2)

- C. Create policies for compliance with relevant laws, regulations, standards, technologies and best practices related to access to motor vehicle data.

Subsequently, during its Second Regular Session, the 131<sup>st</sup> Legislature considered two pieces of legislation relating to the Right to Repair law: LD 1911, *An Act Concerning Automotive Right to Repair*, and LD 2289, *Resolve, to Establish an Automotive Right to Repair Working Group*. LD 1911 began as a competing measure to the citizen-initiated LD 1677. Amendments were subsequently introduced to either eliminate an independent entity or at least delay the designation of an independent entity. LD 2289 was likely intended to complement these amendments because it proposed a working group to immediately make a study of what is needed for an effective independent entity.

Specifically, with respect to LD 2289, this resolve directed the Attorney General to “convene a working group to develop recommendations for legislation to establish an entity with rule-making and enforcement authority to adopt standards governing access to motor vehicle telematics systems and to otherwise implement and enforce the requirements of the Maine Revised Statutes, Title 29-A, section 1810.” The working group is directed to address the entity’s ability to, among other things, “[i]dentify and adopt relevant standards for implementing the requirements of Title 29-A, section 1810,” “[d]evelop and monitor policies for the evolving use and availability of data generated by the operations of motor vehicles,” and “[c]reate policies for compliance with relevant laws, regulations, standards, technologies and best practices related to motor vehicle data.” The entity the working group is to study creating is thus the same as the “independent entity” the Attorney General is to designate pursuant to 29-A M.R.S. § 1810(2).

Ultimately, LD 2289 was passed into law, while LD 1911 was not. This left my office in a position of having to create a working group to study what is needed for an effective entity *and* the requirement to designate an independent entity. After consideration of the requirements placed upon my office, it makes sense to convene a working group in order to develop legislation to create the entity that could then be designated as the independent entity. Importantly, the effectiveness of the independent entity would benefit from clarification of the entity’s legal status and its ability to promulgate rules, issue enforceable orders, and receive funding to carry out its activities. Consideration could also be given to privacy and cybersecurity concerns relating to potentially sensitive motor vehicle information. Accordingly, I have decided to proceed with creating the study group as set forth in Chapter 171 before designating an independent entity.

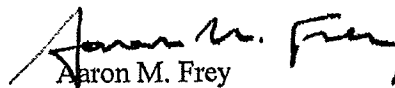
I have instructed my Chief Deputy, Chris Taub, and the Chief of my Consumer Protection Division, Christina Moylan, to coordinate the creation and work of the study group. In the coming weeks, they will be inviting individuals, as described in Chapter 171, to participate in the group. Upon formation, the group will meet throughout the remainder of this year and into early next year. By February 28, 2025, I will submit to this Committee a report detailing the findings and recommendations of the working group.

*The Honorable Chip Curry*  
*The Honorable Tiffany Roberts*  
*July 3, 2024*  
*Page 3*

---

If I may provide any additional information regarding this matter, please let me know.

Sincerely,

  
Aaron M. Frey  
Attorney General



# **EXHIBIT B**

## §1810. Right to repair

**1. Access to diagnostic systems.** Access to the vehicle on-board diagnostic systems of all motor vehicles, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, must be standardized and made accessible to owners and independent repair facilities and the access may not require authorization by the manufacturer, directly or indirectly, unless that authorization is standardized across all makes and models of motor vehicles sold in this State and is administered by the independent entity described in subsection 2.

### **2. ~~Independent entity~~ Motor Vehicle Right to Repair Commission established.**

**A. Commission established.** The Motor Vehicle Right to Repair Commission, as established in Title 5, section 12004-G, subsection [X] and referred to in this section as "the commission," shall carry out the purposes of this subsection.

**B. Membership.** The Attorney General Governor shall designate an independent entity appoint eleventwelve members to the commission. These members must include: not controlled by one or more motor vehicle manufacturers to establish and administer access to vehicle-generated data that is available through the on-board diagnostic system or that is transmitted by the standardized access platform authorized under this section. The independent entity must consist of one representative each from a cross section of industry trade groups including but not limited to organizations representing motor vehicle manufacturers, aftermarket parts manufacturers, aftermarket parts distributors and retailers, independent motor vehicle service providers and new car dealers. The independent entity shall manage cyber-secure access to motor vehicle-generated data, including ensuring on an ongoing basis that access to the on-board diagnostic system and standardized access platform is secure based on all applicable United States and international standards.

\_\_\_\_\_ (1) Three members representing motor vehicle manufacturers, at least one of whom represents an organization of motor vehicle manufacturers, and at least one of whom represents a heavy duty vehicle manufacturer;

\_\_\_\_\_ (2) One member representing aftermarket parts manufacturers;

\_\_\_\_\_ (3) One member representing diagnostic tool manufacturers;

\_\_\_\_\_ (4) One member representing aftermarket parts distributors and retailers;

\_\_\_\_\_ (5) Three members representing Maine independent repair facilities, at least one of whom is an

owner or operator of an independent repair facility specializing in automobiles, and at least one of whom is an owner or operator of an independent repair facility specializing in heavy duty vehicles;

\_\_\_\_\_ (6) One member representing Maine new motor vehicle dealers;

\_\_\_\_\_ (7) One member with expertise in automotive cyber-security matters; and

\_\_\_\_\_ (8) One member representing the public who is a resident of Maine, who shall serve as chair.

**C. Terms.** Members are appointed to 3-year terms. Of the initial appointees, ~~three~~four appointees shall be appointed to an initial term of one year, ~~three~~four appointees shall be appointed to an initial term of two years, and four appointees shall be appointed to an initial term of three years. In making appointments, the Governor may take into consideration the nominations timely made by industry stakeholders or trade associations.

D. Meetings. The commission shall meet at least quarterly, but may meet more frequently at the chair's discretion.

E. Staff. The Attorney General may provide administrative support within the limits of existing resources.

F. Duties. The independent entity shall:

A. (1) The commission shall

- a. Monitor and assess implementation of and motor vehicle manufacturers' compliance with this section;
- b. Attempt to informally resolve any complaints from owners and independent repair facilities alleging a manufacturer's non-compliance with this section, and, if a complaint cannot be resolved, considering whether to refer the matter to the Attorney General for enforcement action; and
- c. Designate one or more technical experts with whom the Attorney General may consult in assessing enforcement referrals and maintaining enforcement actions.

(2) The commission may

- a. —Issue recommendations for best practices for manufacturers to use in providing access to vehicle data.; and
- b. Hear from stakeholders and other interested parties regarding privacy issues associated with the disclosure of motor vehicle-generated data.

Identify and adopt relevant standards for implementation of this section and relevant provisions for accreditation and certification of organizations and for a system for monitoring policy compliance;

B. Monitor and develop policies for the evolving use and availability of data generated by the operations of motor vehicles; and

C. Create policies for compliance with relevant laws, regulations, standards, technologies and best practices related to access to motor vehicle data.

G. -Report. The commission shall submit annually to the joint standing committee of the legislature having jurisdiction over innovation, development, economic advancement, and business matters, the Governor, and the Attorney General, a report describing the commission's activities during the preceding year, identifying any implementation or compliance issues that it encountered, and recommending any amendments to the statute, including amendments providing the entity with additional authority, to address any implementation or compliance issues.

**3. Model year 2002 and later motor vehicles.** For model year 2002 motor vehicles, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, each manufacturer of motor vehicles sold in this State shall make available for purchase under fair and reasonable terms by owners and independent repair facilities all diagnostic repair tools, parts, software and components incorporating the same diagnostic, functional repair and wireless capabilities that the manufacturer makes available to its authorized repair shops. Each manufacturer shall:

A. Provide diagnostic repair information to each aftermarket scan tool company and each 3rd-party service information provider with whom the manufacturer has appropriate licensing, contractual or confidentiality agreements for the sole purpose of building aftermarket diagnostic tools and 3rd-

party service information publications and systems. ~~Once a~~ A manufacturer who makes information available pursuant to this paragraph, ~~the manufacturer is considered to have has~~ satisfied its obligations under this paragraph and thereafter is not responsible for the content and functionality of aftermarket diagnostic tools or service information systems;

B. Make available for purchase by owners of motor vehicles and by independent repair facilities the same diagnostic and repair information, including repair technical updates, that the manufacturer makes available to its authorized repair shops through the manufacturer's Internet-based diagnostic and repair information system; and

C. Provide access to the manufacturer's diagnostic and repair information system for purchase by owners of motor vehicles and independent repair facilities on a daily, monthly and yearly subscription basis and upon fair and reasonable terms.

All parts, tools, software and other components necessary to complete a full repair of the vehicle, as referenced in this subsection, must be ~~included and~~ provided to owners of motor vehicles and authorized independent repair shops.

**4. Model year 2002-2017 motor vehicles.** For model year 2002-2017 motor vehicles, including commercial motor vehicles and heavy-duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, manufacturers must provide access to a vehicle's on-board diagnostic and repair information system ~~must be the same for to an owner or an owner-authorized~~ independent repair facility to the same extent as that provided to a new vehicle dealer.

**5. Model year 2018 and later motor vehicles.** For model year 2018 and later motor vehicles, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, manufacturers must provide access to the on-board diagnostic and repair information system ~~must be available through use of an off-the-shelf personal computer with sufficient memory, processor speed, connectivity and other capabilities as specified by the vehicle manufacturer and:~~

A. A nonproprietary vehicle interface device that complies with SAE International standard J2534, SAE International standard J1939, commonly referred to as SAE J2534 and SAE J1939, the International Organization for Standardization standard 22900, commonly referred to as ISO 22900, or any successor to SAE J2534, SAE J1939 or ISO 22900 as may be accepted or published by SAE International or the International Organization for Standardization, as appropriate;

B. An on-board diagnostic and repair information system integrated into and entirely self-contained within the vehicle, including, but not limited to, service information systems integrated into an on-board display; ~~and or~~

C. A system that provides direct access to on-board diagnostic and repair information through a nonproprietary vehicle interface, such as ethernet, universal serial bus or digital versatile disc.

Each manufacturer shall provide access to the same on-board diagnostic and repair information available to their dealers, including technical updates to such on-board systems, through such nonproprietary interfaces as referenced in this subsection. All parts, tools, software and other components necessary to complete a full repair of a vehicle, as referenced in this subsection, must be ~~included and~~ provided to motor vehicle owners and authorized independent repair shops.

**6. ~~Required equipment~~ Telematics.** Not later than one year from the effective date of this section, a manufacturer of motor vehicles sold in this State, including commercial motor vehicles and heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, that uses a telematics

system is required to equip vehicles sold in this State with an inter-operable, ~~and~~ standardized and owner-authorized access platform across all of the manufacturer's makes and models. The platform must be capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform. The platform must be directly accessible by the motor vehicle owner through a mobile-based application and, upon the authorization of the owner, all mechanical data must be directly accessible by an independent repair facility or a licensed dealer as described in section 851, subsections 2 and 9, limited to the time to complete the repair or for a period of time agreed to by the motor vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle. Access must include the ability to receive data and send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair and that the manufacturer makes available to its authorized repair shops. All parts, tools, software and other components necessary to complete a full repair of the vehicle, as referenced in this subsection, must be ~~included and~~ provided to motor vehicle owners and owner-authorized independent repair shops.

**7. Exclusions.** Manufacturers of motor vehicles sold in the United States may exclude diagnostic, service and repair information necessary to reset an immobilizer system or security-related electronic modules from information provided to motor vehicle owners and independent repair facilities. If excluded under this subsection, the information necessary to reset an immobilizer system or security-related electronic modules must be made available to motor vehicle owners and independent repair facilities through the secure data release model system as used on the effective date of this section by the National Automotive Service Task Force or other known, reliable and accepted systems.

**8. Enforcement.** If the ~~independent entity commission~~ described by subsection 2 has reason to believe that a manufacturer has violated any provision of this section, the ~~independent entity commission~~ shall notify the Attorney General. In response to a referral from the commission, or in any other instance where the Attorney General believes this section may have been violated, the Attorney General shall promptly may institute any actions or proceedings the Attorney General considers appropriate. The independent entity, through the Attorney General, may apply to in the Superior Court of any county of the State to enforce any lawful order made or action taken by the independent entity pursuant to this section. The Attorney General may seek injunctive relief and a civil penalty of not more than \$10,000 for each violation of this section.

A motor vehicle owner or independent repair facility authorized by an owner who has been denied access to mechanical data in violation of this section may initiate a civil action seeking any remedies under law. Each denial of access is compensable by an award of treble damages or \$10,000, whichever amount is greater.

# Massachusetts Right to Repair Law

General Law – Part I, Title XV, Chapter 93K, Section 2

2020

**Part I****ADMINISTRATION OF THE GOVERNMENT****Title XV****REGULATION OF TRADE****Chapter 93K****AUTOMOTIVE REPAIR****Section 2****ACCESS BY OWNERS OF MOTOR VEHICLES AND BY  
INDEPENDENT REPAIR FACILITIES TO MOTOR VEHICLE  
MANUFACTURER DIAGNOSTIC AND REPAIR INFORMATION  
AND DIAGNOSTIC REPAIR TOOLS OTHERWISE MADE  
AVAILABLE TO DEALERS**

Section 2. (a) Except as provided in subsection (e), for model year 2002 motor vehicles and thereafter and model year 2013 heavy duty vehicles and thereafter, a manufacturer of motor vehicles sold in the commonwealth shall make available for purchase by owners of motor vehicles manufactured by such manufacturer and by independent repair facilities the same diagnostic and repair information, including repair technical updates, that such manufacturer makes available to its dealers through the manufacturer's internet-based diagnostic and repair information system or other electronically accessible manufacturer's repair information system. All content in any such manufacturer's repair information system shall be made available to owners and to independent repair facilities in the same form and manner and to the same extent as is made available to dealers utilizing such diagnostic and repair information system. Each manufacturer shall provide access to such manufacturer's

diagnostic and repair information system for purchase by owners and independent repair facilities on a daily, monthly and yearly subscription basis and upon fair and reasonable terms.

(b) A manufacturer that sells any diagnostic, service or repair information to an independent repair facility or other third party provider in a format that is standardized with other manufacturers, and on terms and conditions more favorable than the manner and the terms and conditions which a dealer obtains the same diagnostic, service or repair information, shall be prohibited from requiring any dealer to continue purchasing diagnostic, service or repair information in a proprietary format, unless such proprietary format includes diagnostic, service, repair or dealership operations information or functionality that is not available in such standardized format.

(c) (1) For model year 2002 motor vehicles and thereafter and model year 2013 heavy duty vehicles and thereafter, each manufacturer of motor vehicles sold in the commonwealth shall make available for purchase by owners and independent repair facilities all diagnostic repair tools incorporating the same diagnostic, repair and wireless capabilities that such manufacturer makes available to its dealers. Such tools shall incorporate the same functional repair capabilities that such manufacturer makes available to dealers. Each manufacturer shall offer such tools for sale to owners and to independent repair facilities upon fair and reasonable terms.

(2) Any diagnostic tool or information necessary to diagnose, service or repair a motor vehicle that a manufacturer sells to an independent repair facility in a manner and on terms and conditions more favorable than the manner and the terms and conditions which a dealer obtains the same



diagnostic tool or information necessary to diagnose, service or repair a motor vehicle, shall also be offered to the dealer in the same manner and on the same terms and conditions as provided to such independent repair facility.

A manufacturer that sells to an independent repair facility any diagnostic tool necessary to diagnose, service or repair a motor vehicle and such diagnostic tool communicates with the vehicle using the same non-proprietary interface used by other manufacturers, the manufacturer delivering such a diagnostic tool shall be prohibited from requiring any dealer from continuing to purchase that manufacturer's proprietary tool and interface unless such proprietary interface has a capability not available in the non-proprietary interface.

(3) Each manufacturer shall provide diagnostic repair information to each aftermarket scan tool company and each third party service information provider with whom the manufacturer has appropriate licensing, contractual or confidentiality agreements for the sole purpose of building aftermarket diagnostic tools and third party service information publications and systems. Once a manufacturer makes such information available pursuant to this section, the manufacturer shall be considered to have satisfied its obligations under this section and thereafter not be responsible for the content and functionality of aftermarket diagnostic tools or service information systems.

(d) (1) Beginning in model year 2018, except as provided in subsection (e), manufacturers of motor vehicles sold in the commonwealth, including heavy duty vehicles that are not heavy duty vehicles built to custom specifications sold in the commonwealth for commercial purposes, shall provide access to their onboard diagnostic and repair

information system, as required under this section, using an off-the-shelf personal computer with sufficient memory, processor speed, connectivity and other capabilities as specified by the vehicle manufacturer and: (i) a non-proprietary vehicle interface device that complies with the Society of Automotive Engineers standard J2534, Society of Automotive Engineers J1939, commonly referred to as SAE J2534 and SAE J1939, the International Organization for Standardization standard 22900, commonly referred to as ISO 22900 or any successor to SAE J2534, SAE J1939 or ISO 22900 as may be accepted or published by the Society of Automotive Engineers or the International Organization for Standardization; (ii) an onboard diagnostic and repair information system integrated and entirely self-contained within the vehicle, including, but not limited to, service information systems integrated into an onboard display; or (iii) a system that provides direct access to onboard diagnostic and repair information through a non-proprietary vehicle interface, such as ethernet, universal serial bus or digital versatile disc. Each manufacturer shall provide access to the same onboard diagnostic and repair information available to their dealers, including technical updates to such onboard systems, through such non-proprietary interfaces as referenced in this paragraph. Nothing in this chapter shall be construed to require a dealer to use a non-proprietary vehicle interface specified in this paragraph, nor shall this chapter be construed to prohibit a manufacturer from developing a proprietary vehicle diagnostic and reprogramming device; provided, however, that: (i) the manufacturer also complies with this paragraph; and (ii) the manufacturer also makes this device available to independent repair facilities upon fair and reasonable terms and otherwise complies with subsection (a).

Notwithstanding anything in the preceding paragraph, motor vehicle owners' and independent repair facilities' access to vehicle on-board diagnostic systems shall be standardized and not require any authorization by the manufacturer, directly or indirectly, unless the authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer.

(2) No manufacturer shall be prohibited from making proprietary tools available to dealers if such tools are for a specific specialized diagnostic or repair procedure developed for the sole purpose of a customer service campaign meeting the requirements set out in 49 CFR 579.5, or performance of a specific technical service bulletin or recall after the vehicle was produced, and where original vehicle design was not originally intended for direct interface through a non-proprietary interface set out in paragraph (1). Provision of such proprietary tools under this paragraph shall not constitute a violation of this chapter even if such tools provide functions not available through the interface set forth in paragraph (1); provided, however, that such proprietary tools are also available to the aftermarket upon fair and reasonable terms. Nothing in this paragraph authorizes manufacturers to exclusively develop proprietary tools, without a non-proprietary equivalent as set forth in paragraph (1), for diagnostic or repair procedures that fall outside the provisions of this paragraph or to otherwise operate in a manner inconsistent with paragraph (1).

(e) Manufacturers of motor vehicles sold in the commonwealth may exclude diagnostic, service and repair information necessary to reset an immobilizer system or security-related electronic modules from

information provided to owners and independent repair facilities. If excluded under this subsection, the information necessary to reset an immobilizer system or security-related electronic modules shall be obtained by owners and independent repair facilities through the secure data release model system currently used by the National Automotive Service Task Force or other known, reliable and accepted systems.

(f) Commencing in model year 2022 and thereafter a manufacturer of motor vehicles sold in the Commonwealth, including heavy duty vehicles having a gross vehicle weight rating of more than 14,000 pounds, that utilizes a telematics system shall be required to equip such vehicles with an inter-operable, standardized and open access platform across all of the manufacturer's makes and models. Such platform shall be capable of securely communicating all mechanical data emanating directly from the motor vehicle via direct data connection to the platform. Such platform shall be directly accessible by the owner of the vehicle through a mobile-based application and, upon the authorization of the vehicle owner, all mechanical data shall be directly accessible by an independent repair facility or a class 1 dealer licensed pursuant to section 58 of chapter 140 limited to the time to complete the repair or for a period of time agreed to by the vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle. Access shall include the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair.

(g) The Attorney General is hereby directed to establish for prospective vehicle owners a motor vehicle telematics system notice that includes, but is not limited to, the following features: (i) an explanation of motor vehicle telematics and its purposes, (ii) a description summarizing the mechanical data collected, stored and transmitted by a telematics system,

(iii) the prospective owner's ability to access the vehicle's mechanical data through a mobile device, and (iv) an owner's right to authorize an independent repair facility to access the vehicle's mechanical data for vehicle diagnostics, repair and maintenance purposes. The notice form shall provide for the prospective owner's signature certifying that the prospective owner has read the telematics system notice.

(h) When selling or leasing motor vehicles containing a telematics system, a dealer holding a class 1 or class 2 license as defined in section 58 of chapter 140 shall provide the motor vehicle telematics system notice to the prospective owner, obtain the prospective owner's signed certification that he or she has read the notice, and provide a copy of the signed notice to the prospective owner. A dealer's failure to comply with the provisions of this subsection shall be grounds for any action by the licensing authority relative to the dealer's license, up to and including revocation, pursuant to section 59 of chapter 140.

# National Highway Traffic Safety Administration (NHTSA)

U.S. Department of Transportation

National Traffic and Motor Vehicle Safety Act Letter

Submitted 6/13/2023 in Case 1:20-cv-12090-DPW



U.S. Department of Transportation  
**National Highway Traffic Safety  
Administration**



June 13, 2023

Ann Marie Dias-Lebrun  
Assistant General Counsel  
BMW of North America, LLC  
annmarie.dias-lebrun@bmwna.com

Natalia Medley  
Senior Counsel  
Fisker Group Inc.  
nmedley@fiskerinc.com

Suzanne Miklos  
Vice President - Global Product Safety &  
Systems  
General Motors LLC  
suzanne.miklos@gm.com

Jason Erb  
Chief Legal Officer  
Vice President, Legal  
Hyundai Motor America  
jerb@hmausa.com

Jeremy Close  
Attorney  
Kia Motors America  
jclose@kiausa.com

Nick Ball  
General Counsel  
McLaren Automotive Incorporated  
nick.ball@mclaren.com

David M. Wertheim  
Vice President & General Counsel  
Ferrari North America, Inc.  
david.wertheim@ferrari.com

Christina Michaels  
Attorney  
Ford Motor Company  
cmicha18@ford.com

Jack Alden  
Senior Counsel  
American Honda Motor Co.  
jack\_alden@na.honda.com

Ramsey Ong  
General Counsel  
Jaguar-Land Rover  
rong2@jaguarlandrover.com

Charles Kim  
Assistant General Counsel  
Mazda North American Operations  
ckim1@mazdausa.com

Anthony Zeph  
Associate General Counsel  
Mercedes-Benz North America  
Anthony.Zeph@mbusa.com

Katherine Knight  
Vice President, General Counsel  
Mitsubishi Motors North America, Inc.  
katherine.knight@na.mitsubishi-motors.com

Emily Landry  
Assistant General Counsel  
Nissan North America, Inc.  
emily.landry@nissan-usa.com

George Feygin  
General Counsel  
Porsche Cars North America, Inc.  
george.feygin@porsche.us

Nancy Bell  
General Counsel  
Rivian Automotive, LLC  
nbell@rivian.com

Alan Degraw  
Senior Counsel  
Stellantis  
alan.degraw@stellantis.com

Michael Carroll  
Associate General Counsel  
Subaru of America  
mcarro@subaru.com

Eric Williams  
Associate General Counsel, Regulatory  
Tesla, Inc.  
erwilliams@tesla.com

Kimberly Utevic  
Assistant General Counsel  
Toyota Motor North America  
kim.udovic@toyota.com

Brian Kapatkin  
Corporate Counsel  
Volkswagen Group of America, Inc.  
brian.kapatkin@vw.com

Robert Sullivan  
Counsel  
Volvo Car USA, LLC  
robert.sullivan@volvocars.com

Dear Counsel for Vehicle Manufacturers:

The National Highway Traffic Safety Administration (NHTSA) is sending this letter to advise vehicle manufacturers of their obligations under the National Traffic and Motor Vehicle Safety Act (Safety Act), 49 C.F.R. Chapter 301, in light of a Massachusetts law that NHTSA believes poses significant safety concerns. That law, previously known as SD645 and now codified at Chapter 93K of the Massachusetts General Laws (the Data Access Law), requires open remote access to vehicle telematics.<sup>1</sup> As explained below, the Data Access Law conflicts with and therefore is preempted by the Safety Act.

While NHTSA has stressed that it is important for consumers to continue to have the ability to choose where to have their vehicles serviced and repaired, consumers must be afforded choice in

---

<sup>1</sup> NHTSA understands that Massachusetts stated its intent to enforce the law beginning on June 1, 2023. *Alliance for Automotive Innovation v. Campbell*, Case No. 1:20-cv-12090, Dkt. No. 330 (“Notice of Intent to Terminate Non-Enforcement Stipulation”) (D. Mass.) (hereinafter “Notice of Intent”).



a manner that does not pose an unreasonable risk to motor vehicle safety.<sup>2</sup> In this case, NHTSA previously described its serious safety concerns with the Data Access Law's requirement of open remote access in a filing in pending federal district court litigation that challenges the law. *Alliance for Automotive Innovation v. Campbell*, Case No. 1:20-cv-12090, Dkt. No. 202 (D. Mass) ("United States' Statement of Interest").<sup>3</sup> The open remote access to vehicle telematics effectively required by this law specifically entails "the ability to send commands."<sup>4</sup> Open access to vehicle manufacturers' telematics offerings with the ability to remotely send commands allows for manipulation of systems on a vehicle, including safety-critical functions such as steering, acceleration, or braking, as well as equipment required by Federal Motor Vehicle Safety Standards (FMVSS) such as air bags and electronic stability control. A malicious actor here or abroad could utilize such open access to remotely command vehicles to operate dangerously, including attacking multiple vehicles concurrently.<sup>5</sup> Vehicle crashes, injuries, or deaths are foreseeable outcomes of such a situation.

Vehicle manufacturers appear to recognize that vehicles with the open remote access telematics required by the Data Access Law would contain a safety defect. Federal law does not allow a manufacturer to sell vehicles that it knows contain a safety defect. *See* 49 U.S.C. §§ 30112(a)(3); 30118(c)(1). Furthermore, as you are aware, the Safety Act imposes an affirmative obligation on vehicle manufacturers to initiate a recall of vehicles that contain a safety defect. 49 U.S.C. § 30118(c).

Given the serious safety risks posed by the Data Access Law, taking action to open remote access to vehicles' telematics units in accordance with that law, which requires communication pathways to vehicle control systems, would conflict with your obligations under the Safety Act.<sup>6</sup> "The purpose of the Safety Act . . . is not to protect individuals from the risks associated with defective vehicles only after serious injuries have already occurred; it is to prevent serious

---

<sup>2</sup> To ensure consumers have adequate access to repair facilities, a 2014 Memorandum of Understanding (MOU) already provides secure access to vehicle telematics to independent repair facilities nationwide. *See* MOU (Jan. 15, 2014) *available at* <https://www.autocare.org/docs/default-source/government-affairs/r2r-mou-and-agreement-signed.pdf>.

<sup>3</sup> *See also* Letter from James Owens, Deputy Administrator, NHTSA, to Massachusetts's Joint Committee on Consumer Protection and Professional Licensure (Jul. 20, 2020) *available at* [https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/nhtsa\\_testimony\\_in\\_response\\_to\\_ma\\_committee\\_letter\\_july\\_20\\_2020.pdf](https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/nhtsa_testimony_in_response_to_ma_committee_letter_july_20_2020.pdf).

<sup>4</sup> Mass. Gen. Laws 93K § 2(f).

<sup>5</sup> As NHTSA has previously stated: "Wireless interfaces into vehicle systems create new attack vectors that could potentially be remotely exploited. Unauthorized wireless access to vehicle computing resources could scale rapidly to multiple vehicles without appropriate controls." *Cybersecurity Best Practices for the Safety of Modern Vehicles* at 15 (Sept. 2022), *available at* <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf>.

<sup>6</sup> *See, e.g.*, NHTSA Recall No. 15V-461, *available at* <https://static.nhtsa.gov/odi/rcl/2015/RCLRPT-15V461-9313.PDF>; NHTSA Recall No. 15V-508, *available at* <https://static.nhtsa.gov/odi/rcl/2015/RCLRPT-15V508-8738.PDF>.

injuries stemming from established defects before they occur.” *United States v. Gen. Motors Corp.*, 565 F.2d 754, 759 (D.C. Cir. 1977).

NHTSA is aware that certain vehicle manufacturers have stated an intent to disable vehicle telematics, presumably to avoid the application of the Data Access Law to their vehicles.<sup>7</sup> This measure has its own adverse impacts on safety. For example, telematics-based safety features could facilitate better emergency response in the event of a vehicle crash. Telematics data can also be an important source of information for safety oversight and field performance monitoring by the authorities and vehicle manufacturers. NHTSA often utilizes telematics data in its investigations, and the inability to obtain these data from vehicles with this capability undermines the agency’s ability to fully examine safety-related issues. In addition, some vehicle manufacturers have the ability to fix safety problems by remedying recalls through vehicle telematics, which will be lost if those systems are disabled. Manufacturers should assess the impacts of any planned actions on roadway safety comprehensively.

We appreciate your attention to this important safety matter and trust you will give your highest priority to ensuring motor vehicle safety. Because the Safety Act conflicts with and therefore preempts the Data Access Law, NHTSA expects vehicle manufacturers to fully comply with their Federal safety obligations.

Sincerely,

KERRY E  
KOLODZIEJ

Digitally signed by  
KERRY E KOLODZIEJ  
Date: 2023.06.13  
12:47:08 -04'00'

Kerry Kolodziej  
Assistant Chief Counsel  
for Litigation and Enforcement

CC:

Robert E. Toone  
Assistant Attorney General  
Commonwealth of Massachusetts  
robert.toone@mass.gov

Jessica Simmons  
Assistant General Counsel  
Alliance for Automotive Innovation  
jsimmons@autosinnovate.org

---

<sup>7</sup> Notice of Intent.

# National Highway Traffic Safety Administration (NHTSA)

U.S. Department of Transportation

National Traffic and Motor Vehicle Safety Act Letter 2

Dated 8/22/2023 – Follow-up to June letter

(Sometimes referred to as the “Retraction Letter”)



U.S. Department of Transportation  
**National Highway Traffic Safety  
Administration**



August 22, 2023

Eric A. Haskell  
Assistant Attorney General  
Office of the Attorney General  
Commonwealth of Massachusetts  
One Ashburton Place  
Boston, MA 02108

Dear Mr. Haskell:

Thank you for your engagement with the United States Department of Transportation, National Highway Traffic Safety Administration (NHTSA), and our other Federal government partners to advance our mutual interest in ensuring safe consumer choice for automotive repair and maintenance. NHTSA strongly supports the right to repair. We are pleased to have worked with you to identify a way that the Massachusetts Data Access Law may be successfully implemented—promoting consumers’ ability to choose independent or do-it-yourself repairs—without compromising safety. We write to confirm our mutual understanding of that path forward.

As you are aware, NHTSA’s concerns regarding the Massachusetts Data Access Law arise from the risk associated with the ability to, at scale, remotely access and send commands that affect a vehicle’s critical safety systems.

Based on our further conversations, NHTSA understands that, according to the Massachusetts Attorney General, one way that vehicle manufacturers can comply with the Data Access Law is by providing independent repair facilities wireless access to a vehicle from within close physical proximity to the vehicle, without providing long-range remote access. For instance, NHTSA understands that, according to the Attorney General, vehicle manufacturers could comply with the Data Access Law by using short-range wireless protocols, such as via Bluetooth, to allow the vehicle owner or an independent repair facility authorized by the owner to access all “mechanical data,” as defined by the Law, for that individual vehicle. In NHTSA’s view, a solution like this one, if implemented with appropriate care, would significantly reduce the cybersecurity risks—and therefore the safety risks—associated with remote access. Limiting the geographical range of access would significantly reduce the risk that malicious actors could exploit vulnerabilities at scale to access multiple vehicles, including, importantly, when vehicles are driven on a roadway. Such a short-range wireless compliance approach, implemented appropriately, therefore would not be preempted.

NHTSA requests your confirmation that a solution allowing wireless access when in close physical proximity to the vehicle would be compliant with the Massachusetts Data Access Law.

Based on our discussions to-date, it appears that the Massachusetts Attorney General and NHTSA also share a common understanding that implementing this compliance option with the secure “open access platform,” as required in the Law, is not immediately available, and that vehicle manufacturers may require a reasonable period of time to securely develop, test, and implement this technology. We welcome the opportunity to work with you and other stakeholders on the safe and timely implementation of this option.

Two additional points bear emphasis. First, NHTSA wishes to reiterate the point made in its June 13 letter that some vehicle telematics functions—when and if appropriately secured—can advance vehicle safety. Disabling vehicle telematic functions as an attempt to comply with the Data Access Law would harm vehicle owners, first responders, and other telematics users. For example, vehicle telematics can be life-saving technology, communicating essential data about a vehicle’s location to emergency services in the event of a crash. Safety investigators, including police, NHTSA, and other governmental authorities, increasingly rely on access to vehicle data about crashes and other safety issues collected via telematics. NHTSA would have substantial concerns about the detriment to safety if vehicle telematics functionality were disabled, and believes such a result would disserve vehicle owner safety without advancing the right to repair.

Second, NHTSA wishes to emphasize that its concerns regarding risk associated with the broad ability to remotely access and send commands that control a vehicle’s critical safety systems do not arise from a belief that any particular entity or person seeking to repair a vehicle—whether a vehicle manufacturer or manufacturer-affiliated dealer, an independent repair facility, or a do-it-yourself vehicle owner—necessarily poses a greater cybersecurity concern than another. Whenever access to write or execute command functionality remotely is contemplated, it is important to be vigilant to minimize risks. NHTSA works to minimize this risk at any level of access—whether by an original equipment manufacturer, dealer, or independent repair facility—and is continually overseeing existing systems for cybersecurity vulnerabilities. NHTSA supports technological developments that can enhance vehicle safety and consumer choice. NHTSA will continue to evaluate safety programs and protocols as technology in this area evolves, which may also enable additional safe compliance pathways under the Massachusetts Data Access Law.

NHTSA values the dialogue with the Massachusetts Attorney General toward achieving the dual goals of consumer choice in repair facilities and vehicle safety, and looks forward to continued dialogue to help ensure that vehicle manufacturers safely and expeditiously comply with their obligations under the Data Access Law and the Federal Vehicle Safety Act.

Sincerely,

KERRY ELIZABETH  
KOLODZIEJ

Digitally signed by KERRY  
ELIZABETH KOLODZIEJ  
Date: 2023.08.22 12:23:02  
-04'00'

Kerry Kolodziej  
Assistant Chief Counsel  
for Litigation and Enforcement

# Automotive Repair Data Sharing Commitment

Automotive Service Association  
Society of Collision Repair Specialists  
Alliance for Automotive Innovation

2014



### **Automotive Repair Data Sharing Commitment**

This commitment was created with one group of people in mind: vehicle owners. It recognizes and reaffirms the belief that consumers should have access to safe and proper repairs throughout a vehicle's lifecycle.

The parties commit to ensure consumer choice in vehicle repair decisions and support the independent repair community as provided below and as outlined in the existing 2014 Memorandum of Understanding:

**Access to diagnostic and repair information** – There shall be available for purchase by owners of motor vehicles and by independent repair facilities on fair and reasonable terms the same diagnostic and repair information, including service manuals and technical repair updates, that a manufacturer makes available to its authorized dealers through the manufacturer's internet-based diagnostic and repair information system or other electronically accessible repair information system.

**Access to vehicle systems** – There shall be available access to vehicle diagnostic systems through (i) a non-proprietary vehicle interface device that complies with the Society of Automotive Engineers standard J2534, commonly referred to as SAE J2534, the International Organization for Standardization standard 22900, commonly referred to as ISO 22900 or any successor to SAE J2534 or ISO 22900 as may be accepted or published by the Society of Automotive Engineers or the International Organization for Standardization; (ii) an onboard diagnostic and repair data system integrated and entirely self-contained within the vehicle, including, but not limited to, diagnostic or service information systems integrated into an onboard display; or (iii) a system that provides direct access to onboard diagnostic and repair data through a non-proprietary vehicle interface, such as ethernet, universal serial bus or digital versatile disc; provided that each manufacturer provides access to the same onboard diagnostic and repair data and functions available to their dealers, including technical updates to such onboard systems, through such non-proprietary interfaces as referenced in this paragraph.

**Alternate Fueled Vehicles** – Just as is the case for traditional internal combustion vehicles, access to vehicle diagnostic data and to vehicle systems for diagnostic and repair purposes shall be available for purchase by vehicle owners and by independent repair facilities on fair and reasonable terms for alternately fueled vehicles. This commitment applies to all vehicle technologies regardless of powertrain, including gasoline, diesel, fuel cell, electric battery, hybrid, and plug-in hybrid electric powertrains.

**Telematics** – Telematics systems shall not be used to circumvent the commitments made in this commitment to provide independent repair facilities with access to vehicle diagnostic data. To the extent that specific telematic diagnostic and repair data is needed to complete a repair, and also provided to an automaker’s authorized dealers, the automaker shall make such information available to vehicle owners and independent repair facilities, if it is not otherwise available through a tool or third-party service information provider. This does not apply to any telematics data beyond what is necessary to diagnose and repair a vehicle.

**Access to tools** – There shall be made available for purchase by owners of motor vehicles and by independent repair facilities diagnostic repair tools incorporating the same functional capabilities that a manufacturer makes available to its authorized dealers.

**Fair and Reasonable Terms** – There shall be access to diagnostic and repair information and tools on fair and reasonable terms, consistent with U.S. Environmental Protection Agency, California Air Resources Board, and Massachusetts statutory requirements.

**Support of Third-Party Tool Manufacturers** – Diagnostic and repair information shall be made available to each third-party tool manufacturer and each third-party service information provider with whom a manufacturer has appropriate licensing, contractual, or confidentiality commitment for the sole purpose of building diagnostic tools and third-party service information publications and systems.

**Trade secret protections** – Nothing in this commitment shall be construed to require a manufacturer to divulge a trade secret.

**Education** – The parties shall develop a plan to educate both mechanical and collision repair facilities on the avenues by which they can access repair information, including directly through manufacturer repair websites, on [www.oem1stop.com](http://www.oem1stop.com), or by accessing third-party tool and data service providers, among others.

**Training** – The parties shall review existing training options for both mechanical and collision repair facilities and work to ensure repairers have access to the latest training opportunities.

### **Working Together to Address Any Identified Gaps**

As a complement to the existing process for resolving disputes involving the availability of diagnostic and repair information from specific manufacturers established in the 2014 MOU, the parties commit to establish a Vehicle Data Access Panel (VDAP) to identify issues a party may have with respect to the availability of diagnostic data and repair information as pledged in this commitment and collaborate on potential solutions where feasible. The VDAP shall be comprised of representatives from Automotive Service Association, Society of Collision Repair Specialists and Alliance for Automotive Innovation, and shall meet, at a minimum, biannually.



## **Periodic Review to Ensure Continued Relevancy**

In recognition of this industry's dynamic marketplace, the parties commit to review this commitment annually and update, if appropriate. To that end, the parties shall establish a Data Access Working Group to consider any technological advancements that may alter the vehicle repair marketplace. The size and membership of this Working Group shall be established by the parties and can be altered at any time with the commitment of the signing parties.

## **Cooperation and Advocacy**

**Federal legislation** – The parties commit to working together in support of federal legislation to codify the various provisions of this commitment, ensuring consumer choice in vehicle repair across the country. The parties also commit to working together against any legislation that is in direct conflict with the tenets of this document.

**Federal regulations** – The parties commit to working together in support of a petition to the Environmental Protection Agency to ensure reparability of electric vehicles by requiring standardized data communication protocols from OBDII-type connectors on all battery electric, plug-in hybrid, hybrid, and fuel cell vehicles model year 2026 and beyond in alignment with California's Advanced Clean Cars II regulation.

**State legislation** – The parties commit to working together against any legislation that is in conflict with the tenets of this commitment. Engagement on state legislation not in conflict with the tenets of this commitment shall be evaluated on its merits and subject to the commitment of the parties.

## **Signing Parties**

### **Automotive Service Association (ASA)**

ASA is the largest and oldest national organization committed to protecting the automotive repair industry with ONE VOICE. Our members own and operate automotive mechanical and collision repair facilities responsible for the majority of all, post warranty, repair services in the United States. ASA advocates for the interests of its members and their customers in Washington, D.C. The education, resources, and services ASA provides empowers its members in all 50 states to remain trusted stewards of mobility in their communities. [www.ASAShop.org](http://www.ASAShop.org)

### **Society of Collision Repair Specialists (SCRS)**

Through our direct members and affiliate associations, SCRS proudly represents over 6,000 collision repair businesses and 58,500 specialized professionals who work to repair collision-damaged vehicles. Since 1982, SCRS has served as the largest national trade association solely dedicated to the hardworking collision repair facilities across North America. Since its formation, SCRS has provided repairers with an audible voice, and an extensive grassroots network of industry professionals who strive to better our trade. Additional information about SCRS including other news releases is available at the SCRS website. [www.scrs.com](http://www.scrs.com)

**Alliance for Automotive Innovation**

From the manufacturers producing most vehicles sold in the U.S. to autonomous vehicle innovators to equipment suppliers, battery producers and semiconductor makers – Alliance for Automotive Innovation represents the full auto industry, a sector supporting 10 million American jobs and five percent of the economy. Active in Washington, D.C. and all 50 states, the association is committed to a cleaner, safer and smarter personal transportation future.

[www.autosinnovate.org](http://www.autosinnovate.org)

**Effective Date**

This Commitment is effective immediately upon signed letter transmittal to Chairwoman Cantwell, Ranking Member Cruz, Chairwoman McMorris Rodgers, Ranking Member Pallone, Chairman Jordan, Ranking Member Nadler, Chairman Durbin, and Ranking Member Graham.

# Right to Repair Memorandum of Understanding

Auto Alliance Driving Innovation

Global Automakers

Automotive Aftermarket Industry Association

CARE

1/15/2014



**AUTO ALLIANCE**  
DRIVING INNOVATION®

**AAIA**®  
Automotive Aftermarket  
Industry Association

GlobalAutomakers

**CARE**

## MEMORANDUM of UNDERSTANDING

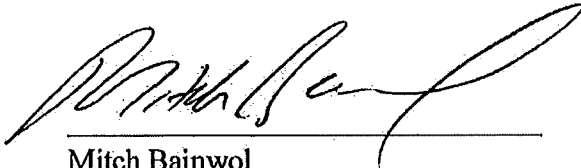
The Automotive Aftermarket Industry Association (“AAIA”), Coalition for Auto Repair Equality (“CARE”), Alliance of Automobile Manufacturers (“Alliance”) and Association of Global Automakers (“Global Automakers”) (“the Original Parties”) enter into this Memorandum of Understanding (MOU) on this Fifteenth (15th) day of January, 2014 and voluntarily agree as follows:

1. The Original Parties fully support this MOU and attached “Right to Repair” (R2R) agreement (“R2R Agreement”). Automobile manufacturer members of the Alliance and Global Automakers indicate their individual company’s agreement to comply with the MOU and R2R Agreement in all fifty (50) States and the District of Columbia through their individual letters of endorsement.
2. Until such time as the provisions of Section 2(c)(i) (common interface device) of the R2R Agreement have been fully implemented, with respect to model year 2018 and newer vehicles, for two years or January 2, 2019, whichever is earlier, and provided the OEMs comply with the MOU during this period, CARE and AAIA agree to continue to work with other Original Parties to fully implement the MOU and to oppose and not to fund or otherwise support, directly or indirectly, any new state R2R legislation.
3. The Original Parties agree to work to strongly encourage any new entrants to the U.S. automotive market or to R2R issues to become signatories to the MOU.
4. The Original Parties agree to work together to resolve any future or related R2R issues that might otherwise be the subject of state legislation and, subject to the mutual consent of the Original parties, amend the MOU and R2R Agreement to include these additional matters.
5. Once the Original Parties have signed on to the MOU, additional parties may join but any amendments or revisions to the terms of the MOU and R2R Agreement, triggered by admission of additional participants, shall require consent of the Original Parties.
6. The Original Parties agree to meet as needed and at least semi-annually, to assess how the MOU is operating, address operational concerns and discuss any other matters relevant to R2R or the MOU or future amendments or parties to the MOU. In the event that one of

the Original Parties concludes that, due to changed circumstances, the MOU or R2R Agreement may no longer be viable, that party shall, upon thirty (30) days written notice to the other three Original Parties, call a meeting to discuss the need for the MOU and R2R Agreement to continue.

7. The Original Parties agree that should a state(s) pass a law relating to issues covered by this MOU and R2R Agreement, after the effective date of the MOU and R2R Agreement, any automobile manufacturer member of the Alliance and Global Automakers may elect to withdraw its letter of endorsement for the MOU and R2R Agreement partially or entirely for the impacted state(s).

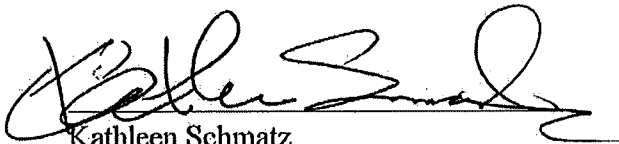
Signed on this 15<sup>th</sup> day of January, 2014:



Mitch Bainwol  
President & CEO  
Alliance of Automobile Manufacturers



Michael Stanton  
President & CEO  
Association of Global Automakers



Kathleen Schmatz  
President & CEO  
Automotive Aftermarket Industry Association



Ray Pohlman  
President  
Coalition for Auto Repair Equality

## **R2R AGREEMENT**

**Section 1.** As used in this agreement, the following words shall, unless the context clearly indicates otherwise, have the following meanings:

**“Dealer”**, any person or business who, in the ordinary course of its business, is engaged in the business of selling or leasing new motor vehicles to consumers or other end users pursuant to a franchise agreement and who has obtained a license, as required under applicable law, and is engaged in the diagnosis, service, maintenance or repair of motor vehicles or motor vehicle engines pursuant to said franchise agreement.

**“Franchise agreement”**, a written arrangement for a definite or indefinite period in which a manufacturer or distributor grants to a motor vehicle dealer a license to use a trade name, service mark or related characteristic and in which there is a community of interest in the marketing of new motor vehicles or services related thereto at wholesale, retail, leasing or otherwise.

**“Fair and Reasonable Terms”** Provided that nothing in this MOU and R2R Agreement precludes an automaker and an owner or independent repair shop who is subject to the agreement from agreeing to the sale of information and tools on any other terms on which they agree, in determining whether a price is on “fair and reasonable terms,” consideration may be given to relevant factors, including, but not limited to, the following:

- (i) The net cost to the manufacturer’s franchised dealerships for similar information obtained from manufacturers, less any discounts, rebates, or other incentive programs.

- (ii) The cost to the manufacturer for preparing and distributing the information, excluding any research and development costs incurred in designing and implementing, upgrading or altering the onboard computer and its software or any other vehicle part or component. Amortized capital costs for the preparation and distribution of the information may be included.

- (iii) The price charged by other manufacturers for similar information.

- (iv) The price charged by manufacturers for similar information prior to the launch of manufacturer web sites.

- (v) The ability of aftermarket technicians or shops to afford the information.

- (vi) The means by which the information is distributed.

- (vii) The extent to which the information is used, which includes the number of users, and frequency, duration, and volume of use.

- (viii) Inflation.

**“Immobilizer system”**, an electronic device designed for the sole purpose of preventing the theft of a motor vehicle by preventing the motor vehicle in which it is installed from starting without the correct activation or authorization code.

**"Independent repair facility"**, a person or business that is not affiliated with a manufacturer or manufacturer's authorized dealer of motor vehicles, which is engaged in the diagnosis, service, maintenance or repair of motor vehicles or motor vehicle engines;

**"Manufacturer"**, any person or business engaged in the business of manufacturing or assembling new motor vehicles.

**"Dispute Resolution Panel (DRP)"**, a 5-person panel established by the Original Parties comprised of the following: one Alliance representative, Alliance member or Alliance designee, one Global Automakers representative, Global Automakers' manufacturer member or Global Automakers designee, two representatives of the independent vehicle repair industry to be selected and mutually agreed upon by AAIA and CARE, and one DRP Chair. The DRP Chair shall be an independent professional mediator with no affiliation to any of the Original Parties, shall be selected by unanimous consent of the Original Parties and shall be funded in equal amounts by each of the Original Parties. The Original Parties shall, at one of the two annual meetings, have an opportunity to revisit their respective representative or ask the Original Parties to revisit the person acting as DRP Chair.

**"Motor vehicle"**, any vehicle that is designed for transporting persons or property on a street or highway and that is certified by the manufacturer under all applicable federal safety and emissions standards and requirements for distribution and sale in the United States, but excluding (i) a motorcycle; (ii) a vehicle with a gross vehicle weight over 14,000 pounds; or (iii) a recreational vehicle or an auto home equipped for habitation.

**"Owner"**, a person or business who owns or leases a registered motor vehicle.

**"Trade secret"**, anything, tangible or intangible or electronically stored or kept, which constitutes, represents, evidences or records intellectual property including secret or confidentially held designs, processes, procedures, formulas, inventions, or improvements, or secret or confidentially held scientific, technical, merchandising, production, financial, business or management information, or anything within the definition of 18 U.S.C. § 1839(3).

## **Section 2.**

(2)(a). Except as provided in subsection (2)(e), for Model Year 2002 motor vehicles and thereafter, a manufacturer of motor vehicles sold in United States shall make available for purchase by owners of motor vehicles manufactured by such manufacturer and by independent repair facilities the same diagnostic and repair information, including repair technical updates, that such manufacturer makes available to its dealers through the manufacturer's internet-based diagnostic and repair information system or other electronically accessible manufacturer's repair information system. All content in any such manufacturer's repair information system shall be made available to owners and to independent repair facilities in the same form and manner and to the same extent as is made available to dealers utilizing such diagnostic and repair information system. Each manufacturer shall provide access to such manufacturer's diagnostic and repair information system for purchase by owners and independent repair facilities on a daily, monthly and yearly subscription basis and upon fair and reasonable terms.

**(2)(b)(i)** For Model Year 2002 motor vehicles and thereafter, each manufacturer of motor vehicles sold in the United States shall make available for purchase by owners and independent repair facilities all diagnostic repair tools incorporating the same diagnostic, repair and wireless capabilities that such manufacturer makes available to its dealers. Such tools shall incorporate the same functional repair capabilities that such manufacturer makes available to dealers. Each manufacturer shall offer such tools for sale to owners and to independent repair facilities upon fair and reasonable terms.

**(ii)** Each manufacturer shall provide diagnostic repair information to each aftermarket scan tool company and each third party service information provider with whom the manufacturer has appropriate licensing, contractual or confidentiality agreements for the sole purpose of building aftermarket diagnostic tools and third party service information publications and systems. Once a manufacturer makes such information available pursuant to this section, the manufacturer will have fully satisfied its obligations under this section and thereafter not be responsible for the content and functionality of aftermarket diagnostic tools or service information systems.

**(2)(c)(i)** Commencing in Model Year 2018, except as provided in subsection (2)(e), manufacturers of motor vehicles sold in the United States shall provide access to their onboard diagnostic and repair information system, as required under this section, using an off-the-shelf personal computer with sufficient memory, processor speed, connectivity and other capabilities as specified by the vehicle manufacturer and:

**(a)** a non-proprietary vehicle interface device that complies with the Society of Automotive Engineers SAE J2534, the International Standards Organizations ISO 22900 or any successor to SAE J2534 or ISO 22900 as may be accepted or published by the Society of Automotive Engineers or the International Standards Organizations; or,

**(b)** an on-board diagnostic and repair information system integrated and entirely self-contained within the vehicle including, but not limited to, service information systems integrated into an onboard display, or

**(c)** a system that provides direct access to on-board diagnostic and repair information through a non-proprietary vehicle interface such as Ethernet, Universal Serial Bus or Digital Versatile Disc. Each manufacturer shall provide access to the same on-board diagnostic and repair information available to their dealers, including technical updates to such on-board systems, through such non-proprietary interfaces as referenced in this paragraph. Nothing in this agreement shall be construed to require a dealer to use the non-proprietary vehicle interface (i.e., SAE J2534 or ISO 22900 vehicle interface device) specified in this subsection, nor shall this agreement be construed to prohibit a manufacturer from developing a proprietary vehicle diagnostic and reprogramming device, provided that the manufacturer also complies with Section 2(c)(i) and the manufacturer also makes this device available to independent repair facilities upon fair and reasonable terms, and otherwise complies with Section 2(a).

**(2)(c)(ii)** No manufacturer shall be prohibited from making proprietary tools available to dealers if such tools are for a specific specialized diagnostic or repair procedure developed for



the sole purpose of a customer service campaign meeting the requirements set out in 49 CFR 579.5, or performance of a specific technical service bulletin or recall after the vehicle was produced, and where original vehicle design was not originally intended for direct interface through the non-proprietary interface set out in (2)(c)(i). Provision of such proprietary tools under this paragraph shall not constitute a violation of this agreement even if such tools provide functions not available through the interface set forth in (2)(c)(i), provided such proprietary tools are also available to the aftermarket upon fair and reasonable terms. Nothing in this subsection (2)(c)(ii) authorizes manufacturers to exclusively develop proprietary tools, without a non-proprietary equivalent as set forth in (2)(c)(i), for diagnostic or repair procedures that fall outside the provisions of (2)(c)(ii) or to otherwise operate in a manner inconsistent with the requirements of (2)(c)(i).

**(2)(d)** Manufacturers of motor vehicles sold in the United States may exclude diagnostic, service and repair information necessary to reset an immobilizer system or security-related electronic modules from information provided to owners and independent repair facilities. If excluded under this paragraph, the information necessary to reset an immobilizer system or security-related electronic modules shall be obtained by owners and independent repair facilities through the secure data release model system as currently used by the National Automotive Service Task Force or other known, reliable and accepted systems.

**(2)(e)** With the exception of telematics diagnostic and repair information that is provided to dealers, necessary to diagnose and repair a customer's vehicle, and not otherwise available to an independent repair facility via the tools specified in 2(c)(i) above, nothing in this agreement shall apply to telematics services or any other remote or information service, diagnostic or otherwise, delivered to or derived from the vehicle by mobile communications; provided, however, that nothing in this agreement shall be construed to abrogate a telematics services or other contract that exists between a manufacturer or service provider, a motor vehicle owner, and/or a dealer. For purposes of this agreement, telematics services include but are not limited to automatic airbag deployment and crash notification, remote diagnostics, navigation, stolen vehicle location, remote door unlock, transmitting emergency and vehicle location information to public safety answering points as well as any other service integrating vehicle location technology and wireless communications. Nothing in this agreement shall require a manufacturer or a dealer to disclose to any person the identity of existing customers or customer lists.

**Section 3.** Nothing in this agreement shall be construed to require a manufacturer to divulge a trade secret.

**Section 4.** Notwithstanding any general or special law or any rule or regulation to the contrary, no provision in this agreement shall be read, interpreted or construed to abrogate, interfere with, contradict or alter the terms of any franchise agreement executed and in force between a dealer and a manufacturer including, but not limited to, the performance or provision of warranty or recall repair work by a dealer on behalf of a manufacturer pursuant to such franchise agreement.

**Section 5.** Nothing in this agreement shall be construed to require manufacturers or dealers to provide an owner or independent repair facility access to non-diagnostic and repair information

provided by a manufacturer to a dealer, or by a dealer to a manufacturer pursuant to the terms of a franchise agreement.

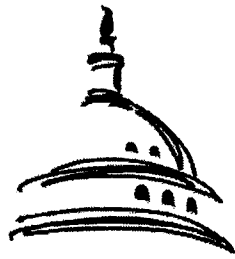
**Section 6.** If an independent repair facility or owner believes that a manufacturer has failed to provide the information or tool required by this MOU, he may challenge the manufacturer's actions by first notifying the manufacturer in writing. The manufacturer has thirty (30) days from the time it receives the reasonably clear and specific complaint to cure the failure, unless the parties otherwise agree. If the complainant is not satisfied, he has thirty (30) days to appeal the manufacturer's decision to the DRP. The DRP shall be convened by the Chair within thirty (30) days of receipt of the appeal of the manufacturer's decision. The DRP will attempt to reach agreement between the parties. If unsuccessful, the DRP shall convene and issue its decision. The decision must be issued within 30 days of receipt of the appeal of the manufacturer's decision, unless otherwise agreed to by the parties. The DRP decision shall be disseminated to the complainant, the manufacturer, and the Original Parties. If the manufacturer and complainant still cannot reach agreement, the complainant may take whatever legal measures are available to it.

# Access to Motor Vehicle Software and Data

Congressional Research Service

Dana A. Scherer, Specialist in Telecommunication Policy

7/19/2024



**Congressional  
Research Service**

Informing the legislative debate since 1914

---

# Access to Motor Vehicle Software and Data

**Dana A. Scherer**

Specialist in Telecommunications Policy

July 19, 2024

**Congressional Research Service**

7-5700

[www.crs.gov](http://www.crs.gov)

R48131



## Access to Motor Vehicle Software and Data

The marketplace of goods and services after the initial sale of a vehicle—including replacement parts, maintenance services, and repair services—is known as the *aftermarket*. Some industry participants and consumers contend that the growing prevalence of software and sensors within motor vehicles has enabled motor vehicle manufacturers—*original equipment manufacturers* (OEMs)—to limit competition in the aftermarket. *Right to repair* is a term used by various advocacy groups supporting fewer restrictions on consumers' ability to repair products they have purchased through legislative changes and other means. In the context of the aftermarket, it refers to consumers' ability to select who repairs and/or maintains their motor vehicles.

Motor vehicles' software supports many functions, including (1) controlling the vehicle's safety and comfort features and (2) assisting drivers via a set of in-vehicle technologies (also known as *advanced driver assisted systems*). In addition, the software enables *telematics*, that is, the wireless transmission of data to and from vehicles and data centers hosted by the vehicle manufacturers. Access to motor vehicles' telematics data has become a focal point of the motor vehicle right-to-repair policy debate.

In addition to consumers and workshops (i.e., entities that offer repair and maintenance goods and services), several other participants have a financial stake in the flow of goods and services in the aftermarket supply chain. During the warranty period of motor vehicles, OEMs pay for goods and services covered by the warranty. In addition, OEMs sell replacement parts and licenses for access to motor vehicle software, data, repair manuals, and diagnostic tools to workshops. Insurance companies pay workshops directly or reimburse consumers for post-collision repairs.

Copyright laws, typically enforced by courts and administered by the Library of Congress, penalize consumers and third parties that violate copyright holders' exclusive rights to creative works, including software. Pursuant to a congressionally mandated triennial rulemaking, the Librarian of Congress may grant temporary three-year exemptions from certain copyright laws to allow third parties and consumers to access, store, and share vehicle operational data.

Third-party and consumer access to vehicle data, and the ability to transmit data to motor vehicles wirelessly, have been at the center of the debate about laws enacted in Massachusetts and Maine and about a bill introduced in the 118<sup>th</sup> Congress, H.R. 906, the Right to Equitable and Professional Auto Industry Repair Act (REPAIR Act). The Massachusetts law, enacted in 2020, stipulates that beginning with model year 2022 vehicles, OEMs selling or leasing motor vehicles in Massachusetts must equip them with a standardized open data platform. The platform would enable vehicle owners and independent repair workshops to access, via a mobile application, any vehicle-specific data without obtaining prior authorization from OEMs. OEMs sued the state of Massachusetts, claiming the state law conflicts with federal laws, including copyright and vehicle safety laws. The judge presiding over the trial has not yet issued a ruling. In 2023, Maine also enacted a law with this provision, applicable to motor vehicles sold in Maine no later than January 1, 2025.

The REPAIR Act would require a manufacturer to make vehicle-generated data available to the vehicle's owner and designees through a standardized access platform. It would give the Federal Trade Commission the authority to adopt a rule that would require OEMs to provide consumers and independent workshops with data, "critical repair information," and tools needed to repair motor vehicles. In addition, it would permit the agency, in consultation with the National Highway Traffic Safety Administration to require OEMs to enable third parties to access motor vehicle data unrelated to repair and maintenance.

Groups advocating for federal or state legislation to guarantee consumers' right to repair advocate that OEMs should allow workshops and consumers to access motor vehicle telematics data. OEMs and dealership representatives contend that such laws are unnecessary and could compromise consumer safety. In addition to access, Congress may also consider the scope of such information that might be shared.

R48131

July 19, 2024

Dana A. Scherer  
Specialist in  
Telecommunications  
Policy  
dscherer@crs.loc.gov

For a copy of the full report,  
please call 7-5700 or visit  
[www.crs.gov](http://www.crs.gov).

## Contents

Introduction .....	1
Motor Vehicle and Aftermarket Industries .....	2
Vehicle Aftermarket Structure and Competition .....	4
Software-Defined Vehicles (SDVs).....	5
ADAS Costs of Repairs .....	6
Telematics .....	7
Potential Direct OEM-Consumer Relationship and Bypass of Dealers .....	8
Diagnostics, Telematics, and OEM Steering.....	8
Executive Branch Oversight of Aftermarket .....	9
Federal Trade Commission .....	10
Magnuson-Moss Warranty—Federal Trade Commission Improvement Act.....	11
White House.....	12
Copyright Laws Related to the SDV Aftermarket.....	13
The Digital Millennium Copyright Act and Section 1201 .....	14
Section 1201 Temporary Exemptions .....	15
State Laws and Reactions: 2012-2024 .....	19
2012-2014: Massachusetts Right-to-Repair Law and Industry MOU.....	19
Similarities Between 2013 Massachusetts Law and 2014 Industry MOU.....	20
Differences Between 2013 Massachusetts Law and 2014 Industry MOU.....	20
Debate Over Access to Telematics Data: 2015-2024 .....	21
2020 Massachusetts Data Access Law and Implementation.....	22
2023 Maine Vehicle Right-to-Repair Law and Proposed 2024 Amendments .....	23
2023 Update to 2014 Industry MOU .....	23
Options for Congress.....	24
Observe Impact of Industry Participants’ Private Negotiations .....	24
Permit Current Federal and State Policy Framework to Develop .....	24
Enact Federal Legislation.....	25

## Figures

Figure 1. Consumer Price Increases for Vehicles: Purchases and Aftermarket Expenses .....	3
Figure 2. Structure of Motor Vehicle Aftermarket Industry .....	4

## Contacts

Author Contact Information .....	26
----------------------------------	----

## Introduction

Between 2000 and today, an increasing number of consumer products—from watches<sup>1</sup> to cat litter boxes<sup>2</sup>—contain software and sensors to enable the products to connect to the internet and receive and transmit data. Internet-connected devices with software pose unique challenges for consumers' ability to select who maintains and repairs their products, often referred to as a *right to repair*.<sup>3</sup> The ability of repair shops that are independent of the original manufacturers to access software and data has implications for copyright, consumer protection, competition, and cybersecurity laws.<sup>4</sup>

This report focuses on the repair of motor vehicles.<sup>5</sup> As the complexity of motor vehicles has increased, conflict among manufacturers, repair service providers, and replacement part retailers regarding control over the repair process has also grown.<sup>6</sup>

A central issue of the motor vehicle debate is the extent to which third parties, such as independent repair shops, need to directly access motor vehicles' software and data in order to repair them. Vehicle manufacturers claim that providing access could harm consumers by potentially lowering the quality of repair services and increasing risks to cybersecurity and passenger safety.<sup>7</sup> Vehicle manufacturers also claim that third parties accessing vehicle software without obtaining prior authorization would violate the manufacturers' intellectual property rights.<sup>8</sup>

Executive branch agencies have also weighed in on the debate. The National Highway Traffic Safety Administration (NHTSA) stated in 2023 that it “strongly supports the right to repair” and

<sup>1</sup> “The Internet of Things (IoT) Revolution in Wearables,” *IoT Business News* (blog), November 3, 2023, <https://iotbusinessnews.com/2023/11/03/97971-the-internet-of-things-iot-revolution-in-wearables/>. See also “Major Milestones in IoT Technology History,” *IoT Business News* (blog), January 11, 2024, <https://iotmktg.com/major-milestones-iot-technology-history/>.

<sup>2</sup> Jeff Weishaupt, “10 Best Automatic Litter Boxes for Self-Cleaning in 2024 – Review & Top Pics,” *Caster*, May 3, 2024, <https://www.catster.com/lifestyle/best-automatic-cat-litter-box/>.

<sup>3</sup> *Right to repair* is a term used by various advocacy groups supporting fewer restrictions on consumers' ability to repair products they have purchased through legislative changes and other means. For one view on the term, see Irene Calboli, “The Right to Repair: Recent Developments in the USA,” *WIPO Magazine*, August 2023, [https://www.wipo.int/wipo\\_magazine\\_digital/en/2023/article\\_0023.html](https://www.wipo.int/wipo_magazine_digital/en/2023/article_0023.html).

<sup>4</sup> Christopher Boniface, Lacklan Urquhart, and Melissa Terras, “Towards the Right to Repair for the Internet of Things: A Review of Legal and Policy Aspects,” *Computer Law & Security Review*, vol. 52, no. 52 (April 2024), <https://doi.org/10.1016/j.clsr.2024.105934>.

<sup>5</sup> In the context of this report, the term *motor vehicles* refers to vehicles purchased by consumers, also known as *light-duty vehicles*, including automobiles, pickup trucks, and sport utility vehicles. David Stone and Mason Hamilton, “Crossover Utility Vehicles Blur Distinction Between Passenger Cars and Light Trucks,” *Today in Energy* (blog), U.S. Energy Information Administration, U.S. Department of Energy, May 24, 2017, <https://www.eia.gov/todayinenergy/detail.php?id=31352>.

<sup>6</sup> Robert Cunningham and Darby Hobbs, “The Evolution of the Right to Repair,” *Antitrust*, vol. 37, no. 3 (Summer 2023), p. 43.

<sup>7</sup> See generally Federal Trade Commission (FTC), *Nixing the Fix: An FTC Report to Congress on Repair Restrictions*, May 2021, pp. 24-43, [https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing\\_the\\_fix\\_report\\_final\\_5521\\_630pm-508\\_002.pdf](https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf) (reviewing the debate between manufacturers and right-to-repair advocates) (hereinafter *FTC Nixing the Fix Report*).

<sup>8</sup> Opposition Comment of the Alliance for Automotive Innovation to the U.S. Copyright Office on Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, February 20, 2024, p. 4, [https://www.copyright.gov/1201/2024/comments/opposition/Class%207%20-%20Opp'n%20-%20Alliance%20for%20Automotive%20Innovation%20\(Auto%20Innovators\).pdf](https://www.copyright.gov/1201/2024/comments/opposition/Class%207%20-%20Opp'n%20-%20Alliance%20for%20Automotive%20Innovation%20(Auto%20Innovators).pdf).

has also stressed that “whenever access to write or execute command functionality [of a motor vehicle] is contemplated, it is important to be vigilant to minimize [cybersecurity] risks.”<sup>9</sup>

The White House, several executive branch agencies, consumer advocacy groups, and repair service providers contend that manufacturers’ restrictions on accessing embedded software and/or data can lead to higher prices for consumers, shorter product life cycles, and greater environmental waste.<sup>10</sup> The North American vehicle supplier trade association MEMA<sup>11</sup> claims that “unfairly restricting access to vehicle generated data and repair and replacement components” reduces competition and increases costs.<sup>12</sup> At the same time, the Federal Trade Commission (FTC) has advised vehicle manufacturers that it will “take action to protect consumers against the illegal collection, use, and disclosure of their personal data [collected from motor vehicles].”<sup>13</sup>

As an example of the relationships between federal and state government agencies’ jurisdictions and policy considerations in the right-to-repair debate, this report discusses how the debate applies to the motor vehicle industry. This report describes technological developments in the motor vehicle industry, the post-sales segment of the motor vehicle industry (i.e., repair and maintenance parts and services), and the growing role of vehicle data within this sector. In addition, this report explains how federal competition, consumer protection, and copyright laws intersect in the right-to-repair debate more generally. This report also describes the status of laws enacted in Massachusetts and Maine aimed at facilitating the right to repair and H.R. 906, the Right to Equitable and Professional Auto Industry Repair Act (REPAIR Act). Finally, this report discusses options for Congress.

## Motor Vehicle and Aftermarket Industries

The U.S. Department of Commerce’s Bureau of Economic Analysis reports that in 2023, household purchases of motor vehicles and parts accounted for about \$768 billion, or 4.2%, of the \$18.6 trillion in total consumer expenditures.<sup>14</sup> Motor vehicles and parts were the second-largest category of durable consumer goods expenditures in 2023.<sup>15</sup> After consumers purchase motor vehicles, they also pay to maintain and repair them. The marketplace of goods and services after the initial sale of a vehicle is known as the *aftermarket*.

<sup>9</sup> Letter from Kerry Kolodziej, Assistant Chief Counsel for Litigation and Enforcement, U.S. Department of Transportation, National Highway Safety Administration, to Eric A. Haskell, Assistant Attorney General, Office of the Attorney General, Commonwealth of Massachusetts, August 22, 2023 <https://s3.documentcloud.org/documents/23925257/letter.pdf>.

<sup>10</sup> The White House, “Readout of the White House Convening on Right to Repair,” press release, December 25, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/25/readout-of-the-white-house-convening-on-right-to-repair/>.

<sup>11</sup> Prior to changing its name to “MEMA” in 2023, the association was called “the Motor and Equipment Manufacturers Association.” MEMA, “About MEMA: History,” <https://www.mema.org/about-mema/history>.

<sup>12</sup> MEMA, “Advocacy, Aftermarket Issues: Take Action, ‘Vehicle Right to Repair,’” <https://www.mema.org/advocacy/aftermarket-action-center>.

<sup>13</sup> Staff in the Office of Technology and The Division of Privacy and Identity Protection, “Cars & Consumer Data: On Unlawful Collection & Use,” *Office of Technology Blog* (blog), Federal Trade Commission, May 14, 2024, <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use>.

<sup>14</sup> St. Louis Federal Reserve, Economic Research Resources, “Table 2.4.5 Personal Consumption Expenditures by Type of Product: Annual, 2023,” <https://fred.stlouisfed.org/release/tables?rid=53&eid=44183#snid=44254> (citing data from the U.S. Bureau of Economic Analysis).

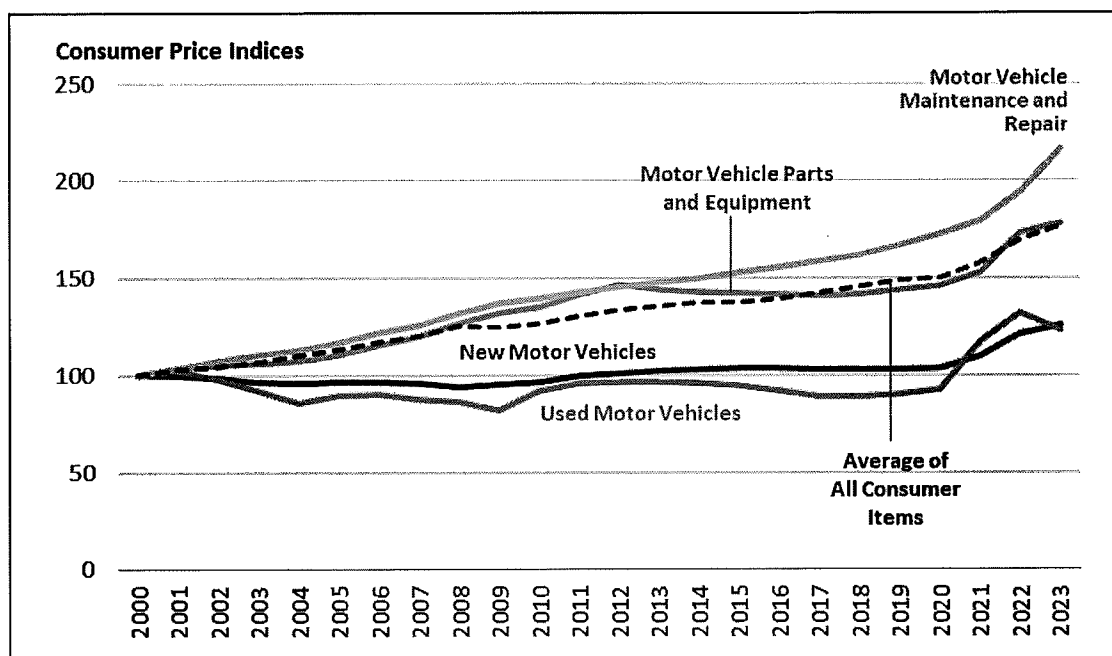
<sup>15</sup> Ibid.



As **Figure 1** indicates, between 2000 and 2023, prices increases in the motor vehicle aftermarket (i.e., parts, equipment, maintenance and repair services) were greater than price increases for new and used motor vehicles. During this period, price increases for motor vehicle maintenance and repair services were also greater than increases in the average price for all urban consumer products, a measure of inflation. Price increases for motor vehicle parts and equipment, however, generally grew at the same rate as the average price for all urban consumer products.

**Figure 1. Consumer Price Increases for Vehicles:  
Purchases and Aftermarket Expenses**

Year 2000 Consumer Price Indices = 100



**Sources:** Bureau of Labor Statistics; St. Louis Federal Reserve.

**Notes:** Consumer Price Indices for all urban consumers, annual, seasonally adjusted.

Several factors may be responsible for the increase in motor vehicle maintenance and repair service prices relative to inflation. For example, the increases may reflect the power of suppliers in a concentrated market to raise prices above a competitive rate.<sup>16</sup> Alternatively, economists have noted that a combination of COVID-19 pandemic-related economic shocks and long-term factors has restricted supply of new motor vehicles and increased demand for repairs of older motor vehicles.<sup>17</sup> The increased complexity of interconnected software and sensors in motor vehicles may have increased the costs of parts and labor needed to replace and repair them.

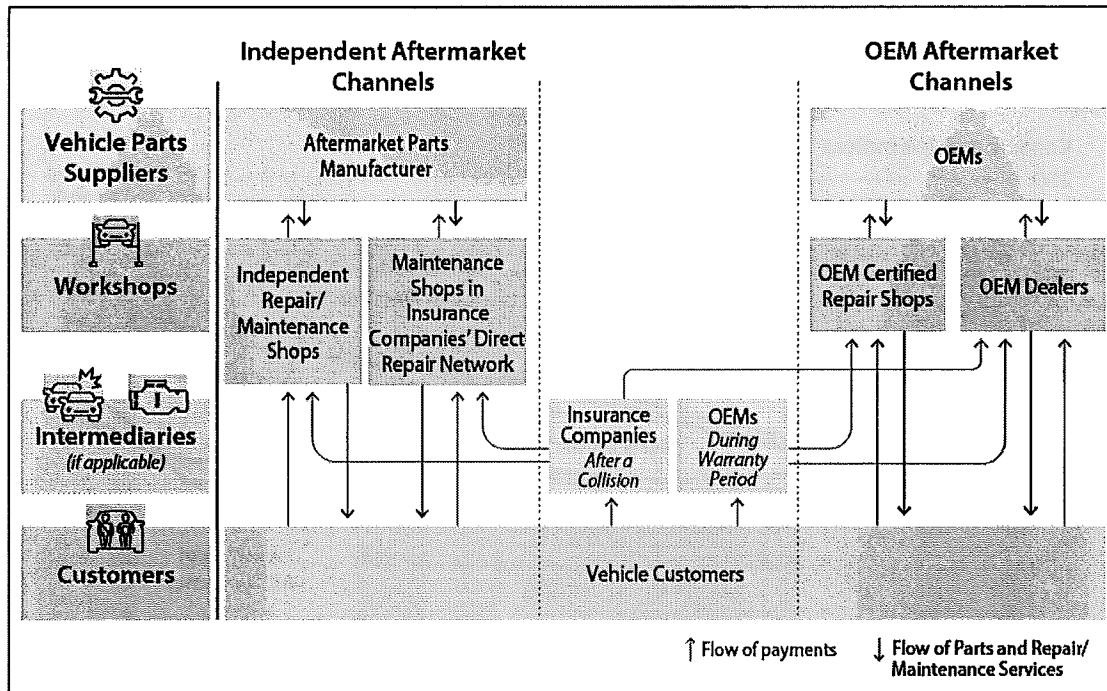
<sup>16</sup> According to a 2022 note published by staff from the Competition Division of Organisation for Economic Co-operation and Development (OECD), "ineffective competition leads to higher prices, but it does not follow that rising prices are necessarily the result of ineffective competition." Richard May, *Competition and Inflation*, OECD Competition Policy Roundtable Background Note, Competition Division, OECD, Paris, 2022, p. 9, <https://www.oecd.org/daf/competition/competition-and-inflation-2022.pdf>.

<sup>17</sup> Haley Chinander and Erik Garcia Luna, "Despite Easing Inflation, Vehicle Repair Costs Soar," The Federal Reserve Bank of Minneapolis, October 6, 2023, <https://www.minneapolisfed.org/article/2023/despite-easing-inflation-vehicle-repair-costs-soar>. The authors maintain that disruptions in motor vehicle supply chains and production during the (continued...)

## Vehicle Aftermarket Structure and Competition

As **Figure 2** illustrates, the vehicle aftermarket comprises two types of sales channels:<sup>18</sup> (1) independent channels and (2) original equipment manufacturer (OEM) channels. Each aftermarket channel contains two types of repair shops.

**Figure 2. Structure of Motor Vehicle Aftermarket Industry**



**Source:** CRS analysis of Exhibit I in Albert Waas et al., *At the Crossroads: The European Aftermarket in 2030*, Boston Consulting Group, European Association of Automotive Suppliers, Wolk After Sales Experts, Munich, March 2021, <https://web-assets.bcg.com/36/39/e80d073a4067bfe89c7482d6db69/the-european-aftermarket-in-2030.pdf>.

**Notes:** OEM = original equipment manufacturer. This figure, for the sake of clarity, excludes vehicle parts wholesalers, which act as intermediaries between vehicle parts suppliers and workshops.

Within independent channels, body/maintenance shops may be (1) independent or (2) part of an insurance company's "direct repair network." With the exception of repairing and servicing air conditioners,<sup>19</sup> federal laws do not require motor vehicle service technicians and/or mechanics to be certified. State requirements for certification vary. Some states require service technicians and/or mechanics to have professional licenses, while others require licenses for certain types of

COVID-19 pandemic led to a decrease in supply and an increase in new vehicles, which in turn prompted consumers to retain older vehicles, which require more repairs than newer vehicles, for a longer time.

<sup>18</sup> Albert Waas et al., *At the Crossroads: The European Aftermarket in 2030*, Boston Consulting Group, European Association of Automotive Suppliers, Wolk After Sales Experts, Munich, March 2021, p. 4, <https://web-assets.bcg.com/36/39/e80d073a4067bfe89c7482d6db69/the-european-aftermarket-in-2030.pdf>. See also Automotive Aftermarket Network, "Automotive Aftermarket Definition," <https://automotiveaftermarket.org/aftermarket-industry-trends/definition/>.

<sup>19</sup> 40 C.F.R. §82.34 (the Environmental Protection Agency's [EPA's] rules governing servicing of motor vehicle air conditioners).

work, such as vehicle safety inspections.<sup>20</sup> Nevertheless, employers may require service technicians/mechanics to be certified.<sup>21</sup>

Mechanics in independent shops may receive certifications from organizations unaffiliated with OEMs, including the nonprofit National Institute for Automotive Service Excellence,<sup>22</sup> Inter-Industry Conference for Auto Collision Repair,<sup>23</sup> and AAA.<sup>24</sup> When maintaining and/or repairing motor vehicles, shops within independent aftermarket channels generally use *aftermarket parts* (i.e., parts that work with multiple vehicles).

Participants in OEM channels specialize in producing/selling parts and/or repairing/servicing specific OEM makes and models. Within OEM channels, body/maintenance shops may be (1) certified by OEMs to work with the OEMs' specific motor vehicle makes and models and (2) units within dealerships franchised by the OEMs to sell and repair/service vehicles. OEM parts generally cost more than aftermarket parts.<sup>25</sup>

## Software-Defined Vehicles (SDVs)

### Software-Defined Vehicles (SDVs)

While a standard industry definition for an SDV does not exist,<sup>26</sup> for the purposes of this report, an SDV is any vehicle that "manages its operations, adds functionality, and enables new features primarily or entirely through software."<sup>27</sup> The term SDV encompasses vehicles that are self-driving (*automated vehicles*) as well as vehicles that transmit data via spectrum (*connected vehicles*).<sup>28</sup>

Software in vehicles may support any of several functions.<sup>29</sup> These functions include (1) controlling the vehicle's safety and comfort features (e.g., climate control, mirrors, and windshield wipers),<sup>30</sup> (2) transferring energy from the vehicle's engine to its wheels to make it move,<sup>31</sup> (3) informing and entertaining drivers with systems that provide such services as

<sup>20</sup> Ashley Henshaw, "Mechanic License and Insurance Requirements by State: NEXT Insurance Guide," *Auto Services and Repair* (blog), NEXT Insurance, Inc., February 14, 2022, <https://www.nextinsurance.com/blog/mechanic-license-requirements/#h-manufacturer-certification>.

<sup>21</sup> Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Outlook Handbook*, Automotive Service Technicians and Mechanics, "How to Become an Automotive Service Technician or Mechanic," <https://www.bls.gov/ooh/installation-maintenance-and-repair/automotive-service-technicians-and-mechanics.htm>.

<sup>22</sup> National Institute for Automotive Service Excellence, "About ASE," <https://www.ase.com/about-ase/>.

<sup>23</sup> Inter-Industry Conference on Auto Collision Repair, "About Us," <https://info.i-car.com/about-us>.

<sup>24</sup> AAA Club Alliance Inc., "Auto, Car Care Centers, Become an Approved Shop," <https://cluballiance.aaa.com/automotive/auto-repair-approval?pcrdl=true>.

<sup>25</sup> Dustin Hawley, "Aftermarket vs. Manufacturer Car Parts," *J.D. Power*, May 31, 2023, <https://www.jdpower.com/cars/shopping-guides/aftermarket-vs-manufacturer-car-parts>.

<sup>26</sup> Sebastian Blanco, "CES 2024: SDVs Redefine OEM and Supplier Relationships, Deliver New Features," *Automotive Engineering*, January 8, 2024, <https://www.sae.org/news/2024/01/software-defined-vehicles-ces>.

<sup>27</sup> BlackBerry Limited, "Software-Defined Vehicles," 2024, <https://blackberry.qnx.com/en/ultimate-guides/software-defined-vehicle>.

<sup>28</sup> Ibid.

<sup>29</sup> Robert N. Charette, "How Software Is Eating the Car," *IEEE Spectrum*, June 7, 2021, <https://spectrum.ieee.org/software-eating-car>.

<sup>30</sup> "What Is a Body Control Module in a Car?" *Bamboo Apps* (blog), December 28, 2022, <https://bamboapps.eu/blog/body-control-module>.

<sup>31</sup> Universal Technical Institute, "What Is a Powertrain?" *Automotive* (blog), December 8, 2021, <https://www.uti.edu/blog/automotive/powertrain>.

navigation and music streaming,<sup>32</sup> and (4) assisting drivers via a set of in-vehicle technologies (i.e., advanced driver assisted systems, or ADAS) that, among other functions, detect blind spots, automate parking, and adapt headlight beams to outside conditions.<sup>33</sup>

Many OEMs have published guidelines for repairing their vehicles. Some direct mechanics to perform diagnostic scans before and after repair work.<sup>34</sup>

### Vehicle Diagnostics

A vehicle diagnostic check involves looking over a vehicle's systems and components to help identify issues and rectify them. Although *diagnostics* can refer to the analysis of equipment in all vehicles, it generally applies to the investigation of functions and equipment (e.g., engine systems) in the electronics of SDVs.<sup>35</sup>

## ADAS Costs of Repairs

In December 2023, AAA<sup>36</sup> published a study investigating additional repair costs that drivers incurred when ADAS cameras and sensors were damaged during a minor collision. The study found that ADAS “can add up to 37.6% to the total repair cost after a collision.”<sup>37</sup> According to AAA, several variables can affect repair costs of ADAS.<sup>38</sup>

Some contend that OEMs may be limiting competition from aftermarket suppliers of ADAS parts. An insurance executive stated that OEM’s patenting and branding of ADAS sensors and cameras

<sup>32</sup> Ibid.

<sup>33</sup> BlackBerry Limited, “What Is an Advanced Driver Assistance System?” 2024, <https://blackberry.qnx.com/en/ultimate-guides/software-defined-vehicle/advanced-driver-assistance-system>. Chiradeep BasuMallick, “What Is ADAS (Advanced Driver Assistance Systems)? Meaning, Working, Types, Importance, and Applications,” *Internet of Things* (blog), Spiceworks Inc., July 15, 2022, [https://www.spiceworks.com/tech/iot/articles/what-is-adas/#\\_003](https://www.spiceworks.com/tech/iot/articles/what-is-adas/#_003). See also U.S. Department of Transportation, National Highway Traffic Safety Administration (NHTSA), “Vehicle Safety, Driver Assistance Technologies,” <https://www.nhtsa.gov/vehicle-safety/driver-assistance-technologies>.

<sup>34</sup> AAA, *Cost of Advanced Driver Assistance Systems (ADAS) Repairs*, December 2023, p. 7, [https://newsroom.aaa.com/wp-content/uploads/2023/11/Report\\_Cost-of-ADAS-Repairs-FINAL-23.pdf](https://newsroom.aaa.com/wp-content/uploads/2023/11/Report_Cost-of-ADAS-Repairs-FINAL-23.pdf). See, for example, General Motors, “Service Information – Position Statement: Pre- and Post-Scan of Collision Vehicles,” 2022, <https://www.gmparts.com/content/dam/gmparts/na/us/en/index/technical-resources/position-statements/02-pdfs/new/pre-post-scan-collision-vehicles.pdf>.

<sup>35</sup> “What Is Vehicle Diagnostics?” *John Delany Motors* (blog), February 24, 2022, <https://www.delany-motors.co.uk/blog/what-is-vehicle-diagnostics/>. Section 202(m) of the Clean Air Act (P.L. 101-549; 42 U.S.C. §7521(m)) directs the EPA to promulgate regulations requiring OEMs to install diagnostics systems on motor vehicles that would identify, alert, store, and retrieve information regarding emission-related systems deterioration or malfunction. EPA’s regulations for onboard diagnostics are at 40 C.F.R. §86.1806-05. For more information on the Clean Air Act, see CRS Report RL30853, *Clean Air Act: A Summary of the Act and Its Major Requirements*, by Richard K. Lattanzio. In its 2022 cybersecurity guidelines for OEMs, NHTSA states that “vehicle diagnostic features provide utilities to support repair and serviceability of vehicles.” NHTSA, U.S. Department of Transportation, *Cybersecurity Best Practices for the Safety of Modern Vehicles*, Updated 2022, p. 13, <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf> (hereinafter *NHTSA 2022 Cybersecurity Guidelines*).

<sup>36</sup> AAA is a membership organization representing motor vehicle drivers. AAA, “About AAA,” <https://cluballiance.aaa.com/about>. Prior to changing its name in 1997, the organization was called the “American Automobile Association.”

<sup>37</sup> Brittany Moye, “Fixing Advanced Vehicle Systems Makes Up Over One-Third of Repair Costs Following a Crash,” AAA, press release, December 14, 2023, <https://newsroom.aaa.com/2023/12/fixing-advanced-vehicle-systems-makes-up-over-one-third-of-repair-costs-following-a-crash/>.

<sup>38</sup> AAA, *Fact Sheet: Advanced Driver Assistance Systems (ADAS) Repair Costs*, December 2023, <https://newsroom.aaa.com/wp-content/uploads/2023/12/ADAS-Repair-Fact-Sheet-FINAL-12.23.pdf>.

limits competition from independent manufacturers.<sup>39</sup> In comments filed with the FTC for its *Nixing the Fix* report, LKQ Corporation, a supplier of aftermarket parts, stated that OEMs “generally enjoy exclusive supply relationships” with manufacturers of their ADAS sensors.<sup>40</sup>

## Telematics

Some industry analysts assert that the ability of OEMs to remotely diagnose and send software updates to motor vehicles via wireless internet networks may reduce maintenance costs for vehicle owners.<sup>41</sup> At the same time, the ability to transmit and receive vehicle data presents opportunities for OEMs to generate post-sales revenue via subscription services.<sup>42</sup> As discussed in the rest of this report, much of the vehicle right-to-repair debate hinges on issues of third-party access to vehicle software and data.

### Telematics

The word *telematics* is a portmanteau of “telecommunications” and “informatics.”<sup>43</sup> The term *informatics* refers to the use of computers to gather and analyze data and manage real-world systems. The field of vehicle telematics includes wireless safety communications, Global Positioning System (GPS) navigation, integrated hands-free mobile devices, and ADAS.<sup>44</sup> OEM telematics systems are closed networks that require two-way communications between the vehicle and an OEM data center.<sup>45</sup>

In 2012, Tesla became the first vehicle OEM to deliver software updates via wireless internet networks.<sup>46</sup> By 2022, several other OEMs reportedly had followed suit, offering updates for information and entertainment systems, navigation systems, and telematics platforms.<sup>47</sup>

Beginning in 2014, pursuant to a memorandum of understanding (MOU) between various national motor vehicle industry groups (hereinafter “2014 Industry MOU”), OEMs must provide independent workshops with the same “telematics diagnostic and repair information that [OEMs provide] to dealers, necessary to diagnose and repair a customer’s vehicle, and not otherwise available to an independent repair facility via the tools specified [in an earlier section of the MOU].”

<sup>39</sup> Lurah Lowery, “The Reasons Behind Soaring Repair Prices: OEM Materials, Technicians, Vehicle Types & More,” *Repairer Driven News*, September 13, 2022, <https://www.repairerdrivennews.com/2022/09/13/the-reasons-behind-soaring-repair-prices-oem-materials-technicians-vehicle-types-more/>.

<sup>40</sup> Comments of MEMA, the Vehicle Suppliers Association, to the U.S. Federal Trade Commission in response to a call for research and data related to repair restrictions; Exhibit 1, Research Submitted by Josh Meyer, Vice President, Strategy & Innovation, LKQ Corporation, April 30, 2019, <https://www.copyright.gov/1201/2024/comments/Class%207%20-%20Initial%20Comments%20-%20MEMA.pdf>.

<sup>41</sup> Mike Colias, “Detroit Downloads Tesla’s Software Strategy,” *Wall Street Journal*, March 20, 2019, <https://www.wsj.com/articles/auto-makers-steer-in-teslas-direction-on-wireless-updates-11553083202>.

<sup>42</sup> Sean Trucker, “GM to Add 50 Subscription Services by 2026,” *Kelly Blue Book*, February 25, 2022, <https://www.kbb.com/car-news/gm-to-add-50-subscription-services-by-2026/>.

<sup>43</sup> NHTSA defines *telematics* as “the integration of telecommunications and informatics for intelligent applications in vehicles, such as fleet management” (*NHTSA 2022 Cybersecurity Guidelines*, p. 19).

<sup>44</sup> Geotab Team, “What Is Telematics?” *Geotab Inc.* (blog), April 11, 2024, <https://www.geotab.com/blog/what-is-telematics/>.

<sup>45</sup> Charlie Gorman, “Diagnostic Telematics and the Aftermarket: What Does the Aftermarket Actually Need in Order to Make This Work?” *Equipment and Tool Institute* (blog), <https://etools.org/telematics/>.

<sup>46</sup> Damon Lavrinc, “In Automotive First, Tesla Pushes Over-the-Air Software Patch,” *Wired*, September 24, 2012, <https://www.wired.com/2012/09/tesla-over-the-air/>.

<sup>47</sup> Admin, “Over-the-Air (OTA): A Differentiator for Software-Defined-Vehicles,” *Telematics Wire*, July 21, 2022, <https://www.telematicswire.net/over-the-air-ota-a-differentiator-for-software-defined-vehicles/>.

The 2014 Industry MOU does not, however, apply to “telematics services or any other remote or information service, diagnostic or otherwise, delivered to or derived from the vehicle by mobile communications.”<sup>48</sup>

The extent to which, if at all, independent workshops’ ability to access telematics and diagnostic data remotely, without seeking prior permission from or paying OEMs—including data unrelated to the repair and maintenance of vehicles—preserves competition in the motor vehicle aftermarket is at the heart of several policy debates described in this report.

## Potential Direct OEM-Consumer Relationship and Bypass of Dealers

ABI Research estimates that as of 2023, in-person software updates cost OEMs \$500 million per year.<sup>49</sup> OEMs pay for aftermarket services during the lifetime of a vehicle’s warranty.<sup>50</sup> When consumers visit workshops and dealers to service their vehicles, the workshops and dealers receive payments from the OEMs.<sup>51</sup> Automotive software company Modera stated that

[as OEMs] increasingly take ownership of customer relationships, which [had] belonged to dealerships ... [i]n this connected, direct-to-consumer landscape, the high margins of the servicing revenue stream from dealerships could be well eroded. Both OEMs and dealerships have to go over their revenue models and relationships with a [fine-tooth comb] for survival.<sup>52</sup>

In 2022, the National Automobile Dealers Association (NADA), the trade association representing OEM dealers, released its *Guiding Principles on Evolving Business Models and the Dealer Franchise System*.<sup>53</sup> Among other positions, NADA states that it supports OEMs’ free provision of wireless software updates related to repairs, safety and emission recalls, and vehicle performance improvements. NADA opposes OEMs’ use of telematics to bypass dealer revenue-sharing by selling additional features directly to consumers.<sup>54</sup>

## Diagnostics, Telematics, and OEM Steering

In the context of the right-to-repair debate, some industry participants contend that telematics enable OEMs to steer consumers to workshops within the OEM aftermarket channel.

<sup>48</sup> Memorandum of Understanding Among Automotive Aftermarket Industry Association, Coalition for Auto Repair Equality, Alliance of Automobile Manufacturers, and Association of Global Automakers, January 15, 2014, §(2)(e), <http://www.njgca.org/wp-content/uploads/Right-to-Repair-national-MOU-01-23-14.pdf> (hereinafter 2014 Industry MOU). For more information about events predating the 2014 Industry MOU, see “2012-2014: Massachusetts Right-to-Repair Law and Industry MOU.”

<sup>49</sup> Lurah Lowery, “OEM Shift to OTA Recall Fixes Predicted to Occur by 2028,” *Repairer Driven News*, May 9, 2023, <https://www.repairerdrivennews.com/2023/05/09/oem-shift-to-ota-recall-fixes-predicted-to-occur-by-2028/>.

<sup>50</sup> “What Will the Future Hold for OEM Dealerships,” *Modera* (blog), December 29, 2021, <https://modera.com/automotive/what-will-the-future-hold-for-oem-dealerships/>.

<sup>51</sup> Some states, including Illinois, Wisconsin, and Montana, have changed franchise laws to increase the rates OEMs pay for work done during the vehicle’s warranty. Larry P. Vellequette, “Billions at Stake as Dealers Ask State Lawmakers to Get Paid More for Warranty Work,” *Automotive News*, February 24, 2023, <https://www.autonews.com/dealers/warranty-reimbursement-rates-car-dealers-battle-automakers>.

<sup>52</sup> *Ibid.*

<sup>53</sup> National Automobile Dealers Association, *NADA Guiding Principles on Evolving Business Models and the Dealer Franchise System*, 2022, <https://www.nada.org/media/6439/download?inline>.

<sup>54</sup> *Ibid.*, p. 2.

Disagreement exists about whether access to real-time, remote access to vehicle data at zero or low cost affects aftermarket competition.<sup>55</sup>

Allstate Insurance Company's Senior Vice President, Claims Design and Delivery, Donald Jones, has stated that "it is increasingly difficult for independent workshops to service newer, more technologically advanced cars without the same wireless access to car data that dealers have."<sup>56</sup> In April 2024, according to a survey of independent workshops nationwide that was commissioned by the Auto Care Association, 51% of respondents reported sending as many as five vehicles per month to an OEM dealer for repairs because of limits on their ability to access vehicle data.<sup>5758</sup>

However, the Alliance for Automotive Innovation (Auto Innovators)—a group representing OEMs and equipment manufacturers and suppliers—contends that

automakers already make available to independent repair businesses all the information needed to diagnose and repair a vehicle via [a] 2014 nationwide agreement guaranteeing repairers and vehicle owners access to the same repair and diagnostic information provided to auto dealers.<sup>59</sup>

In a July 2023 letter to congressional committee leaders, three trade organizations—the Society of Collision Repair Specialists (SCRS), the Automotive Service Association (ASA), and Auto Innovators—stated that

70 percent of post-warranty vehicle repairs today happen outside the dealer network, while automakers' own certified collision networks are comprised of shops that are more than 70 percent non-dealer owned. In other words, competition is alive and well in the auto repair industry.<sup>60</sup>

The organizations do not specify what percentage of post-warranty vehicle repairs are made by shops that are not OEM certified.

## Executive Branch Oversight of Aftermarket

The authority of various federal agencies to regulate the activities of the motor vehicle industry—each with a different policy objective—further impacts the right-to-repair debate.

<sup>55</sup> Aarian Marshall, "Automakers Say They Resolved the Right-to-Repair Fight. Critics Aren't Ready to Make Peace," *Wired*, July 17, 2023, <https://www.wired.com/story/automakers-say-they-resolved-the-right-to-repair-fight/>.

<sup>56</sup> The White House, "White House Convening on Right to Repair," YouTube, October 24, 2023, <https://www.youtube.com/watch?v=Ug3DkX7VRy8> (beginning at 45:00).

<sup>57</sup> Auto Care Association, "Survey: 84% of Vehicle Repair Shops View Vehicle Data Access as Top Issue in Their Business," press release, April 10, 2024, <https://www.autocare.org/news/latest-news/details/2024/04/10/survey-84-of-independent-repair-shops-view-vehicle-data-access-as-top-issue-for-their-business>.

<sup>58</sup> National Automobile Dealers Association, *NADA Guiding Principles on Evolving Business Models and the Dealer Franchise System* (2022), pp. 2-3, <https://www.nada.org/media/6439/download?inline>.

<sup>59</sup> Letter from John Bozzella, President and CEO, Alliance for Automotive Innovation, to The Honorable Aaron Frey, Maine Attorney General, April 27, 2023, <https://www.autosinnovate.org/posts/communications/Maine%20AG%20Letter%20R2R%20with%20Attachment-combined.pdf>. The Alliance for Automotive Innovation sent a letter to 20 state attorneys general discussing federal right-to-repair legislation in April 2023. See also Alliance for Automotive Innovation, "Right to Repair," <https://www.autosinnovate.org/RightToRepair>.

<sup>60</sup> Letter from John Bozzella, President and CEO, Alliance for Automotive Innovation; Julie Massaro, President, Automotive Service Association; and Aaron Schulenburg, Executive Director, Society of Collision Repair Specialists to The Honorable Maria Cantwell, Chairwoman, U.S. Senate Committee on Commerce, Science, and Transportation et al., July 11, 2023, <https://www.autosinnovate.org/posts/letters/1-%20Letter%20to%20Congress%20Automotive%20Repair%20Data%20Sharing%20Commitment%20July%202023.pdf>.

Federal regulations related to the motor vehicle industry cover safety, fuel, and emissions.<sup>61</sup> The National Highway Traffic and Safety Administration (NHTSA), an agency within the Department of Transportation, oversees vehicle safety<sup>62</sup> and issues the Corporate Average Fuel Economy (CAFE) standards.<sup>63</sup> The Environmental Protection Agency (EPA) regulates vehicle emissions.<sup>64</sup>

In addition, the U.S. Department of Commerce's Bureau of Industry and Security regulates the export of goods and technologies for national security and foreign policy purposes.<sup>65</sup> In March 2024, BIS issued an advance notice of proposed rulemaking (NPRM) seeking, among other things, comment on national security risks associated with connected vehicles.<sup>66</sup>

With respect to the motor vehicle aftermarket, antitrust, competition, and consumer protection laws govern the conduct of industry participants. The antitrust laws are the Sherman Act, enacted in 1890, and the Clayton Antitrust Act of 1914.<sup>67</sup> While both the U.S. Department of Justice (DOJ) and the FTC enforce antitrust laws, this report primarily focuses on the FTC's role and authority.

## Federal Trade Commission

The Federal Trade Commission Act of 1914, as amended (FTC Act), sets forth the agency's dual mission of protecting consumers and promoting competition.<sup>68</sup> Section 5(a)(1) prohibits "unfair methods of competition" and "unfair or deceptive acts or practices" (UDAP).<sup>69</sup> Specifically, the "unfair methods of competition" standard prohibits conduct that violates the Sherman and Clayton Acts, as well as conduct that does not meet the technical requirements of those statutes.<sup>70</sup>

In exercising its UDAP authority, the FTC cannot declare an act or practice unlawful on the grounds that it is "unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."<sup>71</sup> The FTC defines "deceptive" practices as those "involving a material representation, omission or practice that is likely to mislead a

<sup>61</sup> Library of Congress, "Industry Regulations," in "Automotive Industry: A Research Guide," <https://guides.loc.gov/automotive-industry/regulations>.

<sup>62</sup> U.S. Department of Transportation, NHTSA, "Laws and Equipment," <https://www.nhtsa.gov/laws-regulations>.

<sup>63</sup> For more on NHTSA's CAFE standards and EPA regulations, see CRS In Focus IF12433, *Automobiles, Air Pollution, and Climate Change*, by Richard K. Lattanzio.

<sup>64</sup> EPA, "Regulations for Emissions from Vehicles and Engines," <https://www.epa.gov/regulations-emissions-vehicles-and-engines>.

<sup>65</sup> U.S. Department of Commerce, Bureau of Industry and Security, "About Export Administration Regulations (EAR)," <https://www.bis.gov/regulations>.

<sup>66</sup> U.S. Department of Commerce, Bureau of Industry and Security, "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles," 89 *Federal Register* 15066, March 1, 2024.

<sup>67</sup> For additional background information about antitrust laws, see CRS In Focus IF11234, *Antitrust Law: An Introduction*, by Jay B. Sykes.

<sup>68</sup> 15 U.S.C. §§41-58, as amended. For additional information about the FTC, see CRS Legal Sidebar LSB10388, *Will the FTC Need to Rethink Its Enforcement Playbook (Part II)? Circuit Split Casts Doubt on the FTC's Ability to Seek Restitution in Section 13(b) Suits*, by Chris D. Linebaugh.

<sup>69</sup> 15 U.S.C. §45(a)(1).

<sup>70</sup> *FTC Nixing the Fix Report*, p. 11.

<sup>71</sup> 15 U.S.C. §45(n).



consumer acting reasonably in the circumstances.”<sup>72</sup> Such deceptive practices may include sharing of vehicle data with third parties without obtaining consumers’ prior consent.<sup>73</sup>

In addition to initiating enforcement actions against individual companies to determine whether practices are unfair or deceptive, the FTC may proactively use trade regulation rules to address common UDAPs.<sup>74</sup> Section 18(a)(1)(B) of the FTC Act (15 U.S.C. §57a(1)(B)) authorizes the FTC to prescribe “rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce (within the meaning of section 5(a)(1) of [the FTC Act; 15 U.S.C. §45(a)(1)]).”<sup>75</sup> The FTC must have reason to believe that the practices to be addressed by the rulemaking are “prevalent” (15 U.S.C. §57a(b)(3)) before initiating a proceeding.<sup>76</sup>

### Magnuson-Moss Warranty—Federal Trade Commission Improvement Act

The FTC also enforces certain consumer protection statutes that prohibit specific practices. These statutes generally specify that violations are to be treated as if they were UDAP under Section 5(a) of the FTC Act and as violations of trade regulation rules issued under Section 18 of the FTC Act.<sup>77</sup> Retail consumers’ rights with respect to products they purchase are covered by the Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, as amended<sup>78</sup> (or “MMWA”), which Congress enacted in 1975. Section 102(c) of the MMWA prohibits a warrantor of a consumer product from conditioning its warranty on the consumer using any article or service that is identified by brand name unless the article or service is provided for free or the warrantor obtains a waiver from the FTC (the “tying prohibition”).<sup>79</sup>

In May 2021, the FTC, at the direction of Congress,<sup>80</sup> published a report on industry practices in several aftermarkets, including the motor vehicle aftermarket.<sup>81</sup> The FTC found that based on information the agency gathered to prepare the report, “it is clear that repair restrictions have

<sup>72</sup> FTC, “About the FTC: Enforcement Authority: A Brief Overview of the Federal Trade Commission’s Investigative, Law Enforcement, and Rulemaking Authority,” <https://www.ftc.gov/about-ftc/mission/enforcement-authority> (hereinafter FTC Enforcement Authority Overview), citing FTC, “FTC Policy Statement on Deception,” October 14, 1983, [https://www.ftc.gov/system/files/documents/public\\_statements/410531/831014deceptionstmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf).

<sup>73</sup> Staff in the Office of Technology and The Division of Privacy and Identity Protection, “Cars & Consumer Data: On Unlawful Collection & Use,” *Office of Technology Blog* (blog), Federal Trade Commission, May 14, 2024, <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use>.

<sup>74</sup> FTC Enforcement Authority Overview.

<sup>75</sup> Ibid.

<sup>76</sup> In addition, during rulemaking proceedings, the FTC must provide interested parties with limited rights of cross-examination during informal hearings.

<sup>77</sup> The FTC has enforcement or administrative responsibilities under more than 80 laws. FTC, “Legal Library: Statutes,” <https://www.ftc.gov/legal-library/browse/statutes>.

<sup>78</sup> P.L. 93-637 (15 U.S.C. §§2301-2312).

<sup>79</sup> MMWA §102(c) (15 U.S.C. §2302(c)). See also Comment of United States Department of Justice and Federal Trade Commission to the U.S. Copyright Office on Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, March 14, 2023, p. 5, <https://www.copyright.gov/1201/2024/comments/reply/Class%205%20&%207%20-%20Reply%20-%20Department%20of%20Justice%20Antitrust%20Division%20and%20Federal%20Trade%20Commission.pdf> (hereinafter DOJ-FTC March 2023 Comment).

<sup>80</sup> U.S. Congress, House Committee on Appropriations, Financial Services and General Government Appropriations Bill, 2021, report to accompany H.R. 7668, 116<sup>th</sup> Cong., 2<sup>nd</sup> sess., July 17, 2020, H.Rept. 116-456 (Washington: GPO, 2020), p. 67. The report stated, “Not later than 120 days after the enactment of this Act, the FTC is directed to provide to the Committee, and to publish online, a report on anticompetitive practices related to repair markets. The report shall provide recommendations on how to best address these problems.”

<sup>81</sup> *FTC Nixing the Fix Report*.

diluted the effectiveness of Section 102(c) [of the MMWA] and steered consumers into manufacturers' repair [channels] or to replace products before the end of their useful lives."<sup>82</sup> Nonetheless, the FTC, citing the 2014 Industry MOU found that "the car manufacturing industry has taken important steps to expand consumer choice."<sup>83</sup>

In July 2021, the FTC announced that it would devote more enforcement resources to combating unlawful practices related to repair restrictions.<sup>84</sup> While noting that "current law does not provide for civil penalties or redress,"<sup>85</sup> the FTC stated that, among other actions, it would consider filing suit against violators of the MMWA to seek appropriate injunctive relief (i.e., a court restraint on a violator's illegal behavior). In addition, the FTC stated that it would scrutinize repair restrictions for potential violations of antitrust laws and assess whether those restrictions constitute unfair acts or practices.<sup>86</sup>

In October 2022, after a public comment period, the FTC approved a final order against motorcycle manufacturer Harley-Davidson Motor Company Group, alleging that the company violated the MMWA by illegally restricting consumers' right to repair their vehicles.<sup>87</sup> Specifically, the FTC found that Harley Davidson had violated (1) the MMWA's tying prohibition, (2) the FTC Act's prohibition of deceptive conduct, and (3) the FTC's rule requiring OEMs to disclose all warranty terms in a single document.<sup>88</sup> The order requires Harley-Davidson to take multiple steps, including adding specific language to their warranties alerting consumers that using aftermarket parts or an independent workshop will not violate the company's warranty.<sup>89</sup>

In April 2024, the FTC announced that it had created a form for consumers to report their warranty or repair stories related to "a wide range of products."<sup>90</sup>

## White House

In July 2021, President Joe Biden issued Executive Order 14306 called "Promoting Competition in the American Economy."<sup>91</sup> Among other actions, the executive order stated "the Chair of the FTC, in the Chair's discretion, is also encouraged to consider working with the rest of the Commission to exercise the FTC's statutory rulemaking authority, as appropriate and consistent

<sup>82</sup> *FTC Nixing the Fix Report*, p. 6.

<sup>83</sup> *Ibid.*, pp. 6, 45-47.

<sup>84</sup> FTC, *Policy Statement of the Federal Trade Commission on Repair Restrictions Imposed by Manufacturers and Sellers, Matter Number P194400*, July 21, 2021, [https://www.ftc.gov/system/files/documents/public\\_statements/1592330/p194400repairrestrictionspolicystatement.pdf](https://www.ftc.gov/system/files/documents/public_statements/1592330/p194400repairrestrictionspolicystatement.pdf).

<sup>85</sup> *Ibid.*

<sup>86</sup> *Ibid.*, p. 2.

<sup>87</sup> FTC, "FTC Approves Final Orders in Right-to-Repair Cases Against Harley-Davidson, MWE Investments, and Weber," press release, October 27, 2022, <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-approves-final-orders-right-repair-cases-against-harley-davidson-mwe-investments-weber> (hereinafter 2022 FTC press release). See also FTC, "In the Matter of Harley-Davidson Motor Company, Group, LLC, a Limited Liability Company, Complaint, 2123140," October 21, 2022, [https://www.ftc.gov/system/files/ftc\\_gov/pdf/2123140-Harley-Davidson-combined-package-without-signatures.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/2123140-Harley-Davidson-combined-package-without-signatures.pdf) (hereinafter 2022 FTC Complaint.)

<sup>88</sup> 2022 FTC Complaint, pp. 3-4.

<sup>89</sup> 2022 FTC press release.

<sup>90</sup> Lesley Fair, "FTC Wants Your Repair Stories," *FTC* (blog), April 4, 2024, <https://consumer.ftc.gov/consumer-alerts/2024/04/ftc-wants-your-repair-stories>.

<sup>91</sup> Executive Order 14306, "Promoting Competition in the American Economy," 86 *Federal Register* 36987, July 14, 2021.

with applicable law, in areas such as ... unfair anticompetitive restrictions on third-party repair or self-repair of items.”<sup>92</sup>

In October 2023, the White House convened a roundtable discussion with federal and state officials, small business owners, and private-sector officials to discuss “the importance of the right to repair.”<sup>93</sup> Several participants called on Congress to enact federal right-to-repair legislation.<sup>94</sup>

## Copyright Laws Related to the SDV Aftermarket

Copyright law may restrict a user’s ability to access or alter the software within SDVs. Copyright grants certain exclusive legal rights to authors of original creative works.<sup>95</sup> At least since 1980,<sup>96</sup> U.S. copyright law has protected computer programs as a type of literary work.<sup>97</sup> Thus, software developers may claim copyright in the code they write, just as writers may claim copyright in the books they author.<sup>98</sup> Copyright protection means that, generally speaking, authors of computer programs have the exclusive right to make copies of, or changes to, their code.<sup>99</sup> Third parties who reproduce, distribute, or adapt a copyrighted work without the copyright owner’s permission are said to infringe the copyright and may be sued in court by the copyright holder for monetary damages or other legal remedies.<sup>100</sup>

<sup>92</sup> Ibid., p. 36992. The 2021 executive order specified one example of a practice it encouraged the FTC to investigate: “restrictions imposed by powerful manufacturers that prevent farmers from repairing their own equipment.” For more information on such issues in the agriculture sector, see Emily Stone, “Update on Right to Repair,” *The Ag and Food Law Update* (blog), The National Agriculture Law Center, November 7, 2023, <https://nationalaglawcenter.org/update-on-right-to-repair/>.

<sup>93</sup> The White House, “Readout of the White House Convening on Right to Repair,” press release, October 25, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/25/readout-of-the-white-house-convening-on-right-to-repair/>.

<sup>94</sup> The White House, “White House Convening on Right to Repair,” YouTube, October 24, 2023, <https://www.youtube.com/watch?v=Ug3DkX7VRy8>.

<sup>95</sup> 17 U.S.C. §102(a). See also Library of Congress, U.S. Copyright Office, “Help: Types of Work,” <https://www.copyright.gov/eco/help-type.html>.

<sup>96</sup> In 1974, because of uncertainty about whether copyright protection was available to computer programs under existing law, Congress created the National Commission on New Technological Uses of Copyrighted Works (known as CONTU) to study the issue and make recommendations. United States, “Final Report of the National Commission on New Technological Uses of Copyrighted Works,” July 31, 1978, pp. 3-9. CONTU recommended that Congress amend the Copyright Act “to make it explicit that computer programs, to the extent that they embody an author’s original creation, are proper subject matter of copyright” (p. 1). In 1980, Congress adopted CONTU’s recommendations. P.L. 96-517 §10, 94 Stat. 3015, 3028 (1980).

<sup>97</sup> 17 U.S.C. §101 (defining *computer program* and *literary work*); 17 U.S.C. §§102(a) and 102(a)(1) (“Copyright protection subsists ... in original works of authorship fixed in any tangible medium of expression [including] literary work[s].”).

<sup>98</sup> 17 U.S.C. §§101-102, 106. The scope of copyright may vary given the nature of the work; the “fact that computer programs are primarily functional” affects the application of copyright doctrines such as fair use (*Google v. Oracle*, 141 S. Ct. 1183, 1208 (2021)).

<sup>99</sup> 17 U.S.C. §106(1)-(2) (exclusive rights to reproduce copyrighted works and make derivative works of them). These exclusive rights are subject to a number of defenses and limitations, including the fair use doctrine (17 U.S.C. §§107-122).

<sup>100</sup> 17 U.S.C. §§501-505.

In addition to being a copyrighted work, computer code may be used to protect other copyrighted works. Owners of copyrighted content have sometimes used digital safeguards—known as *technological protection measures* (TPMs)—to prevent access to or uses of copyrighted works.<sup>101</sup>

## The Digital Millennium Copyright Act and Section 1201

In 1998, Congress enacted Section 1201 of the Copyright Act of 1976, as amended (17 U.S.C. §1201), as part of the Digital Millennium Copyright Act (DMCA).<sup>102</sup> Since 1998, the variety of products that incorporate software—including motor vehicles—has proliferated. Because computer code is a copyrightable work,<sup>103</sup> Section 1201 and other copyright laws generally prohibit persons from accessing vehicle software without first obtaining permission from OEMs.

In explaining how the internet prompted its consideration of copyright laws amendments, the House Committee on the Judiciary stated,

The digital environment now allows users of electronic media to send and retrieve perfect reproductions of copyrighted material easily and nearly instantaneously, to or from locations around the world. With this evolution in technology, the law must adapt in order to make digital networks [i.e., the internet] safe places to disseminate and exploit copyrighted works.<sup>104</sup>

To enable copyright owners to protect their works, Section 1201 prohibits actions relating to two types of TPMs: “access controls” and “copy controls.”<sup>105</sup> *Access controls* are technologies that limit the ability of users to access a copyrighted work, such as encryption on Blu-ray disks or authentication codes needed to play a video game or use licensed software.<sup>106</sup> Section 1201(a)(1), sometimes referred to as the “anti-circumvention prohibition,” prohibits users from

<sup>101</sup> For example, copyright owners may use TPMs to limit the number of devices that consumers can use to access media they have purchased. See the section “Sound Recording Reproduction and Distribution Licenses” in CRS Report R43984, *Money for Something: Music Licensing in the 21st Century*, by Dana A. Scherer. (“In the case of electronic reproductions of songs, record labels initially conditioned their sale of songs to iTunes on Apple’s incorporation of digital rights management software.”)

<sup>102</sup> P.L. 105-304 §§103, 112 Stat. 2860, 2863-2876 (1998).

<sup>103</sup> 17 U.S.C. §101 (definition of *computer program*).

<sup>104</sup> U.S. Congress, House Committee on the Judiciary, *WIPO Copyright Treaties Implementation and Online Copyright Infringement Liability Limitation*, Report to Accompany H.R. 2281, 105<sup>th</sup> Cong., 2<sup>nd</sup> sess., May 22, 1998, H.Rept. 105-551, Part 1 (Washington: GPO, 1998), p. 9. The report also stated, “While there are no objections to preventing piracy on the Internet, it is not easy to draw a line between legitimate and non-legitimate uses of decoding devices. ... The bill, as reported, presents a reasonable compromise” (Ibid., p. 10). See also U.S. Congress, Senate Committee on the Judiciary, *The Digital Millennium Copyright Act of 1998*, report to accompany S. 2037, 105<sup>th</sup> Cong., 2<sup>nd</sup> sess., May 11, 1998, S.Rept. 105-190 (Washington: GPO, 1998), which states “Title I of this bill [creating Section 1201] ... will make available via the Internet the movies, music, software, and literary works that are the fruit of American creative genius” (p. 2).

<sup>105</sup> Karyn Temple Claggett, *Section 1201 of Title 17*, U.S. Copyright Office, Library of Congress, June 2017, p. 2, <https://www.copyright.gov/policy/1201/section-1201-full-report.pdf> (hereinafter *U.S. Copyright Office Section 1201 Report*).

<sup>106</sup> Ibid.; 17 U.S.C. §1201(a)(3)(A)-(B).

circumventing access controls.<sup>107</sup> Section 1201(a)(2) proscribes the manufacturing or trafficking of technologies and devices primarily designed to circumvent access controls.<sup>108</sup>

*Copy controls* are technologies that protect the exclusive rights of the copyright holder after access to the work is obtained, such as by limiting the number of copies a user is able to make of a digital song or e-book they purchased.<sup>109</sup> Section 1201(b)(1) prohibits manufacturing or trafficking of technologies and devices primarily designed to circumvent copy controls.<sup>110</sup> Section 1201 does not prohibit the circumvention of copy controls. However, reproducing a copyrighted work without authorization after circumventing copy controls may violate the copyright owner's exclusive rights under other provisions of the Copyright Act.<sup>111</sup> Copyright holders may sue in federal court for injunctive relief and money damages for violations of Section 1201.<sup>112</sup> They may seek either actual damages or statutory damages ranging from \$200 to \$7,500 per act of circumvention.<sup>113</sup> Criminal remedies are available when people violate Section 1201 "willfully and for purposes of commercial advantage or private financial gain."<sup>114</sup>

## Section 1201 Temporary Exemptions

Section 1201 empowers the Librarian of Congress to make temporary regulatory exceptions to the anti-circumvention prohibition, Section 1201(a)(1), for particular classes and uses of copyrighted works.<sup>115</sup> The Librarian does not have comparable regulatory authority regarding Section 1201's prohibitions on the manufacturing or trafficking of circumvention devices.<sup>116</sup> The Librarian makes these exceptions subsequent to a determination that particular users are "adversely affected by [the anti-circumvention prohibition] in their ability to make non-infringing uses."<sup>117</sup> After examining several statutory factors, the Librarian bases such determinations on the recommendation of the Register of Copyrights. To make these recommendations, the Register conducts a public rulemaking proceeding every three years<sup>118</sup> and consults the head of the U.S.

<sup>107</sup> 17 U.S.C. §1201(a)(1). To *circumvent* means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner" (17 U.S.C. §1201(a)(3)(A)). An *access control* is defined as a technological measure that "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work" (17 U.S.C. §1201(a)(3)(B)).

<sup>108</sup> 17 U.S.C. §1201(a)(2)(A). A technology may also not be manufactured or trafficked if it "has only limited commercially significant purpose or use other than to circumvent [access controls]" or is marketed with knowledge of its use for circumventing access controls (17 U.S.C. §1201(a)(2)(B)-(C)).

<sup>109</sup> U.S. Copyright Office Section 1201 Report, p. 2; 17 U.S.C. §1201(b)(2).

<sup>110</sup> 17 U.S.C. §1201(b)(1)(A). A technology may also not be manufactured or trafficked if it "has only limited commercially significant purpose or use other than to circumvent [copy controls]" or is marketed with knowledge of its use for circumventing copy controls (17 U.S.C. §1201(a)(2)(B)-(C)).

<sup>111</sup> 17 U.S.C. §106(1).

<sup>112</sup> 17 U.S.C. §1203(a)-(b).

<sup>113</sup> 17 U.S.C. §1203(c).

<sup>114</sup> 17 U.S.C. §1204(a). The criminal penalties include fines of up to \$500,000 and a maximum of five years' imprisonment for a first offense. Nonprofit libraries, archives, educational institutions, or public broadcasting entities are excluded from possible criminal liability (17 U.S.C. §1204(a)-(b)).

<sup>115</sup> 17 U.S.C. §1201(a)(1)(B)-(E).

<sup>116</sup> U.S. Copyright Office Section 1201 Report, p. 21.

<sup>117</sup> 17 U.S.C. §1201(a)(1)(C).

<sup>118</sup> 17 U.S.C. §1201(a)(1)(C); U.S. Copyright Office Section 1201 Report, pp. 20-21.

Department of Commerce's National Telecommunications and Information Administration (NTIA).<sup>119</sup> The exemptions currently in effect expire on October 27, 2024.<sup>120</sup>

The Copyright Office reviews previously granted exemptions without meaningful opposition via a streamlined process.<sup>121</sup> It reviews previously granted exemptions with meaningful opposition as well as petitions for new exemptions via a comprehensive review process.<sup>122</sup> In June 2023, the Copyright Office initiated the ninth triennial rulemaking proceeding, for exemptions to become effective from October 2024 to October 2027.<sup>123</sup>

Pursuant to an exemption approved by the Librarian in 2018 and 2021, a person may circumvent access controls on computer programs when doing so is a necessary step for diagnosing, maintaining, or repairing a motorized land vehicle, such as a personal automobile or commercial vehicle.<sup>124</sup> As part of its NPRM for the ninth triennial review, the Copyright Office notified the public, pursuant to the streamlined review process, that the Register intends to recommend that the Librarian of Congress renew this exemption for the 2024-2027 period.<sup>125</sup>

In August 2023, MEMA petitioned the Copyright Office to consider a new exemption for circumvention of TPMs

on computer programs that are contained in and control the functioning of a lawfully acquired motorized land vehicle ... such as a personal automobile ... to allow lawful vehicle owners and lessees, or those acting on their behalf, to access, store, and share vehicle operational data, including diagnostic and telematics data.<sup>126</sup>

In its NPRM, the Copyright Office requested comments on including an exemption for the class of works it describes as "Proposed Class 7: Computer Programs – Vehicle Operational Data."<sup>127</sup>

<sup>119</sup> 17 U.S.C. §1201 (a)(1)(C). The statute references the Department of Commerce's Assistant Secretary for Communications and Information, who is the head of the National Telecommunications and Information Administration (NTIA). See U.S. Department of Commerce, NTIA, "Office of the Assistant Secretary (OAS)," <https://www.ntia.doc.gov/office/OAS>.

<sup>120</sup> U.S. Copyright Office, Library of Congress, "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies," 86 *Federal Register* 59267, October 28, 2021 (Eighth Triennial Rulemaking Final Rule); 37 C.F.R. §201.40.

<sup>121</sup> Under the streamlined process, the Copyright Office's notice of proposed rulemaking (NPRM) advises the public that the Register intends to recommend that the Librarian renew previously granted exemptions. U.S. Copyright Office, Library of Congress, "Exemption to Permit Circumvention of Access Controls on Copyrighted Works," 88 *Federal Register* 37486, 37488, June 8, 2023, <https://www.federalregister.gov/documents/2023/06/08/2023-12250/exemptions-to-permit-circumvention-of-access-controls-on-copyrighted-works>.

<sup>122</sup> Under the comprehensive process, the Copyright Office's NPRM seeks comments from the public on newly proposed exemptions, and those previously granted with meaningful opposition, to inform the Register's recommendations to the Librarian (88 *Federal Register* 37489).

<sup>123</sup> 88 *Federal Register* 34786.

<sup>124</sup> Shira Perlmuter, *Section 1201 Rulemaking: Eighth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention*, U.S. Copyright Office, Library of Congress, Washington, DC, October 2021, pp. 232-233, [https://cdn.loc.gov/copyright/1201/2021/2021\\_Section\\_1201\\_Registers\\_Recommendation.pdf](https://cdn.loc.gov/copyright/1201/2021/2021_Section_1201_Registers_Recommendation.pdf). Eighth Triennial Rulemaking Final Rule 59,637; 37 C.F.R. §201.40(13)-(15) (adoption of recommendations by the Librarian of Congress as federal regulations).

<sup>125</sup> Library of Congress, Copyright Office, "Exemptions to Permit Circumvention of Access Controls on Copyrighted Works," 88 *Federal Register* 72013, 72020, October 19, 2023, <https://www.federalregister.gov/documents/2023/10/19/2023-22949/exemptions-to-permit-circumvention-of-access-controls-on-copyrighted-works> (discussing renewal of previously granted Section 1201 exemption for "Computer Programs—Repair of Motorized Land Vehicles, Marine Vessels, or Mechanized Agricultural Vehicles or Vessels") (hereinafter Ninth Triennial NPRM).

<sup>126</sup> MEMA, "Petition for New Exemptions Under 17 U.S.C. § 1201," August 25, 2023, <https://www.copyright.gov/1201/2024/petitions/proposed/New-Pet-MEMA.pdf>.

<sup>127</sup> Ninth Triennial NPRM, p. 72026.

### *Supporters of a New Copyright Exemption*

In December 2023, both the Specialty Equipment Market Association (SEMA)<sup>128</sup> and MEMA filed comments supporting MEMA's proposed exemption.<sup>129</sup> MEMA contends that OEMs' exclusive control over vehicle-generated data (1) reduces competition in the aftermarket, thereby raising consumer prices, and (2) creates inefficiencies in the vehicle repair and maintenance processes by prolonging the lag time between diagnostics, parts ordering, and vehicle repair.<sup>130</sup>

In March 2024, the DOJ and the FTC jointly filed a comment arguing that this exemption would further promote aftermarket competition.<sup>131</sup> Specifically, the agencies stated that

[r]estricting access to non-copyrightable telematics data risks establishing a competitively harmful bottleneck by depriving users of the ability to share this data with aftermarket parts manufacturers, third-party maintenance and repair services, and other adjacent markets that would put such information to valuable commercial use. This restriction is unwarranted in light of the minimal risk of infringing use of copyrighted [motor vehicle software].<sup>132</sup>

### *Opponents of a New Copyright Exemption*

Four groups filed comments opposing this proposed exemption: (1) Auto Innovators,<sup>133</sup> (2) the National Association of Manufacturers (NAM),<sup>134</sup> (3) the Association of Equipment Manufacturers (AEM),<sup>135</sup> and (4) the "Joint Creators"<sup>136</sup> (collectively, the Entertainment Software

<sup>128</sup> SEMA is a nonprofit trade association representing more than 7,000 mostly small businesses nationwide that manufacture, distribute, and sell specialty parts and accessories for motor vehicles. Comments of the Specialty Equipment Market Association to the U.S. Copyright Office on a Proposed Exemption Under 17 U.S.C. § 1201, Class 7 (Computer Programs – Vehicle Operational Data), December 21, 2023, <https://www.copyright.gov/1201/2024/comments/Class%207%20-%20Initial%20Comments%20-%20SEMA.pdf>.

<sup>129</sup> Ibid.; MEMA, "Comments to the U.S. Copyright Office on a Proposed Exemption Under 17 U.S.C. § 1201," December 22, 2023, <https://www.copyright.gov/1201/2024/comments/Class%207%20-%20Initial%20Comments%20-%20MEMA.pdf> (MEMA December 2023 Comments).

<sup>130</sup> MEMA December 2023 Comments, pp. 2-3.

<sup>131</sup> DOJ-FTC March 2023 Comment, p. 3 ("Accordingly, we urge the Copyright Office to recommend that the Librarian renew the existing repair-related exemptions and grant [this] additional proposed exemption[] to the DMCA").

<sup>132</sup> DOJ-FTC March 2023 Comment, p. 17.

<sup>133</sup> Opposition Comment of the Alliance for Automotive Innovation to the U.S. Copyright Office on Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, February 20, 2024, [https://www.copyright.gov/1201/2024/comments/opposition/Class%207%20-%20Opp'n%20-%20Alliance%20for%20Automotive%20Innovation%20\(Auto%20Innovators\).pdf](https://www.copyright.gov/1201/2024/comments/opposition/Class%207%20-%20Opp'n%20-%20Alliance%20for%20Automotive%20Innovation%20(Auto%20Innovators).pdf) (hereinafter Auto Innovators Opposition Comment).

<sup>134</sup> NAM represents 14,000 member companies in every industrial sector, including manufacturers throughout the United States. NAM, "Become a Member," <https://nam.org/member-services/join-the-nam/>. Opposition Comment of the National Association of Manufacturers to the U.S. Copyright Office on Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, February 20, 2024, [https://www.copyright.gov/1201/2024/comments/opposition/Class%207%20-%20Opp'n%20-%20Alliance%20for%20Automotive%20Innovation%20\(Auto%20Innovators\).pdf](https://www.copyright.gov/1201/2024/comments/opposition/Class%207%20-%20Opp'n%20-%20Alliance%20for%20Automotive%20Innovation%20(Auto%20Innovators).pdf) (hereinafter NAM Opposition Comment).

<sup>135</sup> AEM represents North American construction and agricultural equipment manufacturers. AEM, "About AEM," <https://www.aem.org/about>. Opposition Comment of the Association of Equipment Manufacturers to the U.S. Copyright Office on Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, February 20, 2024, <https://www.copyright.gov/1201/2024/comments/opposition/Class%207%20-%20Opp'n%20-%20Association%20of%20Equipment%20Manufacturers.pdf> (hereinafter AEM Opposition Comment).

<sup>136</sup> Opposition Comment of ESA, MPA, and RIAA to the U.S. Copyright Office on Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, February 20, 2024, <https://www.copyright.gov/1201/2024/> (continued...)

Association [ESA],<sup>137</sup> the Motion Picture Association [MPA],<sup>138</sup> and the Recording Industry Association of America [RIAA]<sup>139</sup>).

The groups contend that the exemption's proponents do not specify the relevant vehicle operational data or how they would use it.<sup>140</sup> In addition, they assert that third-party workshops "already have access to all necessary diagnostic and repair tools and information."<sup>141</sup> Auto Innovators maintains that proponents' assertions that the currently available processes for accessing diagnostic information and tools are "burdensome or time-consuming ... [or] may take longer than circumvention should not validate claims that an exemption should be granted."<sup>142</sup> Opponents further claim that granting a copyright exemption could put the Librarian in the position of preempting other federal laws and executive branch jurisdictions, including safety guidelines,<sup>143</sup> environmental regulations,<sup>144</sup> and privacy regulations.<sup>145</sup>

Moreover, NAM claims that addressing right-to-repair policies via the Section 1201 triennial rulemaking process "would circumvent the legislative process at a time when both Congress and state legislatures across the country are considering how to balance manufacturers' intellectual property rights with consumers' desires to repair their equipment."<sup>146</sup> The Joint Creators suggest

---

comments/opposition/Class%207%20-%20Opp'n%20-%20Joint%20Creators.pdf (hereinafter Joint Creators Opposition Comment).

<sup>137</sup> ESA represents video game publishers and video game platform providers. ESA, "Who We Are," <https://www.theesa.com/about-esa/>.

<sup>138</sup> MPA represents U.S. movie and television production studios. MPA, "Who We Are," <https://www.motionpictures.org/who-we-arc/#our-members>.

<sup>139</sup> RIAA represents record (music) labels in the United States. RIAA, "About RIAA," <https://www.riaa.com/about-riaa/>.

<sup>140</sup> Auto Innovators Opposition Comment, pp. 3-6; AEM Opposition Comment, pp. 2, 4 ("MEMA does not sufficiently define the vehicle operational data, telematics data, or diagnostics data as issue."); Joint Creators Opposition Comment, p. 2.

<sup>141</sup> Auto Innovators Opposition Comment, pp. 5-7, 10; NAM Opposition Comment, p. 3; AEM Opposition Comment, p. 2; Joint Creators Opposition Comment, p. 5.

<sup>142</sup> Auto Innovators Opposition Comment, pp. 7-8.

<sup>143</sup> Auto Innovators Opposition Comment, pp. 9, 11-12; NAM Opposition Comment, p. 2 (discussing concerns raised by NHTSA that a Massachusetts state law requiring OEMs to provide "remote, real-time, bi-directional (i.e., read/write capability) access to safety-critical vehicular systems" within a one-year time frame would "prohibit manufacturers from complying with both existing Federal guidance and cybersecurity hygiene best practices" in Letter from James C. Owens, Deputy Administrator, U.S. Department of Transportation, NHTSA, to The Honorable Tackey Chan, House Chair, Joint Committee on Consumer Protection and Professional Licensure, House of Representatives, Commonwealth of Massachusetts and The Honorable Paul R. Feeney, Senate Chair, Joint Committee on Consumer Protection and Professional Licensure, Senate Commonwealth of Massachusetts, July 20, 2020, [https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/nhtsa\\_testimony\\_in\\_response\\_to\\_ma\\_committee\\_letter\\_july\\_20\\_2020.pdf](https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/nhtsa_testimony_in_response_to_ma_committee_letter_july_20_2020.pdf)); Joint Creators Opposition Comment, p. 5.

<sup>144</sup> NAM Opposition Comment, p. 2 (discussing prohibitions against tampering with emissions controls (Section 203(a)(3) of the Clean Air Act (42 U.S.C. §7522))).

<sup>145</sup> Auto Innovators Opposition Comment, p. 8, note 28 (cross-referencing correspondence from Federal Communications Commission Chairwoman Jessica Rosenworcel to OEMs regarding whether OEMs connected to the internet may be "covered providers" under the Safe Connections Act of 2022 (P.L. 117-223, which establishes requirements concerning access to communication services for survivors of domestic violence, human trafficking, and related harms)), Letter from Chairwoman Jessica Rosenworcel, Chairwoman, Federal Communications Commission, to James D. Farley, Jr., President and Chief Executive Officer, Ford Motor Company et al., January 24, 2024, <https://docs.fcc.gov/public/attachments/DOC-399695A1.pdf>); Auto Innovators Opposition Comment, pp. 6-7.

<sup>146</sup> NAM Opposition Comment, p. 2.



that if the Librarian, despite their objections, permits the exemption for Class 7, the exemption “explicitly exclude in-vehicle entertainment systems in the context of the repair exemption.”<sup>147</sup>

## State Laws and Reactions: 2012-2024

### 2012-2014: Massachusetts Right-to-Repair Law and Industry MOU

In 2012, Massachusetts became the first state in the nation to enact a motor vehicle right-to-repair law.<sup>148</sup> The state did so both via a law enacted in July 2012<sup>149</sup> and a ballot measure approved by voters in November 2012.<sup>150</sup> In 2013, Massachusetts enacted a new version of automotive right-to-repair laws to reconcile conflict between the 2012 right-to-repair law and a ballot measure.<sup>151</sup> The provisions of this 2013 law, which are codified in Chapter 93K of the Massachusetts General Laws, formed the basis of a national MOU reached by industry participants the following year (2014 Industry MOU, also described in “Telematics”).

The 2013 Massachusetts law’s definition of an “independent repair facility” includes OEM-certified workshops. A dealer is included in the definition of an independent repair facility with respect to motor vehicles *unaffiliated* with the dealer’s franchise manufacturer; a dealer is excluded with respect to motor vehicles *affiliated* with the dealer’s franchise manufacturer.<sup>152</sup>

Failure to comply with the law “shall be deemed to be an unfair method of competition and unfair or deceptive act or practice in the conduct of trade or commerce” as defined elsewhere in Massachusetts’ statutes.<sup>153</sup> Both dealers and independent workshops have the right to sue OEMs in the event they are unable to agree on a remedy for allegedly violating the 2013 law.<sup>154</sup>

In 2014, using the text of the 2013 Massachusetts law as a model,<sup>155</sup> the Automotive Aftermarket Industry Association (AAIA), Coalition for Auto Repair Equality, Alliance of Automobile Manufacturers, and Association of Global Automakers, entered into a nationwide right-to-repair MOU (2014 Industry MOU).<sup>156</sup>

<sup>147</sup> Joint Creators Opposition Comment, p. 7.

<sup>148</sup> National Conference of State Legislatures, “Right to Repair 2023 Legislation,” November 1, 2023, <https://www.ncsl.org/technology-and-communication/right-to-repair-2023-legislation>. Several other states have right-to-repair laws that either are more limited or pertain to nonvehicle products.

<sup>149</sup> The 193<sup>rd</sup> General Court of the Commonwealth of Massachusetts, “Laws, Session Laws, Acts, 2012, Chapter 368, an Act Protect [sic] Motor Vehicle Owners and Small Businesses in Repairing Motor Vehicles,” <https://malegislature.gov/Laws/SessionLaws/Acts/2012/Chapter368>.

<sup>150</sup> Among the 3.2 million voters who cast their ballots, 86% approved the ballot measure. Secretary of the Commonwealth of Massachusetts, “Elections Division, Elections Results Archive,” [https://electionstats.state.ma.us/ballot\\_questions/search/year\\_from:2012/year\\_to:2012/text:repair](https://electionstats.state.ma.us/ballot_questions/search/year_from:2012/year_to:2012/text:repair).

<sup>151</sup> The 193<sup>rd</sup> General Court of the Commonwealth of Massachusetts, “Laws, Session Laws, Acts, 2013, Chapter 165, an Act Relative to Automotive Repair,” <https://malegislature.gov/Laws/SessionLaws/Acts/2013/Chapter165>.

<sup>152</sup> Massachusetts General Laws Ch. 93K, §1 (defining *independent repair facility*), <https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93K>.

<sup>153</sup> *Ibid.*, §6(a).

<sup>154</sup> *Ibid.*, §§6(b)-(e).

<sup>155</sup> Clifford Atiyeh, “Automakers Agree to Fix Your Car Anywhere in ‘Right to Repair’ Pledge,” *Car and Driver*, January 29, 2014, <https://www.caranddriver.com/news/a15366940/automakers-agree-to-fix-your-car-anywhere-in-right-to-repair-pledge/>.

<sup>156</sup> 2014 Industry MOU. In August 2015, industry participants entered into a separate MOU for commercial vehicles. Memorandum of Understanding Among National Commercial Vehicle Solutions Network, the Equipment and Tool (continued...)

## Similarities Between 2013 Massachusetts Law and 2014 Industry MOU

The following are key provisions in the MOU that mirror those in the 2013 Massachusetts law:

1. For model year 2002 motor vehicles and thereafter, each OEM “shall make available for purchase by owners and independent repair facilities all diagnostic tools incorporating the same diagnostic, repair and wireless capabilities that [the OEM] makes available to its dealers.”<sup>157</sup>
2. For model year 2018 motor vehicles, each OEM “shall provide access to their onboard diagnostic and repair information system” and enable repair facilities to use a standardized diagnostic tool that would work on vehicles from multiple OEMs.<sup>158</sup>
3. With the exception of “telematics diagnostic and repair information that [OEMs provide] to dealers, necessary to diagnose and repair a customer’s vehicle, and not otherwise available to an independent repair facility via the tools specified [in an earlier section of the MOU], nothing in the [MOU] shall apply to telematics services or any other remote or information service, diagnostic or otherwise, delivered to or derived from the vehicle by mobile communications.”<sup>159</sup>

OEMs are not required to give third parties access to nondiagnostic and repair information provided within the terms and conditions of their franchise agreements with dealers.<sup>160</sup> If an independent repair facility or owner believes that an OEM has failed to provide the information or tool required by the MOU, it may challenge the OEM’s actions by first notifying the OEM in writing.<sup>161</sup> The OEM has 30 days from the time it receives the complaint to cure the failure.<sup>162</sup>

## Differences Between 2013 Massachusetts Law and 2014 Industry MOU

The following provisions of the 2014 Industry MOU are not in the 2013 Massachusetts law:

- The 30-day deadline for an OEM to remedy a complaint from an independent repair facility does not apply if the parties agree to an alternative time frame.<sup>163</sup>
- Barring a satisfactory remedy from the OEM, an independent repair facility may appeal to a dispute resolution panel comprising representatives from each of the five signatory organizations.<sup>164</sup>

---

Institute, The Heavy Duty Aftermarket Canada, Auto Care Association, and the Truck and Engine Manufacturers Association, Service Information, August 12, 2015, <https://www.etools.org/Resources/Documents/RTR%20National%20Commercial%20Vehicle%20Service%20Information%20MOU%20executed%20MOU.pdf>.

<sup>157</sup> 2014 Industry MOU, §§2(a)-2(b); Massachusetts General Laws Ch. 93K, §§2(a)-(c)). The 2014 Industry MOU defines a *motor vehicle* as “any vehicle that is designed for transporting persons or property on a street or highway and that is certified by the manufacturer under all applicable federal safety and emissions standards and requirements for distribution and sale in the United States, but excluding (i) a motorcycle; (ii) a vehicle with a gross weight over 14,000 pounds; or (iii) a recreational vehicle or an auto home equipped for habitation” (§1).

<sup>158</sup> 2014 Industry MOU, §(2)(c)(i); Massachusetts General Laws Ch. 93K, §2(d).

<sup>159</sup> 2014 Industry MOU, §(2)(e); 2013 Massachusetts Acts Ch. 165 §2(f)), <https://malegislature.gov/Laws/SessionLaws/Acts/2013/Chapter165>. (As described in “2020 Massachusetts Data Access Law and Implementation,” Massachusetts General Laws 93K, §2(f) was amended in 2020 to include access to telematics data.)

<sup>160</sup> 2014 Industry MOU, §5; Massachusetts General Laws Ch. 93K, §5.

<sup>161</sup> 2014 Industry MOU, §6; Massachusetts General Laws Ch. 93K, §6(b).

<sup>162</sup> Ibid.

<sup>163</sup> 2014 Industry MOU, §6.

<sup>164</sup> 2014 Industry MOU, §6.

The following provisions of the 2013 Massachusetts law are not in the 2014 Industry MOU:

- Model year 2013 vehicles (and thereafter) weighing more than 14,000 pounds—with limited exceptions—are included within the category of vehicles for which each OEM “shall make available for purchase by owners and independent repair facilities all diagnostic tools incorporating the same diagnostic, repair and wireless capabilities that [the OEM] makes available to its dealers.”<sup>165</sup>
- OEMs’ ability to require dealers to purchase proprietary tools for accessing diagnostic, service, or repair information is limited if it provides, with more favorable terms and conditions, the same information to an independent repair facility or other third party via a standardized tool.<sup>166</sup>

## Debate Over Access to Telematics Data: 2015-2024

After the adoption of the 2014 Industry MOU, AAIA raised concerns about a stipulation in the MOU stating that OEMs need provide independent workshops with remote access to telematics data only if an alternative method does not exist.<sup>167</sup> AAIA claims that this provision constrains independent shops’ ability to compete by requiring consumers to travel to the shop in order to get their vehicles diagnosed. In contrast, AAIA claims, consumers need not travel to dealers for a diagnosis, because OEMs share telematics data with them.<sup>168</sup> In addition, when OEMs diagnose vehicles remotely and notify drivers that they may need to get their vehicle serviced, they can include marketing messages that promote aftermarket services from dealers.<sup>169</sup>

Auto Innovators counters that access to telematics data is unrelated to repair data and that initiatives seeking to include this access represent “a monetizable data grab from national aftermarket part manufacturers and retailers masquerading as consumer protection and support for small businesses.”<sup>170</sup> Furthermore, the organization claims that enabling independent workshops to access vehicle data remotely could pose cybersecurity and privacy risks to drivers.<sup>171</sup>

<sup>165</sup> Ibid., §1 (defining *heavy duty vehicle*); §§2(a), 2(c)(1); Massachusetts General Laws Ch. 93K, §§2(a)-(c)).

<sup>166</sup> Ibid., §§2(b), 2(c)(2).

<sup>167</sup> Elliot Maras, “R2R Pact Must Say More on Telematics,” *Professional Tool & Equipment News*, March 1, 2014, <https://www.vehicleservicepros.com/service-repair/diagnostics-and-drivability/article/11318521/r2r-pact-must-say-more-on-telematics>.

<sup>168</sup> Ibid. See also Testimony of Auto Care Association Senior Vice President for Regulatory and Government Affairs, Aaron Lowe, in U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Intellectual Property, *Are Reforms Needed to Section 1201?*, hearings, 116<sup>th</sup> Cong., 2<sup>nd</sup> sess., September 16, 2020, <https://www.judiciary.senate.gov/imo/media/doc/Lowe%20Testimony1.pdf>.

<sup>169</sup> Hiawatha Bray, “What’s the Tech Behind Question 1?” *The Boston Globe*, October 12, 2020, <https://www.bostonglobe.com/2020/10/12/business/whats-tech-behind-question-1/>.

<sup>170</sup> Memorandum from Alliance for Automotive Innovation to Interested Parties, *Dig Deeper: Maine Telematics Ballot Initiative*, October 2022, <https://www.repairerdrivennews.com/wp-content/uploads/2023/01/Maine-Ballot-Memo-to-Interested-Parties.pdf>.

<sup>171</sup> Letter from The Alliance for Automotive Innovation, the Automotive Policy Council, The American International Automobile Dealers Association et al. to The Honorable Cathy McMorris Rodgers, Chair, House Committee on Energy and Commerce; The Honorable Frank Pallone, Ranking Member, House Committee on Energy and Commerce; The Honorable Gus Bilirakis, Chairman, Subcommittee on Innovation, Data, and Commerce; House Committee on Energy and Commerce; The Honorable Jan Schakowsky, Ranking Member, S Subcommittee on Innovation, Data, and Commerce; House Committee on Energy and Commerce, October 31, 2023, <https://www.nada.org/media/8918/download?inline>.

## 2020 Massachusetts Data Access Law and Implementation

To support access to telematics data, Massachusetts Right to Repair—a coalition of independent vehicle workshops, vehicle part stores, and trade organizations—launched a campaign to update the Massachusetts right-to-repair law via a November 2020 ballot initiative.<sup>172</sup> The initiative proposed, beginning with model year 2022 vehicles, requiring OEMs selling or leasing vehicles in Massachusetts to equip them with a standardized open data platform.<sup>173</sup> This platform would enable vehicle owners and independent repair facilities to access, via a mobile application, “any vehicle-specific data, including telematics system data, generated, stored in[,] or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair[,] or maintenance of the vehicle”<sup>174</sup> without obtaining prior authorization from OEMs.<sup>175</sup>

In July 2020, in response to a request from Massachusetts legislators, the Deputy Administrator of NHTSA<sup>176</sup> submitted written testimony to the Massachusetts legislature addressing the proposed ballot initiative.<sup>177</sup> The agency expressed concerns that the ballot initiative would require “manufacturers to redesign their vehicles in a manner that necessarily introduces cybersecurity risks, and to do so in a timeframe that makes design, proof, and implementation of any meaningful countermeasure effectively impossible.”<sup>178</sup> In November 2020, 71% of Massachusetts voters approved the initiative.<sup>179</sup>

In 2021, Subaru and Kia disabled their telematics services for 2022 model year vehicles sold in Massachusetts.<sup>180</sup> A Subaru senior executive claimed that the company took this action because compliance with Massachusetts’s law was “impossible,” given that the data platform stipulated by the law did not exist and “will not exist any time soon.”<sup>181</sup>

In June 2023, NHTSA advised 22 OEMs that the Massachusetts Data Access Law “conflicts with and therefore [is] preempted by the [National Traffic and Motor Vehicle Safety Act (Safety Act), 49 C.F.R. Chapter 301]” due to cybersecurity risks.<sup>182</sup>

<sup>172</sup> Massachusetts Right to Repair, “About Us,” <http://massrighttorepair.org/aboutus.html>.

<sup>173</sup> William Francis Galvin, *Information for Voters, Massachusetts 2020 Ballot Questions, State Election, Tuesday November 3, 2020*, Elections Division, State of Massachusetts, Boston, MA, 2020, pp. 4-6, [https://www.sec.state.ma.us/divisions/elections/download/information-for-voters/IFV\\_2020-English.pdf](https://www.sec.state.ma.us/divisions/elections/download/information-for-voters/IFV_2020-English.pdf).

<sup>174</sup> *Ibid.*, p. 5 (defining *mechanical data*).

<sup>175</sup> *Ibid.*, pp. 5-6. See also Massachusetts General Laws Ch. 93K, §1 (defining *telematics system*), §§2(d)(1), (f).

<sup>176</sup> NHTSA’s statutory authority centers on motor vehicle safety (49 U.S.C. §30101 et. seq.).

<sup>177</sup> Letter from James C. Owens, Deputy Administrator, NHTSA, U.S. Department of Transportation, to the Honorable Tackey Chan, House Chair, Joint Committee on Consumer Protection and Professional Licensure of the State of Massachusetts and the Honorable Paul R. Feeney, Senate Chair, Joint Committee on Consumer Protection and Professional Licensure of the State of Massachusetts, July 20, 2020, [https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/nhtsa\\_testimony\\_in\\_response\\_to\\_ma\\_committee\\_letter\\_july\\_20\\_2020.pdf](https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/nhtsa_testimony_in_response_to_ma_committee_letter_july_20_2020.pdf).

<sup>178</sup> *Ibid.*

<sup>179</sup> William Francis Galvin, *Statewide Ballot Measures: 1919 Through 2020*, Elections Division, State of Massachusetts, Boston, MA, December 24, 2020, p. 65, <https://www.sec.state.ma.us/divisions/elections/download/research-and-statistics/Statewide-Ballot-Measures.pdf>.

<sup>180</sup> Hiawatha Bray, “In Latest ‘Right to Repair’ Move, Kia Shuts Off New Car Tech in Massachusetts,” *The Boston Globe*, January 21, 2022, <https://www.bostonglobe.com/2022/01/21/business/latest-right-repair-move-kia-shuts-off-new-car-tech-massachusetts/>.

<sup>181</sup> Larry P. Vellequette, “Subaru Disables Starlink in Massachusetts New Cars Amid Right-to-Repair Fray,” *Automotive News*, November 8, 2021, <https://www.autonews.com/service/subaru-disables-starlink-massachusetts-amid-right-repair-battle>.

<sup>182</sup> Notice of Transmittal of Letter to Vehicle Manufacturers, U.S. Department of Justice, No. 1:20-cv-12090 (D. Mass. (continued...))

In August 2023, NHTSA and the Assistant Attorney General of the Commonwealth of Massachusetts publicly stated that NHTSA's "understanding that a platform that provides the required features, capabilities, and access using a short-range wireless protocol such as Bluetooth is one approach that a vehicle manufacturer might use to achieve compliance with the [Massachusetts] Data Access Law" and would therefore not be inconsistent with federal vehicle safety regulations.<sup>183</sup> NHTSA expressed concern about the implications of disabling telematics services. The agency stated that disabling telematics services "would dissuade vehicle owner safety without advancing the right to repair."<sup>184</sup>

## 2023 Maine Vehicle Right-to-Repair Law and Proposed 2024 Amendments

In November 2023, 84%<sup>185</sup> of participating Maine voters approved a ballot initiative that requires OEMs to standardize onboard diagnostic systems and enable independent repair facilities and owners to access the diagnostic systems (i.e., telematics data) remotely.<sup>186</sup> In addition, the law directs OEMs to equip certain motor vehicles with a standard access platform.<sup>187</sup>

## 2023 Update to 2014 Industry MOU

In July 2023, organizations representing independent vehicle repair and service shops (ASA and SCRS) signed a separate MOU with Auto Innovators (2023 Industry MOU) updating the 2014 Industry MOU.<sup>188</sup> The 2023 Industry MOU affirms that motor vehicle owners and independent

---

June 13, 2023) (submitting as an attachment a Letter from Kerry E. Kolodziej, Assistant Chief Counsel for Litigation and Enforcement, U.S. Department of Transportation, National Highway Safety Administration, to Ann Maria Dias-Lebrun, Assistant General Counsel, BMW of North America, LLC, et al., June 13, 2023).

<sup>183</sup> Letter from Kerry Kolodziej, Assistant Chief Counsel for Litigation and Enforcement, U.S. Department of Transportation, National Highway Safety Administration, to Eric A. Haskell, Assistant Attorney General, Office of the Attorney General, Commonwealth of Massachusetts, August 22, 2023, <https://s3.documentcloud.org/documents/23925257/letter.pdf>. Letter from Eric A. Haskell, Assistant Attorney General, Commonwealth of Massachusetts, to Kerry Kolodziej, Esq., Assistant Chief Counsel for Litigation and Enforcement, NHTSA, August 22, 2023, <https://www.repairedrivenews.com/wp-content/uploads/2023/08/AG-letter-to-NHTSA.pdf>.

<sup>184</sup> Letter from Kerry Kolodziej, Assistant Chief Counsel for Litigation and Enforcement, U.S. Department of Transportation, National Highway Safety Administration, to Eric A. Haskell, Assistant Attorney General, Office of the Attorney General, Commonwealth of Massachusetts, August 22, 2023, p. 2, <https://s3.documentcloud.org/documents/23925257/letter.pdf>.

<sup>185</sup> State of Maine, Department of the Secretary of State, "Bureau of Corporations, Elections, and Commissions, Tabulations for Elections Held in 2023, Tabulation of Votes," <https://www.maine.gov/sos/cec/elec/results/results23.html> (out of the 404,782 total votes for this ballot initiative statewide, 341,574 were in favor).

<sup>186</sup> Maine Revised Statutes Title 29-A, §1801 (definitions), §1810, <https://legislature.maine.gov/legis/statutes/29-A/title29-Asec1810.html>. The diagnostic repair tools, parts, software, and components the law directs OEMs to release depend on the motor vehicle's model year. *Ibid.*, §§1810(3)-(5).

<sup>187</sup> *Ibid.*, §1810(6). OEMs are not required to provide access to information needed to reset a vehicle immobilizer system or security-related electronic modules. *Ibid.*, §1810(7). However, if such information is withheld, OEMs must make such information available through the secure data release model system used by the National Automotive Service Task Force (NASTF) or some other known, reliable, and accepted system. *Ibid.* NASTF is a nonprofit organization composed of automotive industry participants that provides credentials for technicians, mechanics, and locksmiths to access secure automotive information and systems (NASTF, "Welcome to NASTF," <https://wp.nastf.org/>).

<sup>188</sup> Automotive Service Association, "Independent Auto Repairers, Automakers Strike Major Right-to-Repair Pact," press release, July 11, 2023, <https://members.asashop.org/press-releases/Details/independent-auto-repairers-automakers-strike-major-right-to-repair-pact-175350>. See also Letter from Julie Massaro, President, Automotive Service Administration, Aaron Schulenburg, Executive Director, Society of Collision Repair Specialists, and John Bozzela, President and CEO, Alliance for Automotive Innovation, et al., to The Honorable Maria Cantwell, Chairwoman, U.S. Senate Committee on Commerce, Science, and Transportation, July 11, 2023, <https://sites.sema.org/> (continued...)

repair facilities can purchase repair and diagnostic systems that OEMs make available to authorized dealers on “fair and reasonable terms.”<sup>189</sup> The 2023 Industry MOU specifies that motor vehicle owners and independent workshops do not have access to vehicle-generated data “beyond what is necessary to diagnose and repair a vehicle.”<sup>190</sup> Owners’ and independent workshops’ access to diagnostics and repair data includes only what OEMs provide to their authorized dealers and “is not otherwise available through a tool or third-party service information provider.”<sup>191</sup>

Organizations representing aftermarket suppliers and independent workshops who did not sign the 2023 Industry MOU claim the MOU’s terms are insufficient to ensure competition in the motor vehicle aftermarket, in part because it does not oblige OEMs to provide vehicle owners or independent workshops direct access to telematics data.<sup>192</sup>

## Options for Congress

As congressional policymakers consider the ability for third parties to access software and data—including data unrelated to repair—in SDVs, they may weigh several options. They may decide that current federal laws are appropriate and allow federal government agencies to further develop and implement the proposed policies. In addition, lawmakers may opt to monitor actions by states, courts, and industry participants before taking further actions. Alternatively, congressional policymakers could increase oversight activities and direct the federal government agencies, through hearings, report language, or legislation, to take specific actions to reconcile potentially competing policy goals.

### Observe Impact of Industry Participants’ Private Negotiations

Lawmakers may prefer to observe the effect of the current MOUs between the OEMs, ASA, and SCRS on competition in the aftermarket.

### Permit Current Federal and State Policy Framework to Develop

As states enact different versions of laws requiring OEMs to permit independent workshops to access motor vehicle data and software, lawmakers may wish to observe the impact on consumers (e.g., Subaru’s and Kia’s disabling of telematics services in Massachusetts) prior to taking action.

In addition, lawmakers may choose to wait for courts to assess whether current federal laws preempt such state laws. In November 2023, Auto Innovators filed a lawsuit in the U.S. District Court for the District of Massachusetts.<sup>193</sup> The lawsuit contends that the Massachusetts Data

---

ext-assets/sema-news/National%20Automotive%20Right-to-Repair%20Letter%20to%20Congress%20July%202023%20(005).pdf (hereinafter 2023 Industry MOU).

<sup>189</sup> 2023 Industry MOU, “Automotive Repair Data Sharing Commitment” section.

<sup>190</sup> Ibid.

<sup>191</sup> Ibid.

<sup>192</sup> Auto Care Association, “Right to Repair Agreement a Thinly Veiled Attempt to Confuse Lawmakers and Drivers,” press release, July 11, 2023, <https://www.autocare.org/news/latest-news/details/2023/07/11/right-to-repair-agreement-a-thinly-veiled-attempt-to-confuse-lawmakers-and-drivers>. MEMA, “MEMA Aftermarket Suppliers Statement on Right to Repair Commitment,” press release, July 11, 2023, <https://www.mema.org/news/mema-aftermarket-suppliers-statement-right-repair-commitment>.

<sup>193</sup> Complaint, *Alliance for Automotive Innovation v. Maura Healey*, Attorney General of the Commonwealth of Massachusetts, in her official capacity No. 1:20-cv-12090 (D. Mass. November 20, 2020) (hereinafter *Alliance v. Healey Complaint*).

Access Law is unenforceable because it conflicts with federal laws,<sup>194</sup> including copyright laws (Section 1201 of the DMCA),<sup>195</sup> trade secret laws (the Defend Trade Secrets Act),<sup>196</sup> vehicle safety laws (the National Traffic and Motor Vehicle Safety Act),<sup>197</sup> and consumer data protection laws for financial institutions over which the FTC has jurisdiction (the Gramm-Leach-Bliley Act).<sup>198</sup> Auto Innovators stated that because OEMs routinely finance customers' purchase or lease of new vehicles, several of its members are considered by the FTC to be financial institutions for the purpose of enforcing the Gramm-Leach-Bliley Act.<sup>199</sup> Auto Innovators asked the court to "temporarily and permanently [enjoin] enforcement of the law."<sup>200</sup> As of the publication date of this report, the judge presiding over the bench trial has not issued a ruling.<sup>201</sup>

In addition, Members may observe or review the Librarian of Congress's expected forthcoming decision whether to extend the existing temporary exemption from copyright laws under the DMCA and/or establish a new exemption as proposed for the 2024-2027 time period.

## Enact Federal Legislation

Congressional stakeholders might opt to create a federal standard regarding the access of consumers and third parties to motor vehicle software and data in order to avoid or reduce the potential for a patchwork of state approaches, increase regulatory certainty, and harmonize potentially competing policy goals of different government agencies.

Legislative approaches might consider what agency is best suited to oversee any such effort and to what extent, if any, coordination across agency boundaries might be necessary given the data-centric issues raised. For example, in March 2024, the U.S. Department of Commerce's Bureau of Industry and Security issued an advance NPRM seeking, among other things, comments on national security risks associated with connected vehicles. While the FTC and NHTSA may have expertise with regard to cybersecurity needs based on their oversight of U.S.-based firms, other agencies may have expertise based on their oversight of U.S. trade and international relations.

Such approaches might also address whether to permanently permit access data subject to TPMs under Section 1201 of the Copyright Act. The existing exemption afforded to diagnosing, maintaining, or repairing a motorized land vehicle is temporary and based on a regular triennial decisionmaking process, as described above.

In the 118<sup>th</sup> Congress, H.R. 906, the Right to Equitable and Professional Auto Industry Repair Act (REPAIR Act), was introduced. It would specify that failure by OEMs to provide consumers and independent repair providers with access to "vehicle-generated data," "critical repair information," and tools needed to repair motor vehicles would constitute a violation of a regulation that, pursuant to Section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C.

<sup>194</sup> *Ibid.*, p. 24 (discussing the Gramm-Leach-Bliley Act), pp. 25-28 (discussing federal vehicle safety standards), pp. 28-32 (discussing copyright laws), p. 32 (discussing the Defend Trade Secrets Act).

<sup>195</sup> 17 U.S.C. §1201.

<sup>196</sup> 18 U.S.C. §1836 et seq.

<sup>197</sup> 49 U.S.C. §3101 et seq.

<sup>198</sup> 49 U.S.C. §6801(b).

<sup>199</sup> *Alliance v. Healey Complaint*, p. 24.

<sup>200</sup> *Ibid.*, pp. 53-54.

<sup>201</sup> Brian Dowling, "Automakers Want Mass. 'Right to Repair' Blocked Until Ruling," *Law360*, May 26, 2023, <https://www.law360.com/articles/1681974/automakers-want-mass-right-to-repair-blocked-until-ruling>.

§57a(a)(1)(B)), the FTC has the authority to prescribe.<sup>202</sup> In addition, the bill stipulates that the FTC, may, in consultation with NHTSA, “add additional types of data to the definition of vehicle-generated data under subsection (a)(20) regardless of whether those types of data are related to motor vehicle repair, taking cybersecurity and privacy into consideration, to allow consumers and their designees to directly access additional types of vehicle-generated data, and for additional purposes.”<sup>203</sup> On November 2, 2023, the House Committee on Energy and Commerce’s Subcommittee on Innovation, Data, and Commerce forwarded the bill to the full committee by a voice vote.<sup>204</sup>

## **Author Contact Information**

Dana A. Scherer  
Specialist in Telecommunications Policy  
dscherer@crs.loc.gov, 7-2358

---

<sup>202</sup> H.R. 906 §3(a). Section 18(a)(1)(B) of the Federal Trade Commission Act cross-references Section 5 of the Federal Trade Commission Act (15 U.S.C. §45), which describes the agency’s authority to prohibit unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, as described in “Federal Trade Commission.”

<sup>203</sup> H.R. 906 §5(b)(20).

<sup>204</sup> H.R. 906.



# Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice

U.S. Government Accountability Office (GAO)

GAO-24-106633 – Q&A Report to Ranking Member on Innovation, Data  
and Commerce, Committee on Energy and Commerce, House of  
Representatives

3/21/2024



U.S. Government Accountability Office

# Vehicle Repair: Information on Evolving Vehicle Technologies and Consumer Choice

GAO-24-106633

Q&A Report to the Ranking Member, Subcommittee on Innovation, Data, and Commerce, Committee on Energy and Commerce, House of Representatives

March 21, 2024

## Why This Matters

The term “right-to-repair” refers to consumers’ ability to decide who repairs their products. For vehicles, this means consumers deciding whether to make their own repairs or take their vehicle to repair facilities. Repair facilities may be at businesses franchised with or owned by automakers, known as dealerships, or repair shops not associated with dealerships, known as independent repair shops. Vehicles are becoming more technologically advanced and increasingly transfer data, including repair data, wirelessly directly to automakers. This trend may cause challenges for independent repair shops in conducting repairs as they may not have access to that data as automakers may not share it with them.

The federal government has a limited role regarding vehicle repairs. The Department of Transportation’s National Highway Traffic Safety Administration (NHTSA) is focused on vehicle safety and is involved in vehicle right-to-repair issues only when they affect vehicle safety. The Federal Trade Commission (FTC) is involved in protecting consumers and promoting competition, including in the vehicle repair market.

We were asked to review the effects of changing vehicle technologies on vehicle right-to-repair. This report examines how changes in vehicle technologies could affect competition and consumer choice in the vehicle repair market and NHTSA’s and FTC’s actions related to this issue.

## Key Takeaways

- Most automakers have been operating under a 2014 voluntary right-to-repair agreement that generally resulted in independent repair shops having access to the information, data, and tools needed for repairs. However, stakeholders we interviewed, and a nongeneralizable review of a set of complaints, suggest independent repair shops may face some access limitations.
- Advanced vehicle technologies may make repairs more expensive and complex because they require additional knowledge, equipment, and other investments. Such issues could particularly affect some independent repair shops that are unable to make such investments. In addition, according to some independent repair stakeholders, the wireless transfer of data between vehicles and automakers may disadvantage independent repair shops compared to dealerships.
- If independent repair shops face limitations in access to the information, data, and tools needed for repair, consumers might have fewer repair choices. If independent repair shops face disparities in access, it could make repairs more expensive or inconvenient for some consumers.
- FTC is taking steps to better understand potential vehicle repair limitations by considering new ways to categorize and analyze potentially relevant consumer complaints.

---

## Who repairs vehicles and what do they need to perform repairs?

Vehicle repairs can be done by individual consumers or by repair facilities at dealerships or independent repair shops, using vehicle and repair information, data, and tools. We refer to anyone repairing a vehicle as a “technician.” Mechanical repairs to vehicles generally involve repairs to a vehicle’s working parts, such as its engine, brakes, or electrical components. Repairs can also be body repairs, which often take place after collisions.

Repair shops tend to specialize in either mechanical repairs or body repairs. According to the National Automobile Dealers Association, while all dealerships have mechanical repair centers, per their franchise agreement with their automaker, only about one-third of dealerships have body shops. Beyond dealerships, automakers have networks of certified independent body shops whose employees must take certain training and must purchase certain equipment to be certified to work on their vehicles. All eight automakers we met with told us they have such certifications.

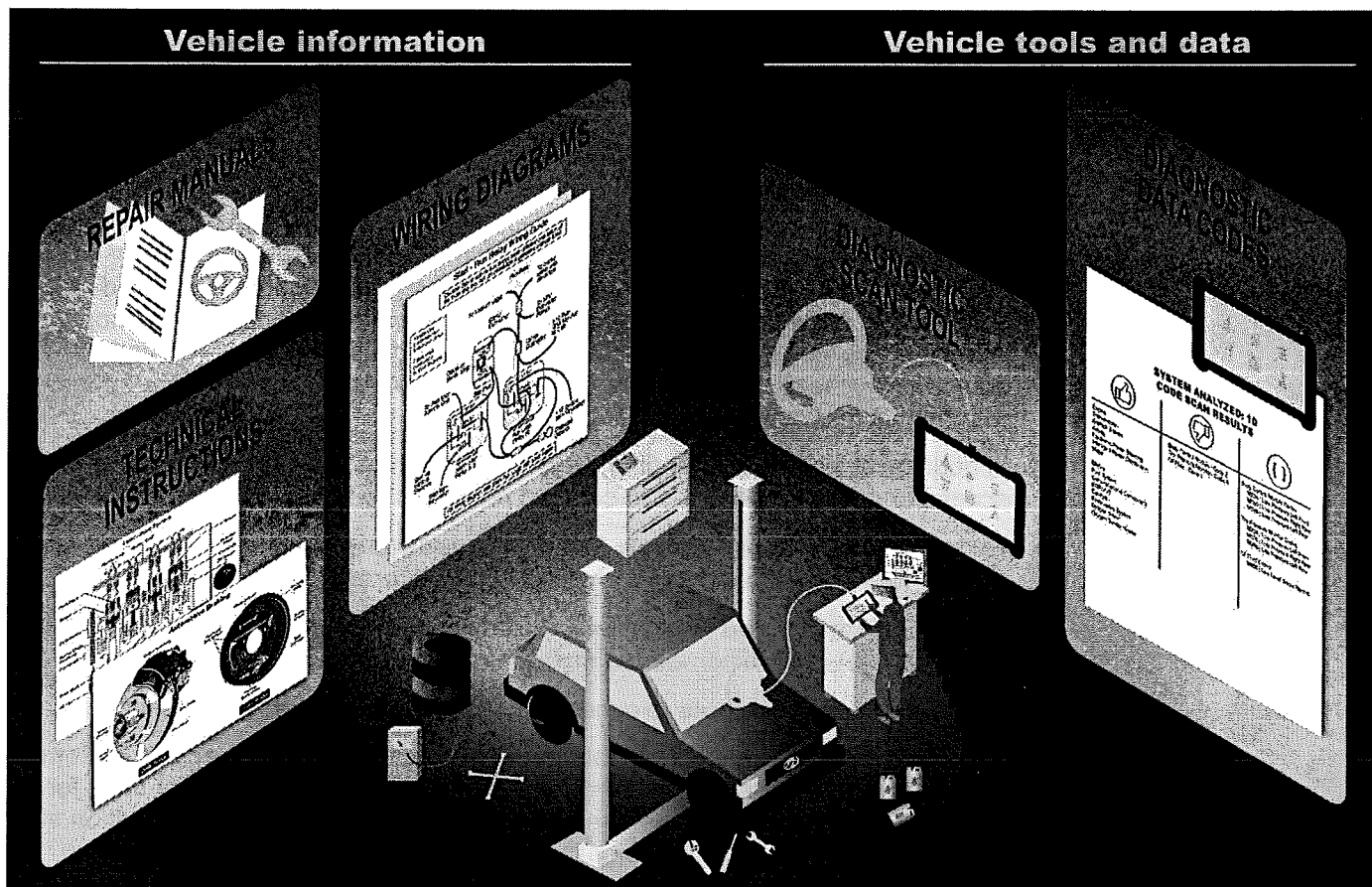
In addition to potentially needing vehicle replacement parts, any technician needs access to multiple resources to conduct repairs (see fig. 1). These include:

- **information on the vehicle and its components**, such as wiring diagrams and repair manuals detailing how to conduct repairs;
- **vehicle health and repair data**, including diagnostic error codes that help a technician determine needed maintenance or repairs; and
- **diagnostic scan tools** to access a vehicle’s health and repair data.

Independent repair shops may obtain vehicle repair information and tools from individual automakers or from third parties that provide information or tools for vehicles from multiple automakers. Dealerships generally obtain information and tools from their franchised automaker based on conditions in their franchise agreement.

Currently, to diagnose a vehicle, technicians generally plug a diagnostic tool into a port inside the vehicle. The tool then reads the vehicle’s data and provides information on the vehicle’s health and potential problems. The technician may then use the vehicle data, along with repair information, to conduct the repair. Technicians may also need to use diagnostic tools after a repair is completed to reprogram the vehicle’s systems or components to “know” that the repair has been made.

Figure 1: Information, Data, and Tools Needed for Vehicle Repairs



Sources: GAO illustration and analysis of industry information. Images (left to right) Udaix/stock.adobe.com, WPEVStartRunWires/en.m.wikipedia.org. | GAO-24-106633

## What attempts have been made to ensure independent repair shops can access the information, data, and tools needed for repair?

While there is no federal law requiring manufacturers to ensure vehicle owners and independent repair shops have access to information, data, and tools needed for vehicle repair, there have been some key relevant state and nationwide industry efforts.<sup>1</sup> We did not conduct a comprehensive review of state laws to determine what other states, if any, have taken relevant actions.

### 2012 Massachusetts Law

In 2012, Massachusetts voters approved a vehicle repair ballot initiative. This law required automakers to provide to independent repair shops and vehicle owners equal access to the same vehicle repair data provided to their dealerships, starting with model year 2002 vehicles. This law also prohibited the sale or lease of new vehicles after model year 2015 if manufacturers did not ensure such access.<sup>2</sup>

### 2014 Industry Memorandum of Understanding

Following passage of the 2012 Massachusetts law, industry associations representing many automakers and associations representing independent repair shops entered into a national Memorandum of Understanding (Memorandum) in 2014. In this Memorandum, automakers committed to providing independent repair shops and owners access to the same information, data, and tools needed for vehicle repair that they provide to dealerships on “fair and reasonable terms”

beginning with model year 2002 vehicles. While non-binding, the Memorandum set up a dispute resolution process—now managed by the National Automotive Security Task Force (Task Force)—for independent repair shops to raise disputes when they believe they do not have full access. According to FTC, the Memorandum had the effect of helping provide consumers with choice in where to get their vehicles repaired.<sup>3</sup>

### **2020 Massachusetts Law**

In 2020, Massachusetts voters approved an amended vehicle repair law—the Massachusetts Data Access law—which required automakers to equip vehicles with a secure interoperable open data platform to allow vehicle owners and independent repair shops to access repair data through telematics by model year 2022.<sup>4</sup> Shortly after voters approved the law, the Alliance for Automotive Innovation—an industry association representing automakers—filed suit in federal court. This suit seeks to block the law’s enforcement in part on the grounds that the law is preempted by the National Traffic and Motor Vehicle Safety Act (Safety Act)—which directs NHTSA to establish vehicle safety standards—and other federal laws.<sup>5</sup> As of March 8, 2024, litigation related to preemption is ongoing.

### **2023 Industry Commitment**

Subsequently, in July 2023, different industry associations representing automakers and independent repair shops entered into a national commitment reaffirming the principles of the 2014 Memorandum.<sup>6</sup> The commitment clarified the application of those principles to electric and hybrid vehicles and stated that automakers will provide access to vehicle telematics data necessary for vehicle diagnostics and repair, if not otherwise available. The commitment also called for the creation of a panel of industry stakeholders to review issues with the availability of repair and diagnostic data and collaborate on potential solutions. In addition, the commitment stated the parties would establish a working group to review changes in vehicle technologies that may affect the vehicle repair market. The parties agreed to annually review and update the commitment if appropriate.

### **2023 Maine Law**

In November 2023, Maine voters approved a vehicle repair ballot initiative similar to the Massachusetts Data Access Law.<sup>7</sup>

---

## **What are trends in the vehicle repair market for independent repair shops and dealerships?**

Revenues for the total vehicle aftercare market—which includes supporting vehicles after they are first sold, including parts and services—grew 41 percent from 2014 to 2022, according to data reported by the Auto Care Association.<sup>8</sup> This figure includes independent repair shops, dealerships, and other businesses. According to an industry report we reviewed, independent repair businesses compete on multiple factors including price, quality of service, and convenience. This report added that there are low barriers to entry for new repair shops, which allows new independent repair shops to enter the market easily.<sup>9</sup>

### **Independent Repair Shops**

According to data reported by the Auto Care Association, independent repair shops and other companies that support vehicle care that are not dealerships consistently earned about 70 percent of all post-sale vehicle-related revenues from 2014 to 2023.<sup>10</sup> However, these revenues include services and goods

beyond repairs and parts. For example, car washes and car care products sold at retail stores, such as hardware stores, are included in this percentage.

In addition, according to our analysis of data reported by the Auto Care Association, in line with the overall growth of the vehicle aftercare market, the independent repair market has grown in recent years. We found that total revenues (which include parts as well as services such as repairs and maintenance) for independent repair shops grew about 43 percent from 2014 to 2022. Our analysis of data reported by the Auto Care Association also found that the number of independent repair shop locations grew 4 percent during that time.<sup>11</sup>

### Dealerships

Total dealership revenues for repair services and parts grew 45 percent from 2014 to 2022, according to estimates by the National Automobile Dealers Association. According to that association, the number of dealerships remained relatively flat, growing by about 2 percent during that time. Dealerships generally compete more with independent repair shops that focus on mechanical repairs than with body shops given that, as noted earlier, not all dealerships do body repair work. The National Automobile Dealers Association estimates that 35 percent of dealerships had on-site body shops in 2022, down from 39 percent in 2017.<sup>12</sup>

---

### Do independent repair shops have access to what they need to conduct vehicle repairs?

Views varied on the extent to which independent repair shops have access to the necessary information, data, and tools to make vehicle repairs. Most automaker and independent repair stakeholders we interviewed stated that, since 2014, independent repair shops have generally had access to what they need to make repairs.<sup>13</sup>

Officials from all eight automakers we interviewed said they provide to independent repair shops, on fair and reasonable conditions, equal access to the information, data, and tools needed for repairs, and will continue to do so. Specifically:

- **Information.** All automakers we interviewed sell subscriptions to repair information, such as repair manuals, to independent shops for as short as a day and as long as a year. Seven of the eight also provide their repair information to third party companies that sell access to independent repair shops.<sup>14</sup>
- **Data and tools.** All automakers we interviewed said their company provides access to vehicle diagnostic and repair data to independent repair shops. All sell their own diagnostic tools to be used with their vehicles and provide the data needed to third party tool companies that offer tools to work with vehicles from multiple automakers.

However, nine of the 14 independent repair stakeholders described limitations related to being able to access specific vehicle data, in some cases for specific automakers. For example:

- One independent repair shop technician described problems using a third-party scan tool that provides basic diagnostic data but does not provide access to certain vehicle components, such as the tire pressure monitoring system. The technician said this, and other data limitations, result in the shop needing to take some vehicles to dealerships to complete repairs.

- One independent repair shop owner said that they have difficulty programming parts installed in many vehicles because they do not have the access needed to do so.
- One independent technician said that they were unable to use third-party scan tools with newer vehicles from one automaker and instead must use the tool sold by that automaker.

It is hard to determine how common those limitations are. Our nongeneralizable review of complaints from independent repair shops filed with the Task Force and a set of consumer vehicle safety complaints filed with NHTSA (which are not intended to be about vehicle repair issues) found some potential instances of independent repair shops not having access to the information, data, or tools needed for repair.<sup>15</sup> For example, one complaint filed with NHTSA alleged that a vehicle owner took their vehicle to an independent repair shop that could not do the work because the shop lacked the access to program the vehicle. In addition, there were multiple Task Force complaints from independent repair shops regarding an inability to diagnose vehicles.

According to FTC officials, the agency has received some relevant complaints in its public complaint system. While officials did not quantify the exact number, they described it as limited. FTC officials noted that it is difficult to determine which, if any, vehicle repair complaints might indicate independent repair shop access limitations because people filing complaints may not use terminology that make such complaints easily identifiable.

### How are changing vehicle technologies presenting challenges for independent repair shops?

Evolving vehicle technologies are presenting challenges for repair shops, including independent repair shops, by making some repairs more complex and expensive. Evolving vehicle technologies include:

- **Advanced driver assistance systems.** These technologies are designed to improve vehicle safety by, for example, helping drivers avoid crashes through the use of sensors, cameras, and other technologies. According to Consumer Reports, these systems were available on more than 50 percent of 2023 model year vehicles. Following repairs, these technologies often need to be recalibrated with expensive, specialized equipment. Ten of the 14 independent repair stakeholders said this complexity may limit a technician's ability to conduct some repairs if, for example, they lack the necessary equipment or training.
- **Software-based components.** Evolving safety features and other advances have led to the use of more electronics and software in vehicles, which may require programming. According to the Institute for Electrical and Electronics Engineers, premium cars contained 100 electronic control units (embedded devices that execute vehicle functions) in 2011; however, they may now have more than 150 electronic control units. In addition, according to the institute, even low-end vehicles now may have almost 100 million lines of software code. Three independent repair shops we interviewed cited instances of not having access needed to be able to reprogram vehicle electronics systems after repairs so that those systems will link to replacement parts.
- **Electric vehicles (EVs).** According to a report by McKinsey & Company, EVs have reduced the need for maintenance overall, but require additional training and investments by repair shops given the use of batteries and other components.<sup>16</sup> Investments in tools, technologies, and training are critical for technicians to work on EVs. One independent repair shop owner said the shop lacked the experience and training to work on EVs, a situation the shop

has addressed by investing the time and resources necessary to train 20 technicians to repair them. The owner added that extensive training is necessary as each automaker approaches EV systems differently. The number of EVs may grow as the current administration has a goal for EVs to comprise 50 percent of all new vehicle sales by 2030.

These evolving vehicle technologies impose challenges on all repair shops. For example, two dealerships we met with cited the high costs of equipment needed to calibrate advanced driver assistance systems. An industry study also reported that more than half of dealerships are not fully prepared to service electric vehicles.<sup>17</sup> In addition, challenges in repairing vehicles with advanced technologies may especially affect the ability of some independent repair shops to be competitive. For example, independent repair shops that do not have the ability or willingness to undertake needed investments and training may not be able to conduct such repair work. According to one industry report we reviewed, repairers that are unable to work on technologically advanced vehicles will lose out on business while those able to keep up with technology will be better able to compete.<sup>18</sup>

---

**How could independent repair shops be affected by potential changes in the availability of repair and diagnostic data?**

The ability of vehicles to transmit repair and diagnostic data wirelessly over telematics systems may disadvantage independent repair shops compared to dealerships, according to independent repair stakeholders. According to the automakers we interviewed, almost all model year 2023 vehicles sold in the U.S. transmit some vehicle data through telematics to automakers. This may include data on the vehicle's health and needed repairs or maintenance, such as the need for an oil change or the diagnostic code behind a check engine light, which might indicate a needed repair.

Six automakers we interviewed told us they do not provide dealerships with any access to telematics data. The two that do provide access to some telematics repair and diagnostic data, provide a similar level of access to independent repair shops. For example, one automaker provides access to telematics data to independent repair shops in some circumstances when it may be useful, but not necessary, for a repair, such as to provide historical information on the vehicle's health. All the automakers said telematics data are not currently needed to diagnose or repair a vehicle, as all the necessary data are available through the physical port in the vehicle. Most (11 of 14) independent repair stakeholders agreed and said that independent repair shops do not currently need telematics data for repairs.

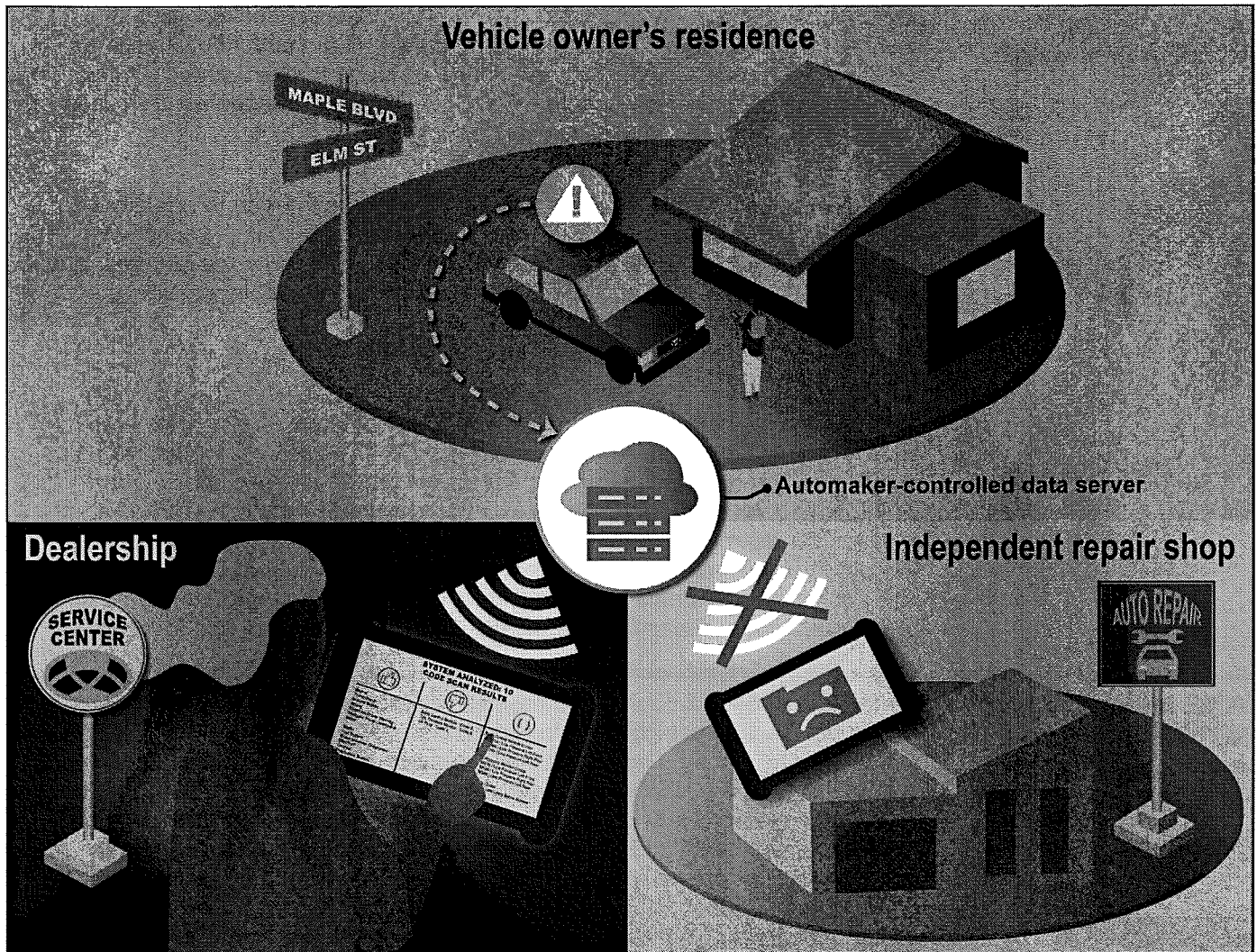
All automakers we interviewed added that their companies plan to continue to make repair and diagnostic data available to independent repair shops through the physical port inside vehicles. They added that should that data no longer be available that way, they will continue to make the data available regardless of the mechanism used for access. However, many independent repair stakeholders expressed concerns about the voluntary nature of the 2014 Memorandum and 2023 commitment and that automakers may not continue to provide access. In addition, all four independent repair shops and six of 10 independent repair associations we interviewed expressed concerns that even if such data continue to be available through physical access in vehicles, any disparities in telematics data access between independent repair shops and dealerships may disadvantage independent repair shops. For example:

- **Remote diagnosis.** If automakers allow dealerships to directly access a vehicle's telematics data, including detailed diagnostic codes, they may, at an owner's request, be able to remotely diagnose a vehicle and tell the vehicle owner what repairs, if any, need to be conducted (see fig. 2). Independent repair shops that do not have access to such data would need the owner to



bring the vehicle to their shop for diagnosis. According to two independent repair stakeholders we interviewed, this would be an inconvenience for customers that may disadvantage independent repair shops.

Figure 2: Example of Potential Remote Vehicle Diagnosis by Dealership via Telematics



Source: GAO illustration and analysis of industry information. | GAO-24-106633

- Marketing.** Currently, because automakers control access to telematics data, they and their dealerships can proactively inform some consumers when vehicles need repair or maintenance. For example, an automaker could notify an owner when a vehicle needs an oil change and direct them to a nearby dealership. While the consumer could still take their vehicle to an independent repair shop, this outreach may make them more likely to go to a dealership. Ten of the 14 independent repair stakeholders expressed concern that this scenario would disadvantage independent repair shops.
- Over-the-air updates.** According to NHTSA, automakers are increasingly using over-the-air updates to address some safety recalls electronically. However, four independent repair stakeholders expressed concern that in the future, automakers may be able to conduct some repairs through wireless over-the-air updates, leaving independent repair shops unable to conduct

such repairs. However, to the extent that over-the-air updates are used by automakers for some repairs in the future, dealerships also would likely miss out on the opportunity to conduct such repairs.

---

**Are there potential cybersecurity concerns with providing access to telematics data?**

There are potential cybersecurity risks with sharing access to vehicle data, including telematics data, as we have previously reported.<sup>19</sup> Cybersecurity risks can include the potential for hackers to exploit vulnerabilities in systems to gain access to vehicle data, including location data, and to control critical vehicle systems such as steering. Our past work also found that researchers have demonstrated that hackers could exploit vulnerabilities in a telematics system to compromise multiple vehicles simultaneously.

According to NHTSA, telematics systems could be leveraged to compromise vehicle systems if not properly designed and protected. Our previous work identified key practices for mitigating vehicle cybersecurity vulnerabilities. These practices include building cybersecurity protections into vehicles starting in their early design phase, separating safety-critical systems from other systems on vehicle networks, and conducting risk assessments.<sup>20</sup>

Despite potential cybersecurity risks, two stakeholders we interviewed with expertise in cybersecurity indicated that it could be possible for automakers to provide secure access to telematic diagnostic and repair data to independent repair shops. All eight automakers expressed concerns with open access systems for telematics data but said they could provide the necessary access through their own closed systems. Two automakers we interviewed told us they use such closed systems to provide, on a limited basis, secure access to some vehicle telematics repair and diagnostic data to independent repair shops.

---

**What actions are NHTSA and FTC taking regarding potential vehicle repair limitations?**

Because NHTSA's authority and mission are focused on vehicle safety, NHTSA's role in the issue of vehicle right-to-repair has been limited to addressing potential cybersecurity concerns as they relate to vehicle safety and ensuring compliance with the Safety Act. NHTSA has recognized that the balance between vehicle repair and cybersecurity is not easy to achieve. NHTSA has also stated that cybersecurity should not be a reason to justify limiting who can conduct repairs and, conversely, the ability to make repairs should not limit cybersecurity controls.<sup>21</sup> In addition, NHTSA has communicated with automakers and state officials regarding whether and what type of telematics access systems would create potential vehicle safety and security risks.

FTC has broadly studied and taken action on repair restrictions in various industries, including vehicle repair. As part of its efforts to broadly study repair issues, FTC held a workshop in July 2019 on repair restrictions across a range of industries and, in May 2021, issued a report in part based on that workshop.<sup>22</sup> While this report highlighted automakers' efforts to increase repair options for consumers, it also noted that stakeholders expressed concerns about potential access limitations, including the potential for automakers to restrict access to telematics data to reduce consumer choice for repairs.

FTC has also taken action against specific automakers regarding vehicle repair issues that may violate federal laws. For example, in 2015, the FTC settled charges with one automaker it alleged told some vehicle owners that the automaker's warranty would be voided if vehicle owners did not use dealerships for maintenance and repair and that the automaker would only cover genuine parts from the automaker.<sup>23</sup> FTC staff also sent a letter to another automaker in

2018 raising concerns about statements made by the automaker indicating that consumers had to use that automaker's official parts in repairs to not void their warranty.<sup>24</sup>

According to agency officials, FTC enforcement actions can be driven by its evaluation of relevant complaints filed with the agency, among other things. FTC officials said that the agency is taking steps to better analyze its complaint data to identify relevant complaints related to vehicle repair limitations. For example, FTC officials said that FTC is developing search tools, informed by research, to better analyze complaints to identify relevant ones. FTC has also been working to improve how complaints are coded when filed by consumers. According to FTC officials, these are ongoing efforts and there are no specific time frames for completion. These efforts may better enable FTC to identify the extent to which limitations for independent repair shops negatively affect consumers and, therefore, potentially take action.

---

**What might all this mean for consumers?**

A reduction in the ability of independent repair shops to conduct repair work could reduce consumer repair choices, whether that reduction is due to limited access to the information, data, and tools needed for repair or to an unwillingness or inability to keep up with technological changes. In addition, a disparity in access to telematics data compared to dealerships could put independent repair shops at a competitive disadvantage. These potential effects could increase prices for consumers as well as affect consumers in other ways. For example, consumers may have to travel farther if local independent repair shops are not available or could experience increased wait times if there are fewer shops overall making repairs.

The potential negative effects of reduced consumer choice may not be felt equally among all vehicle owners. For example, low-income or rural consumers could be harmed the most, according to five independent repair shops and independent repair associations. Specifically, low-income consumers may have more difficulty paying if there is an increased cost of repairs. Rural customers may have fewer local options to begin with so may need to take their vehicles to dealerships or other facilities further away if local repair shops were to close.

Stakeholder views differed on the extent to which, in the future, independent repair shops will have access to the information, data, and tools needed for repairs. All eight automakers we interviewed said that they will continue to provide equal access to information, data, and tools to independent repair shops. All eight of the automakers either are party to or said they support the 2023 commitment. However, eight of the 14 independent repair stakeholders we interviewed expressed concerns about lack of enforceability in the 2014 Memorandum and 2023 commitment. Specifically, because those agreements are voluntary, stakeholders worried that automakers may stop providing access to the information, data, and tools needed for repair. To the extent that happens, independent repair shops may be limited in their ability to conduct some repairs.

---

**Agency Comments**

We provided a draft of this report to the Department of Transportation and the FTC for review and comment. The Department of Transportation and FTC both provided technical comments that we incorporated as appropriate.

## How GAO Did This Study

To inform how changes in vehicle technologies could affect competition and consumer choice in the vehicle repair market we conducted a literature search and reviewed relevant studies and papers. We searched for literature published between January 2018 and May 2023 in database platforms including ProQuest, EBSCO, Scopus, Dialog, and Westlaw using search terms including “vehicle right-to-repair” and “automobile repair.” We reviewed abstracts of publications in the search results to select and obtain those most relevant to vehicle repair limitations. We did not identify sufficient literature to draw broad conclusions about vehicle repair limitations.

We reviewed publications from FTC and NHTSA as well as industry associations. We analyzed industry data on independent repair shops reported by the Auto Care Alliance.<sup>25</sup> To determine the reliability of that data, we interviewed Auto Care Alliance staff regarding how the association collected the underlying data. We concluded that the data were sufficiently reliable to report on trends in the repair market.

We conducted a nongeneralizable review of complaint data from NHTSA and the Task Force to identify possible examples of repair limitations for independent repair shops. We did not review these complaints, or conduct any quantitative analysis, to determine the extent of the problem. We obtained records on over 260,000 vehicle safety complaints (known as Vehicle Owner’s Questionnaires) filed with NHTSA from January 1, 2020 to May 16, 2023. We searched complaints using terms such as “independent shop,” “could not diagnose,” and “local mechanic” to determine if any might indicate a limitation in independent repair shop access to information, data, and tools needed for vehicle repair.

We obtained all 238 complaints filed with the Task Force by independent repair shops or others from December 9, 2020 to June 7, 2023, the time range for which the Task Force could provide records. We reviewed each of these complaints to determine if some may have indicated limitations by automakers in providing access to the information, data, and tools needed for vehicle repair to independent repair shops.

For both sets of complaint data, because it was difficult to determine if any given complaint indicated an issue with limited access to repair information, data, or tools by independent repair shops, we did not attempt to quantify the number of potentially relevant complaints. To determine the reliability of these complaint data, we interviewed NHTSA officials and Task Force staff. We concluded that the data were sufficiently reliable for identifying possible examples of vehicle repair limitations for independent repair shops.

In addition, we interviewed a range of 51 industry stakeholders. For some interviews we selected interviewees in specific states—Illinois, Maine, and Massachusetts. We selected these states to include a range of urban and rural populations, number of auto mechanics, the number of electric vehicles (as a percentage of all registered vehicles in each state), and state-specific advocacy on vehicle right-to-repair issues. In each state we attempted to interview representatives from the following entities: the state Attorney General’s office, independent repair shops, independent repair organizations, state-specific automobile dealership associations, state vehicle fleet management agencies, and franchised dealerships.<sup>26</sup>

Interviewees included:

- Fourteen independent repair stakeholders, including 10 associations selected based on involvement in vehicle repair issues and recommendations from other interviewees and four independent repair shops based on recommendations from state or regional independent repair associations;

- Six dealerships selected based on recommendations by national or state dealership associations and three dealership associations selected based on their representation of dealerships at the national or selected state level;
- One automaker association and eight automakers selected based on market share and to include domestic and foreign automakers as well as one automaker focused only on electric vehicles;
- Five consumer interest groups selected based on web searches for involvement in relevant issues or recommendations from other interviewees;
- Four state agencies involved in fleet management or consumer protections in selected states; and
- Ten other stakeholders, including three involved in cybersecurity issues, based on recommendations from other interviewees on involvement in relevant issues.

For a list of all industry stakeholders we interviewed see table 1. We reviewed interviews to identify how frequently different themes and viewpoints were mentioned.

**Table 1: List of Interviewed Industry Stakeholders**

**Independent repair associations and shops**

Alliance of Automotive Service Providers of Illinois	MEMA Aftermarket Suppliers
Alliance of Automotive Service Providers of Massachusetts, Inc.	Mid Atlantic Auto Care Alliance
Auto Care Association	Midwest Auto Care Alliance
Automotive Service Association	National Independent Automobile Dealers Association
Axel's Automotive (Illinois)	New England Tire and Service Association
Don Foshay's Discount Tire & Alignment (Maine)	Society of Collision Repair Specialists
Direct Tire & Auto Service (Massachusetts)	VIP Tires & Service (Maine)

**Dealership associations and dealerships**

Advantage Acura and Advantage Chevrolet (Illinois)	National Automobile Dealers Association
Herb Connolly Chevrolet (Massachusetts)	Pape Chevrolet-Subaru (Maine)
Illinois Automobile Dealers Association	Quirk Chevrolet of Portland (Maine)
Maine Automobile Dealers Association	<i>One dealership that did not want to be named</i>
MetroWest Subaru (Massachusetts)	

**Automaker associations and automakers**

Alliance for Automotive Innovation	Subaru
Ford Motor Company	Tesla
General Motors	Toyota Motor North America
Hyundai Motor America	<i>One automaker that did not want to be named</i>
Stellantis	

**Consumer interest groups**

AAA	Public Interest Patent Law Institute
Consumer Reports	U.S. Public Interest Research Group
Electronic Frontier Foundation	

State agencies

Commonwealth of Massachusetts, Operational Services Division	Office of the Illinois Attorney General
Maine Central Fleet Management	Office of the Maine Attorney General

Other stakeholders

American Property Casualty Insurance Association	National Association of Mutual Insurance Companies
CAR Coalition	National Automotive Security Task Force
Brian Daugherty, Liberty Advisors Group, Independent Automotive Consultant	National Cyber-Forensics & Training Alliance
Massachusetts Right to Repair Coalition	National Institute for Automotive Service Excellence
Mitchell1	National Institute of Standards and Technology

Source: GAO. | GAO-24-106633

To identify and describe NHTSA and FTC actions related to changes to competition and consumer choice in the vehicle repair market we reviewed relevant NHTSA and FTC documents, including reports and documents on FTC enforcement actions, and interviewed NHTSA and FTC staff.

We conducted this performance audit from February 2023 to March 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

List of Addressees

The Honorable Jan Schakowsky  
Ranking Member  
Subcommittee on Innovation, Data, and Commerce  
Committee on Energy and Commerce  
House of Representatives

We are sending copies of this report to the appropriate congressional committees, the Secretary of Transportation, the Chair of the Federal Trade Commission, and other interested parties.

GAO Contact Information

For more information, contact: Elizabeth Repko, Director, Physical Infrastructure Issues, repkoe@gao.gov, (202) 512-2834.  
  
Chuck Young, Managing Director, Public Affairs, YoungC1@gao.gov, (202) 512-4800.  
  
A. Nicole Clowers, Managing Director, Congressional Relations, ClowersA@gao.gov, (202) 512-4400.

**Staff Acknowledgments:** Nancy Lueke (Assistant Director), Matthew Rosenberg (Analyst-in-Charge), Melissa Bodeau, John Bornmann, Alicia Cackley, Mark Canter, Emily Crofford, Melanie Diemel, Kelley Dugan, Gary Guggolz, Kay Kuhlman, Terrence Lam, Rob Marek, Sam Portnow, and Pamela Snedden.

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.

Visit GAO on the web at <https://www.gao.gov>.

This work of the United States may include copyrighted material, details at <https://www.gao.gov/copyright>.

---

## Endnotes

<sup>1</sup>While relevant bills have been introduced in Congress, at the time of our review none had been enacted. Most recently, the Right to Equitable and Professional Auto Industry Repair Act (REPAIR Act) was introduced in the House of Representatives. This bill, if enacted, would require automakers to provide information and access to data needed for repairs to vehicle owners and independent repair shops. H.R. 906, 118th Cong. § 3(a)(1) (2023).

<sup>2</sup>2012 Mass. Acts Ch. 368.

<sup>3</sup>FTC, *Nixing the Fix: An FTC Report to Congress on Repair Restrictions* (Washington, D.C., May 2021).

<sup>4</sup>2020 Mass. Acts Ch. 386. Vehicle telematics systems provide continuous connectivity to long- and short-range wireless connections. They provide a broad range of features, including some supporting safety (such as the ability to report a crash), diagnostics (such as the ability to receive early alerts of mechanical issues), and convenience (such as hands-free access to driving directions or weather).

<sup>5</sup>Complaint, Alliance for Automotive Innovation v. Campbell, No. 1:20-cv-12090-DPW (Nov. 20, 2020).

<sup>6</sup>The 2014 Memorandum was signed by the Alliance of Automobile Manufacturers and Association of Global Automakers and, representing independent repair shops, the Automotive Aftermarket Industry Association and the Coalition for Auto Repair Equality. The 2023 commitment was signed by the Alliance for Automotive Innovation (which resulted from a merger between the Alliance of Automobile Manufacturers and Global Automakers) and, representing independent repair shops, the Automotive Services Association and the Society of Collision Repair Specialists.

<sup>7</sup>See Maine Citizens Guide to the Referendum Election, 37-40 (2023).

<sup>8</sup>Auto Care Association *Auto Care 2024 Factbook*. (Bethesda, MD, 2023).; Auto Care Association *Auto Care 2020 Factbook* (Bethesda, MD, 2019). The Auto Care Association is an association representing independent repair shops and other companies that support vehicle care. According to the Auto Care Association's estimates, the total vehicle aftercare market increased from about \$255 billion (nominal dollars) in 2014 to about \$360 billion (nominal dollars) in 2022.

<sup>9</sup>Dalal, Michal, IBIS World, *Auto Mechanics in the US*, Industry Report 81111 (April 2023).

<sup>10</sup>Auto Care Association *Auto Care 2024 Factbook* and *Auto Care 2020 Factbook*.

<sup>11</sup>Auto Care Association *Auto Care 2024 Factbook* and *Auto Care 2020 Factbook*. The Factbooks report data for a number of types of vehicle service centers and retailers, including some not likely to conduct vehicle repairs such as car washes and hardware stores. These data include both revenues for services such as repairs as well as for parts sales. For this report, for revenues we included the following categories that we believe are most likely to compete with dealerships: general automotive repair; exhaust system repair; transmission repair; other automotive electrical and mechanical repair and maintenance; body, paint, and interior repair and maintenance; glass replacement shops; all other automotive repair and maintenance; tire dealers; and warehouse clubs and supercenters. For our data on the number of locations we included: general repair, tire dealers, specialty repair, oil change and lubrication, and independent body shops. According to staff with the Auto Care Association, these data include the number of locations and, therefore, any independent repair shop with multiple locations will be represented by each location individually.

<sup>12</sup>National Automobile Dealers Association, *NADA Data 2022*.

<sup>13</sup>We interviewed a total of nine automaker stakeholders, which included eight automakers and one automaker association. We interviewed a total of 14 independent repair stakeholders, which included four independent repair shops and 10 associations.

---

<sup>14</sup>According to officials with the one automaker that does not now provide information to such third parties, the company is in the process of reaching agreements to do so.

<sup>15</sup>The purpose of NHTSA vehicle safety complaints is for consumers to raise issues related to vehicle safety, not repair issues.

<sup>16</sup>McKinsey & Company, *A Turning Point for US Auto Dealers: The Unstoppable Electric Car* (September, 2021).

<sup>17</sup>Cox Automotive, *Path to EV Adoption: Consumer and Dealer Perspectives* (June 2023).

<sup>18</sup>IBIS World, *Industry Report 81111: Auto Mechanics in the US* (April 2023).

<sup>19</sup>GAO, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack*, GAO-16-350 (Washington, D.C.: March 24, 2016).

<sup>20</sup>GAO-16-350.

<sup>21</sup>NHTSA, *Cybersecurity Best Practices for the Safety of Modern Vehicles*, (September 2022).

<sup>22</sup>FTC, *Nixing the Fix*.

<sup>23</sup>BMW of North America, Decision and Order, No. C-4555 (FTC Oct. 21, 2015).

<sup>24</sup>Specifically, among other things, the letters put the recipient on notice that the Magnuson-Moss Warranty Act prohibits warrantors of consumer products costing more than five dollars from conditioning their written warranties on a consumer's use of any article or service which is identified by brand, trade, or corporate name, unless provided to the consumer for free or the warrantor has been granted a waiver by the Commission. See 15 U.S.C. §§ 2301-2312.

<sup>25</sup>Auto Care Association *Auto Care 2024 Factbook*.

<sup>26</sup>We did not interview all identified entities. Some entities declined to meet with us and some entities did not respond to our requests for meetings.



# U.S. International Trade Commission (ITC)

Investigation No. 337-TA-1393

Certain Vehicle Telematics, Fleet Management, and Video-Based Safety  
Systems, Devices, and Components Thereof, Notice of Institution of  
Investigation

3/15/2024

a traditional religious site by practitioners. Tribal entities and other parties providing information on historic resources should designate information that they wish to be held as confidential and provide the reasons why BOEM should do so.

**Authority:** This notice of intent to prepare an EA is published pursuant to the National Environmental Policy Act, 42 U.S.C. 4321 *et seq.*, 40 CFR part 1500, and 43 CFR 46.305.

**Karen Baker,**  
*Chief, Office of Renewable Energy Programs,*  
*Bureau of Ocean Energy Management.*

[FR Doc. 2024-05699 Filed 3-15-24; 8:45 am]

BILLING CODE 4340-98-P

## INTERNATIONAL TRADE COMMISSION

[Investigation No. 337-TA-1393]

### Certain Vehicle Telematics, Fleet Management, and Video-Based Safety Systems, Devices, and Components Thereof, Notice of Institution of Investigation

**AGENCY:** U.S. International Trade Commission.

**ACTION:** Notice.

**SUMMARY:** Notice is hereby given that a complaint was filed with the U.S. International Trade Commission on February 9, 2024, under section 337 of the Tariff Act of 1930, as amended, on behalf of Samsara Inc. of San Francisco, California. A supplement to the complaint was filed on February 29, 2024. The complaint, as supplemented, alleges violations of section 337 based upon the importation into the United States, the sale for importation, and the sale within the United States after importation of certain vehicle telematics, fleet management, and video-based safety systems, devices, and components thereof by reason of the infringement of certain claims of U.S. Patent No. 11,190,373 ("the '373 patent"); U.S. Patent No. 11,127,130 ("the '130 patent"); and U.S. Patent No. 11,611,621 ("the '621 patent"). The complaint further alleges that an industry in the United States exists as required by the applicable Federal Statute.

The complainant requests that the Commission institute an investigation and, after the investigation, issue a limited exclusion order and a cease and desist order.

**ADDRESSES:** The complaint, except for any confidential information contained therein, may be viewed on the Commission's electronic docket (EDIS)

at <https://edis.usitc.gov>. For help accessing EDIS, please email [EDIS3Help@usitc.gov](mailto:EDIS3Help@usitc.gov). Hearing impaired individuals are advised that information on this matter can be obtained by contacting the Commission's TDD terminal on (202) 205-1810. Persons with mobility impairments who will need special assistance in gaining access to the Commission should contact the Office of the Secretary at (202) 205-2000. General information concerning the Commission may also be obtained by accessing its internet server at <https://www.usitc.gov>.

**FOR FURTHER INFORMATION CONTACT:** Pathenia M. Proctor, The Office of Unfair Import Investigations, U.S. International Trade Commission, telephone (202) 205-2560.

#### SUPPLEMENTARY INFORMATION:

**Authority:** The authority for institution of this investigation is contained in section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. 1337, and in section 210.10 of the Commission's Rules of Practice and Procedure, 19 CFR 210.10 (2023).

**Scope of Investigation:** Having considered the complaint, the U.S. International Trade Commission, on March 12, 2024, ordered that—

(1) Pursuant to subsection (b) of section 337 of the Tariff Act of 1930, as amended, an investigation be instituted to determine whether there is a violation of subsection (a)(1)(B) of section 337 in the importation into the United States, the sale for importation, or the sale within the United States after importation of certain products identified in paragraph (2) by reason of infringement of one or more of claims 15, 17, and 18 of the '373 patent; claims 1 and 5 of the '130 patent; and claims 1-5, 8-12, and 15-19 of the '621 patent, and whether an industry in the United States exists as required by subsection (a)(2) of section 337;

(2) Pursuant to section 210.10(b)(1) of the Commission's Rules of Practice and Procedure, 19 CFR 210.10(b)(1), the plain language description of the accused products or category of accused products, which defines the scope of the investigation, is "AI dashcams, vehicle gateways, and corresponding software";

(3) Pursuant to Commission Rule 210.50(b)(1), 19 CFR 210.50(b)(1), the presiding administrative law judge shall take evidence or other information and hear arguments from the parties or other interested persons with respect to the public interest in this investigation, as appropriate, and provide the Commission with findings of fact and a recommended determination on this issue, which shall be limited to the

statutory public interest factors set forth in 19 U.S.C. 1337(d)(1), (f)(1), (g)(1);

(4) For the purpose of the investigation so instituted, the following are hereby named as parties upon which this notice of investigation shall be served:

(a) *The complainant is:* Samsara Inc., 1 De Haro Street, San Francisco, CA 94107.

(b) The respondent is the following entity alleged to be in violation of section 337, and is the party upon which the complaint is to be served: Motive Technologies Inc., 55 Hawthorne Street, Suite 400, San Francisco, CA 94105.

(c) The Office of Unfair Import Investigations, U.S. International Trade Commission, 500 E Street SW, Suite 401, Washington, DC 20436; and

(5) For the investigation so instituted, the Chief Administrative Law Judge, U.S. International Trade Commission, shall designate the presiding Administrative Law Judge.

Responses to the complaint and the notice of investigation must be submitted by the named respondent in accordance with section 210.13 of the Commission's Rules of Practice and Procedure, 19 CFR 210.13. Pursuant to 19 CFR 201.16(e) and 210.13(a), as amended in 85 FR 15798 (March 19, 2020), such responses will be considered by the Commission if received not later than 20 days after the date of service by the complainant of the complaint and the notice of investigation. Extensions of time for submitting responses to the complaint and the notice of investigation will not be granted unless good cause therefor is shown.

Failure of the respondent to file a timely response to each allegation in the complaint and in this notice may be deemed to constitute a waiver of the right to appear and contest the allegations of the complaint and this notice, and to authorize the administrative law judge and the Commission, without further notice to the respondent, to find the facts to be as alleged in the complaint and this notice and to enter an initial determination and a final determination containing such findings, and may result in the issuance of an exclusion order or a cease and desist order or both directed against the respondent.

By order of the Commission.

Issued: March 12, 2024.

**Lisa Barton,**  
*Secretary to the Commission.*

[FR Doc. 2024-05660 Filed 3-15-24; 8:45 am]

BILLING CODE 7020-02-P

# Department of Commerce

Bureau of Industry and Security

15 CFR Part 791

[Docket No. 240919-0245]

Securing the Information and Communications Technology and Services  
Supply Chain: Connected Vehicles

Notice of proposed rulemaking

9/26/2024

**DEPARTMENT OF COMMERCE**

**Bureau of Industry and Security**

**15 CFR Part 791**

[Docket No. 240919–0245]

RIN 0694–AJ56

**Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles**

**AGENCY:** Bureau of Industry and Security, Department of Commerce.

**ACTION:** Notice of proposed rulemaking.

**SUMMARY:** In this notice of proposed rulemaking (NPRM), the Department of Commerce's (Department) Bureau of Industry and Security (BIS) proposes a rule to address undue or unacceptable risks to national security and U.S. persons posed by classes of transactions involving information and communications technology and services (ICTS) that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of certain foreign adversaries, and which are integral to connected vehicles, as defined herein. BIS is soliciting comment on this proposed rule, which builds on the advance notice of proposed rulemaking (ANPRM) issued by BIS on March 1, 2024.

**DATES:** Comments to this proposed rule must be received on or before October 28, 2024.

**ADDRESSES:** All comments must be submitted by one of the following methods:

- *By the Federal eRulemaking Portal:* <http://www.regulations.gov> at docket number BIS–2024–0005.

- *By email directly to:* [connectedvehicles@bis.doc.gov](mailto:connectedvehicles@bis.doc.gov). Include "RIN 0694–AJ56" in the subject line.

- *Instructions:* Comments sent by any other method, to any other address or individual, or received after the end of the comment period, may not be considered. For those seeking to submit confidential business information (CBI), please clearly mark such submissions as CBI and submit by email, as instructed above. Each CBI submission must also contain a summary of the CBI, clearly marked as public, in sufficient detail to permit a reasonable understanding of the substance of the information for public consumption. Such summary information will be posted on [regulations.gov](https://www.regulations.gov). Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be considered.

- The Regulatory Impact Analysis is available at <http://www.regulations.gov> at docket number BIS–2024–0005.

**FOR FURTHER INFORMATION CONTACT:**

Marc Coldiron, U.S. Department of Commerce, telephone: (202) 482–3678. For media inquiries: Jessica Stallone, Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce: [OCA@bis.doc.gov](mailto:OCA@bis.doc.gov).

**SUPPLEMENTARY INFORMATION:**

**I. Background**

In this notice, BIS solicits comment on a proposed rule to prohibit transactions involving Vehicle Connectivity System (VCS) hardware and covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China, including the Hong Kong Special Administrative Region (PRC), or the Russian Federation (Russia). It follows an advance notice of proposed rulemaking (ANPRM), 89 FR 15066 (Mar. 1, 2024), in which BIS sought public comment to inform a rulemaking that would address the undue or unacceptable risks, as identified in Executive Order (E.O.) 13873, "Securing the Information and Communications Technology and Services Supply Chain," 84 FR 22689 (May 17, 2019), posed by a class of transactions that involve information and communications technology and services (ICTS) designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary and integral to Connected Vehicles.

In E.O. 13873, the President delegated to the Secretary of Commerce (Secretary), to the extent necessary to implement the order, the authority granted under the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701, *et seq.*), "to deal with any unusual and extraordinary" foreign threat to the United States' national security, foreign policy, or economy, if the President declares a national emergency with respect to such threat. 50 U.S.C. 1701(a). In E.O. 13873, the President declared a national emergency with respect to the "unusual and extraordinary" foreign threat posed to the ICTS supply chain and has, in accordance with the National Emergencies Act (NEA), extended the declaration of this national emergency in each year since E.O. 13873's publication. *See Continuation of the National Emergency With Respect*

*to Securing the Information and Communications Technology and Services Supply Chain*, 85 FR 29321 (May 14, 2020); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain*, 86 FR 26339 (May 13, 2021); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain*, 87 FR 29645 (May 13, 2022); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain*, 88 FR 30635 (May 11, 2023); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain*, 89 FR 40353 (May 9, 2024).

Specifically, the President identified the "unrestricted acquisition or use in the United States of ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries" as "an unusual and extraordinary" foreign threat to the national security, foreign policy, and economy of the United States that "exists both in the case of individual acquisitions or uses of such technology or services, and when acquisitions or uses of such technologies are considered as a class." *See* E.O. 13873, and 50 U.S.C. 1701(a)–(b).

Once the President declares a national emergency, IEEPA empowers the President to, among other acts, investigate, regulate, prevent, or prohibit, any "acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States." 50 U.S.C. 1702(a)(1)(B).

To address the identified risks to national security from ICTS transactions, the President in E.O. 13873 imposed a prohibition on transactions determined by the Secretary, in consultation with relevant agency heads, to involve foreign adversary ICTS and to pose certain risks to U.S. national security, technology, or critical infrastructure. Specifically, to fall within the scope of the prohibition, the Secretary must determine that a transaction: (1) "involves [ICTS]

designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary," defined in E.O. 13873 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 United States persons;" and (2):

A. "Poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;"

B. "Poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States;" or

C. "Otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons."

These factors are collectively referred to as "undue or unacceptable risks." Further, E.O. 13873 grants the Secretary the authority to design or negotiate mitigation measures that would allow an otherwise prohibited transaction to proceed. E.O. 13873 section 1(b).

The President also delegated to the Secretary the ability to promulgate regulations that, among other things, establish when transactions involving particular technologies may be categorically prohibited. E.O. 13873 section 2(a)–(b); *see also* 3 U.S.C. 301–02. Specifically, the Secretary may issue rules establishing criteria, consistent with section 1 of E.O. 13873, by which particular technologies or market participants may be categorically included in or categorically excluded from prohibitions established pursuant to E.O. 13873.

## II. Introduction

Today's vehicles contain a myriad of connected components that provide greater convenience for consumers and increase road safety for both drivers and pedestrians, such as Wi-Fi, Bluetooth, cellular, and satellite connectivity. However, the incorporation of progressively more complex hardware and software systems that facilitate these features has also increased the attack surfaces through which malign actors may exploit vulnerabilities to gain access to a vehicle. As BIS outlined in its March 1, 2024, ANPRM, certain ICTS integral to Connected Vehicles could present an undue or unacceptable risk to U.S. national security when those

systems are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.

In the *Securing the Information and Communications Technology and Services Supply Chain* interim final rule, 86 FR 4909 (January 19, 2021), the Secretary determined that certain foreign governments or foreign non-government persons including the PRC, Republic of Cuba, Islamic Republic of Iran, Democratic People's Republic of Korea, Russia, and Venezuelan politician Nicolás Maduro constitute foreign adversaries for purposes of E.O. 13873 and rules promulgated pursuant to E.O. 13873. *See* 15 CFR 791.4 (to the extent that the list of foreign adversaries identified in 15 CFR 791.4 is updated to add or remove governments or non-government persons, this proposed rule intends to reflect the most up-to-date designations of foreign adversaries). Additionally, E.O. 13873 provides that the Secretary may issue rules that identify particular technologies or countries with respect to which transactions involving ICTS warrant particular scrutiny. E.O. 13873 2(b). For the purposes of this proposed rule regarding transactions involving ICTS integral to Connected Vehicles, BIS is focusing its regulatory efforts on ICTS that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. BIS has identified that, for the purposes of addressing the national security risks posed by Connected Vehicles, these two foreign adversaries pose particular risks to U.S. national security because of their legal, political, and regulatory regimes, combined with their current and anticipated growth and involvement in the automotive sector, to include Connected Vehicles. However, BIS specifically seeks public comment on whether the other identified foreign adversaries pose similar risks to U.S. national security in the connected vehicle supply chain.

The PRC and Russia are able to leverage domestic legislation and regulatory regimes to compel companies subject to their jurisdiction, including carmakers and their suppliers, to cooperate with security and intelligence services. Such control over companies and their products and services means that equipment is easily exploitable by PRC and Russian authorities. The privileged access that the PRC and Russia may gain to Connected Vehicles through their components, including software, could enable those foreign adversaries to exfiltrate sensitive data

collected by connected vehicles and, potentially, allow remote access and manipulation of connected vehicles driven by U.S. persons. Pursuant to E.O. 13873, BIS has determined that certain classes of transactions that facilitate the exfiltration of data and remote manipulation of connected vehicles pose undue or unacceptable risks to U.S. national security and the safety and security of U.S. persons.

### a. Overview of Proposed Rule

To address these identified undue or unacceptable risks, BIS is proposing regulations that would, absent a General or Specific Authorization, (1) prohibit VCS Hardware Importers from knowingly importing into the United States certain hardware for VCS ("VCS Hardware," as further defined below); (2) prohibit connected vehicle manufacturers from knowingly importing into the United States completed connected vehicles incorporating certain software that supports the function of VCS or ADS (VCS and ADS software are collectively referred to herein as "covered software," as further defined below); (3) prohibit connected vehicle Manufacturers from knowingly Selling within the United States completed connected vehicles that incorporate covered software; and (4) prohibit connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia from knowingly selling in the United States completed connected vehicles that incorporate VCS hardware or covered software. The prohibitions would apply when such VCS hardware or covered software is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

If, following consideration of comments received on this proposed rule, BIS issues a final rule to adopt the proposal, that final rule would take effect 60 days after publication in the *Federal Register*. However, VCS Hardware Importers would be permitted to engage in otherwise Prohibited Transactions involving VCS Hardware and exempt from certain requirements so long as: (1) for VCS Hardware not associated with a Model Year, the import of the VCS Hardware takes place prior to January 1, 2029; or (2) the VCS Hardware unit is associated with a vehicle Model Year prior to 2030 or the VCS Hardware is integrated into a connected vehicle (completed or incomplete) with a Model Year prior to 2030. connected vehicle manufacturers would be permitted to engage in

otherwise prohibited transactions involving covered software and exempt from certain requirements, so long as the completed connected vehicle that is imported, or sold within the United States, is of a model year prior to 2027. connected vehicle Manufacturers that are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia would be permitted to sell completed connected vehicles with a model year prior to 2027 that incorporate VCS hardware or covered software.

BIS is also proposing to implement several mechanisms to facilitate compliance with these prohibitions: (1) Declarations of Conformity submitted to BIS by VCS hardware importers and connected vehicle manufacturers to confirm that they are not engaging in prohibited transactions involving VCS hardware or covered software, as defined herein; (2) Advisory opinions to allow VCS hardware importers and connected vehicle manufacturers to seek guidance from BIS on whether a prospective transaction may be prohibited; (3) General authorizations to allow certain VCS hardware importers and connected vehicle manufacturers to engage in otherwise prohibited transactions without the need to notify BIS prior to the prohibited activity if they qualify under stated conditions; (4) Specific authorizations which, following an application to and approval by BIS, grant VCS hardware importers and connected vehicle manufacturers the ability to engage in otherwise prohibited transactions, including because the associated undue or unacceptable risks have been, or can be, mitigated; and (5) A process to inform VCS hardware importers and connected vehicle manufacturers that a specific authorization may be required because an activity could constitute a Prohibited Transaction.

This proposed rule benefits from the responses received during the public comment period for the ANPRM and incorporates significant portions of that feedback. For example, BIS considered public feedback to define the scope of connected vehicles, identify ICTS integral to Connected Vehicles, and better understand the effects of any potential prohibition. Determining the scope of the prohibitions outlined in this proposed rule required balancing the need to address the undue or unacceptable risk posed by foreign adversary involvement in the connected vehicles supply chain with the impact on the public and industry.

### III. Comments on the Advance Notice of Proposed Rulemaking

On March 1, 2024, the Department published in the *Federal Register* an ANPRM, 89 FR 15066, pursuant to the authority the President delegated to the Secretary in E.O. 13873. The purpose of the ANPRM was to solicit stakeholder feedback and to gather information to further BIS's consideration of a proposed rule to address any undue or unacceptable risks to U.S. national security posed by ICTS used in connected vehicles, when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Specifically, BIS sought public input on certain definitions, capabilities of connected vehicles that may increase the likelihood of vulnerabilities, and consequences to U.S. persons and critical infrastructure if these vulnerabilities are exploited by a foreign adversary. BIS also solicited input on the ICTS most integral to connected vehicles and most vulnerable to compromise, as well as input on mechanisms to address identified risks through potential design, implementation standards and protocols, manufacturing integrity protection systems and procedures, or prohibitions.

BIS received 57 comment submissions in response to the ANPRM, from original equipment manufacturers (OEMs), component suppliers, two foreign governments, nonprofit organizations, and individuals. Five comments contained CBI, and one comment was retracted at the request of the commenter. Each of the comments is available on the public rulemaking docket at <https://www.regulations.gov>.

In general, commenters expressed agreement with BIS on the overall risks posed by compromised ICTS in Connected Vehicles, as outlined in the ANPRM. Commenters were also generally aligned on the need for further clarity on what would constitute a person "owned by, controlled by, or subject to the jurisdiction or direction" of a foreign adversary, the challenge of implementing due diligence requirements due to the complexity of the global automotive supply chain, the need for substantial lead time to implement a regulation given the difficulty of sourcing alternative suppliers, the breadth and depth of data collected by ICTS integral to Connected Vehicles, and the potential negative impact such a regulation could have on long-term U.S. innovation, competitiveness, and health and safety.

On the other hand, commenters disagreed on a number of issues, including the ICTS most integral to connected vehicles, the level of risk that may be posed by transactions involving the identified connected vehicle systems, the definition of connected vehicle, and approaches for how the proposed rule could be most effective in risk mitigation.

Below, BIS addresses in more detail the key issues raised by the comments received and describes how they were considered and, where applicable, addressed in the proposed rule.

#### a. Definitions

In the ANPRM, BIS sought comments on the definition of the term "connected vehicle," proposing to define it as "an automotive vehicle that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device." Commenters offered differing views on BIS's proposed definition with some, but not all, commenters agreeing that it appropriately captured the platform BIS seeks to regulate.

Commenters that disagreed with BIS's proposed definition offered several reasons. For example, many commenters viewed the term as overly broad and noted that it failed to identify the specific types of vehicles that would be captured by a regulation (e.g., commercial, industrial, agricultural, rolling stock). Commenters also noted that the phrase "connected vehicle" is an existing term of art within the automotive industry referring to vehicles with external communication capabilities, particularly in short-range communication. As an alternative, some commenters suggested that BIS adopt the term "networked vehicle" to capture the ability of a vehicle to communicate with networks or devices external to a vehicle while others suggested the term "software-defined vehicles" which would encompass the technologies and capabilities outlined in the ANPRM's proposed connected vehicle definition while also capturing internal software capabilities for functions within a vehicle beyond communication (e.g., starting a vehicle, malfunction checks, navigation).

After full consideration of each of the comments, BIS maintains the use of the term "connected vehicle" in the proposed rule. However, BIS proposes to narrow its definition to mean, "[a] vehicle driven or drawn by mechanical

power and manufactured primarily for use on public streets, roads, and highways, that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device. Vehicles operated only on a rail line are not included in this definition.” This definition captures the vehicles that would be subject to the rule (e.g., passenger vehicles, motorcycles, buses, small and medium trucks, class 8 commercial trucks, recreational vehicles), while excluding those that pose a less acute risk of data exfiltration, modification, or sabotage by foreign adversaries. BIS further believes that the term connected vehicle, as defined in this proposed rule, will capture future trends in vehicle development, particularly as software comes to play a larger role in vehicle operation. BIS emphasizes its belief that, with very few exceptions, all new vehicles sold in the United States will be captured by this definition. BIS seeks comment on this assessment. In the interest of issuing a rule that is narrow, yet also would address the risks posed by connected vehicles, BIS declines to extend this definition to all “rolling stock” or unmanned aerial vehicles as suggested by some comments, although BIS does not preclude the possibility of addressing these vehicles in future regulation. BIS believes that these sectors, to include vehicles operating on a rail line, are materially different from the connected vehicle sector as defined by this proposed rule, and capturing these vehicles in a regulation primarily targeting wheeled on-road vehicles could lead to unintended consequences and supply chain disruption.

A subset of commenters requested further clarity on what would constitute an entity “subject to the jurisdiction or direction” of a foreign adversary and expressed concerns that foreign subsidiaries of U.S. businesses or foreign nationals working in the United States would potentially be captured by this term. Others suggested that BIS should ensure that the subsidiaries of companies located in foreign adversary countries are captured by the proposed rule, even when the subsidiaries are located in third countries outside the United States that are not foreign adversaries, but supply entities within the United States.

After full consideration of the comments, BIS has adopted the definition of a “person owned by, controlled by, or subject to the

jurisdiction or direction of a foreign adversary” to mean, (a) any person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary; (b) any person, wherever located, who is a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, and is not a United States citizen or permanent resident of the United States; (c) any corporation, partnership, association, or other organization with a principal place of business in, headquartered in, incorporated in, or otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary; or (d) any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs (a) through (c) possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity. BIS has also provided, below in Section V, numerous non-exhaustive examples to explain how this term will apply in various representative situations.

#### *b. ICTS Supply Chain for Connected Vehicles*

In the ANPRM, BIS sought comments on “the ICTS supply chain for Connected Vehicles in the United States,” in order to better understand the role played by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries within it. Public comments broadly discussed the ICTS incorporated into Connected Vehicles and noted the difficulty that manufacturers and suppliers may face in conducting supply chain due diligence for the purposes of complying with any potential final rule. Submissions explained the complexity of ICTS systems contained within Connected Vehicles and outlined several categories of technologies incorporated into Connected Vehicles,

including microcontrollers, applications processors, analog products (e.g., power management integrated circuits and transceiver physical layers), automotive software operating systems (OS), automotive vision, light detection and ranging (LiDAR) systems, radar, and other application software systems. Many commenters who identified as OEMs also noted that they do not always know the source of all inputs from hardware and software suppliers, making conducting due diligence beyond tier one and tier two suppliers particularly difficult. Moreover, submissions highlighted that suppliers are often capable of updating the firmware on their components independently of an OEM, further complicating efforts to understand which entities have access to software and when such access occurs.

The comments received on this topic highlight the depth and complexity of connected vehicle supply chains, indicating that it is not always clear to OEMs which suppliers have access to connected vehicle software and when they have access to it. As some commenters pointed out, some of these technologies and their associated supply chains are still in development and will grow even more complex as the industry develops. Such existing and growing complexity, coupled with the likelihood of ICTS that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary being incorporated into connected vehicles, demonstrates the need for regulation to protect U.S. national security. Such regulation will also incentivize greater supply chain transparency for not only existing supply chains but also for developing supply chains. To facilitate compliance, the rule would include a delayed implementation timeline so that industry can adjust their existing supply chains and plans for future supply chains. BIS is not currently proposing specific due diligence requirements. Instead, VCS hardware importers and connected vehicle manufacturers are given flexibility to provide evidence of compliance efforts tailored to their unique operations. Such efforts could include using third-party researchers or independently conducting supply chain diligence.

Several commenters raised a variety of potential trade-related concerns relating to this proposed rulemaking and other recent U.S. government actions related to automotive trade involving the PRC. While some commenters explicitly advocated for exclusionary tariffs on the import of all

PRC vehicles into the United States, others cautioned BIS to avoid creating unnecessary trade barriers when crafting a proposed rule. One commenter specifically warned that BIS regulation of connected vehicle software could amount to a digital trade barrier and urged BIS to avoid certain policies such as data localization requirements, digital service taxes, or forced code inspection. BIS underscores the U.S. government's commitment to the trusted and secure flow of data across borders. This proposed rule seeks to narrowly address, pursuant to E.O. 13873, the acute national security concerns posed by certain foreign adversary ICTS in connected vehicle supply chains while minimizing any unnecessary disruptions in manufacturing and trade. BIS has drafted this proposed rule irrespective of any other automobile-related trade actions taken by the U.S. government.

#### *c. ICTS Most Integral to Connected Vehicles and Their Capabilities*

In its ANPRM, BIS identified six systems (*i.e.*, vehicle operating systems (OS), telematics systems, Advanced Driver-Assistance System (ADAS), Automated Driving Systems (ADS), satellite or cellular telecommunications systems, and battery management systems (BMS)) that it was considering identifying as the ICTS in Connected Vehicles most likely to present undue or unacceptable risks if exploited by foreign adversaries. BIS requested comment on the levels of risk associated with these various ICTS as well as any additional ICTS that commenters might consider integral to Connected Vehicles.

Commenters held differing views on which ICTS are integral to connected vehicles and should be captured by the scope of a rule. For example, whereas some commenters noted that ADAS present a low risk of data exfiltration given that these systems often lack direct external connectivity, others noted that such systems may nevertheless be indirectly connected to external devices and systems (*e.g.*, microcontrollers), thus offering indirect access to the data they collect. As another example, while many commenters identified LiDAR systems as a concern, there was disagreement about the nature of the vulnerability posed by these systems. Some commenters noted that LiDAR systems could be manipulated to cause grave harm (*e.g.*, to ignore pedestrians) given their instrumental role in vehicle guidance. However, BIS's further technical analysis found that LiDAR generally lacks the ability to transmit from the vehicle and does not, as a

standalone system, control the vehicle. Importantly, BIS notes that in many cases, ADS exerts control over both LiDAR and the vehicle and thus presents a higher risk. Other commenters pointed to the growing role of mobile applications that allow drivers to access and control core functions of the vehicle remotely (*e.g.*, keyless driving). A number of commenters also highlighted concerns related to aftermarket connected devices. These devices, which often feature some forms of connectivity, are introduced to the vehicle after manufacture and sale and may contain vulnerabilities over which OEMs have little to no oversight.

Several submissions expressed a desire for BIS to tailor any regulation as narrowly as possible, arguing that BIS should focus only on those systems with direct connectivity to the connected vehicle or the ability to transmit from the connected vehicle. Some commenters pointed specifically to devices that connect to a vehicle's controller area network (CAN) bus as posing a specific cybersecurity risk. Others recommended that BIS should critically examine electric vehicle charging infrastructure and associated technologies due to a potential risk of exploitation by foreign adversaries. A few OEM commenters ascribed the highest level of potential risk to "finished" or "vertically integrated" vehicles from suppliers with a foreign adversary nexus that are operating in the United States. One commenter pointed to ICTS components inside safety-critical systems (*e.g.*, braking systems, steering systems, traction systems, battery-charging and management systems, airbag systems) as posing greater levels of potential risk. On the other hand, some commenters recommended that BIS should aim to address the widest possible aperture of risk by regulating a wide variety of the technologies enumerated in the ANPRM along with additional technology categories (*e.g.*, microcontrollers, analog products).

Following consideration of these comments, BIS is proposing a rule that aims to strike a balance between minimizing supply chain disruptions and the need to address the national security risks posed by Connected Vehicles. BIS proposes to achieve this balance by focusing the rule only on those systems that most directly facilitate the transmission of data both into and from the vehicle, rather than focusing on all systems. Therefore, BIS is proposing to regulate transactions involving two systems of ICTS integral to connected vehicles, VCS and ADS. As further discussed below, in many cases,

these systems serve as controllers for subordinate systems within the Connected Vehicle, like those highlighted in the ANPRM, making them a target for exploitation related to data exfiltration or remote vehicle manipulation. After reviewing comments, BIS has determined that aftermarket telematics devices, including fleet tracking devices and systems, that fulfill functions consistent with the definition of VCS hardware are covered by this proposed rule.

Additionally, the proposed rule does not cover ICTS with the function of enabling the transmission, receipt, conversion, or processing of radio frequency communications at a frequency below 450 megahertz. Setting such a threshold enables BIS to capture those ICTS that pose a higher risk due to their connectivity and transmission functions, while lowering compliance burden by excluding from regulation those ICTS with functions that pose a lower risk and offer high utility to consumers (*e.g.*, tire pressure monitoring systems, electronic key fobs).

For similar reasons, BIS ultimately chose to exclude other systems highlighted in the ANPRM—such as OS, ADAS, or BMS—from this proposed rule unless they have VCS components and fall within the proposed rule's definition of VCS hardware. For example, automotive software systems like BMS and automotive OS do not have their own connectivity, and require communication through a VCS, thereby making VCS a more effective focus for rulemaking. BMS traditionally do not have their own external wireless data link and instead rely on VCS for wireless communication through a VCS. Likewise, automotive OS software, which generally resides on an in-vehicle infotainment unit or centralized head unit, are characterized by a wide diversity in architecture, design, and supply chain among OEMs while also generally lacking their own data link, instead relying on communication through a VCS. Given how these systems are typically placed within connected vehicles and the ways in which they achieve connectivity, BIS has chosen to focus on the systems that ultimately facilitate the transmission of data both to and from the vehicle as opposed to these subordinate systems.

Additionally, to reduce unnecessary economic impacts and supply disruption, BIS is proposing to regulate ADS software rather than the hardware components of ADAS and ADS. The hardware that enables ADAS and ADS varies widely between different OEMs. In contrast, the hardware that enables



VCS are relatively consistent across different automotive architectures and designs. ADAS and ADS hardware encompasses a wide variety of different sensors, distributed electronic control units (ECUs), centralized computing units, actuators, and signaling units, among others. These sensors and internal vehicle networking hardware rarely have independent connectivity. Most, if not all, scalable cybersecurity vulnerabilities to these systems are achieved by connectivity through VCS systems. A rule that coherently and feasibly addresses these varied supply chains would have disproportionate economic and supply chain impacts relative to the reduction of national security risks. Further, focusing on the ADS software supply chain appropriately mitigates the national security risks that they present while limiting the supply chain and economic impact. While BIS recognizes that the scope of data captured by connected automotive systems is vast and that multiple systems may pose national security risks, as discussed above, it has decided to focus its current efforts on VCS hardware and covered software. However, BIS does not foreclose the possibility of further addressing other systems, including additional aspects of VCS and ADS, in future regulation. BIS therefore also specifically seeks comment on its determination that VCS and ADS are automotive ICTS integral to Connected Vehicles and pose the greatest and most addressable national security risk, and on its decision to focus this rule on those systems. BIS also specifically seeks comment on whether any risks posed by other connected vehicle ICTS should also be addressed in this rule.

#### *d. Cybersecurity Best Practices*

In the ANPRM, the Department requested comments regarding cybersecurity concerns with the connected vehicle supply chain, as well as standards, best practices, and norms that are relied upon and built up by the connected vehicle industry. Commenters largely emphasized that OEMs dedicate significant resources to bolstering the cybersecurity of connected vehicle systems in addition to following or conforming to relevant, established best practices and standards. Some commenters referenced work by vehicle manufacturers to deploy advanced encryption techniques as well as the importance of conducting thorough testing on connected vehicle systems and components, to include penetration testing, fuzz testing, and static code analysis. Others identified specific techniques and best practices,

including role-based access controls. Among the best practices and standards most referenced by commenters were the National Highway Traffic Safety Administration's (NHTSA) Cybersecurity Best Practices for the Safety of Modern Vehicles, International Organization for Standardization's (ISO) and SAE International's standard ISO/SAE 21434, Institute of Electrical and Electronics Engineers Standards Association's (IEEE) standard IEEE 1609.2, SAE J3061, and SAE J3161. At the international level, commenters also referenced the United Nations Economic Commission for Europe (UNECE) Regulations 155 (R155) and R156, which address whole-of-vehicle and software update cybersecurity, respectively. One commenter encouraged BIS to pay particular attention to R155 and R156 given the standards' mandatory coverage in UNECE member states and their ability to provide common best practices to vehicle manufacturers globally.

Many commenters underscored that security is a shared responsibility between OEMs and cloud service providers (CSPs), explaining that while CSPs manage the infrastructure layer, CSP customers are responsible for implementing appropriate configurations and controls in the cloud to protect their data. Commenters also emphasized that practices for automotive cloud security and cloud data access vary between OEMs and according to the specific contractual terms between the OEM and CSP. Some submissions pointed to ISO's and International Electrotechnical Commission's (IEC) standard ISO/IEC 27001 and third-party certifications and attestations, such as the Cloud Security Alliance Cloud Controls Matrix, as models for cloud security best practices and standards. With regard to electric vehicle charging infrastructure, commenters pointed to ISO 15118, National Institute of Standards and Technology's (NIST) Internal Report (IR) 8473, and German technical specification DIN 70121, but they emphasized that specific practices vary according to OEM due to differing battery types and configurations.

BIS acknowledges that cybersecurity standards and best practices, particularly many of those mentioned in submissions, serve a crucial function in promoting the safety and security of vehicles. While BIS generally encourages the use of cyber security standards and best practices, BIS also acknowledges that no standard BIS is aware of or that was identified in comments—either currently in effect or under development—would sufficiently

mitigate the undue or unacceptable risks posed by foreign adversary involvement in connected vehicle ICTS supply chains as described in this proposed rule, even if widely adopted by industry. The standards and guidance BIS reviewed are primarily focused on hardening automotive systems from external access. Standards and guidance alone are insufficient to address risks from within the supply chain, as the systems are not, and cannot be hardened against the OEM or tier 1 and 2 suppliers that have or maintain privileged access to them. As a result, BIS is not proposing to adopt cybersecurity standards and best practices as part of the rule but may consider the scope and nature of their adoption on a case-by-case basis as part of the Specific Authorizations process described in greater detail below.

#### *e. Authorizations and Mitigations*

In the ANPRM, BIS sought comment on processes and mechanisms that BIS could implement to authorize an otherwise prohibited transaction with the adoption of mitigation measures. Commenters were generally aligned regarding authorizations and potential mitigation schemes. Several commenters requested that BIS adopt (1) an advisory opinion program for connected vehicles; (2) a trusted trader program to simplify compliance and avoid the complexity and uncertainty associated with a licensing regime; and (3) a program allowing OEMs and suppliers to self-certify compliance with the regulation. BIS has considered each of the comments in full and is proposing an advisory opinion program; procedures for VCS hardware importers and connected vehicle manufacturers to submit Declarations of Conformity, which allow OEMs and suppliers to self-certify their compliance with the regulation; as well as procedures for VCS hardware importers and connected vehicle manufacturers to determine eligibility for a General Authorization or apply for a Specific Authorization. BIS is not proposing a trusted trader program at this time because of the complexity, scale, and opacity of existing connected vehicle supply chains, but may consider establishing such a program to facilitate compliance as supply chains evolve and welcomes comment on such a program as well as any other alternate compliance mechanisms.

A significant portion of commenters raised and rejected data localization requirements as a potential solution to the data exfiltration concerns associated with connected vehicles. Instead, many argued that data exfiltration concerns

could instead be mitigated by securing a demonstrated commitment to privacy and security from OEMs and suppliers, primarily through the adoption of industry cybersecurity best practices and standards. Some commenters also pointed to company membership in the Automotive Information Sharing and Analysis Center (Auto-ISAC) as another method for entities to demonstrate commitment to cybersecurity best practices. As discussed above, BIS has opted not to require adherence to any specific standard or best practice as a prerequisite to securing an authorization to engage in an otherwise prohibited transaction, but BIS reserves the right to consider compliance with them on a case-by-case basis in conjunction with other potential mitigations.

#### *f. Economic Impacts*

Comments generally agreed that prohibitions affecting a major supplier of a component used in Connected Vehicles could result in negative economic outcomes. Commenters raised several concerns, including increased manufacturing costs for U.S. auto manufacturers that would likely be passed onto consumers; a decline in long-term U.S. competitiveness vis-à-vis foreign auto manufacturers; disincentivizing further investment in connected vehicles and autonomous vehicle research and development (R&D), potentially reducing future employment in the U.S. auto industry; and a decline in the safety and quality of connected vehicles available to U.S. consumers. Several commenters also noted that regulation may have an outsized impact on small businesses, which often lack the due diligence and compliance resources of their larger competitors. To mitigate these outcomes, several commenters requested substantial lead time for manufacturers to identify and source from alternative suppliers. Lastly, multiple submissions emphasized that not all components in connected vehicles produced by entities owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary necessarily pose a cybersecurity or national security risk, especially for components with minimal or no connectivity capability.

Following consideration of these comments, BIS proposes to allow (1) until Model Year 2027, for connected vehicle manufacturers to come into compliance for transactions involving covered software, (2) until model year 2030, or January 1, 2029, for VCS hardware importers to come into compliance for transactions involving VCS hardware; and (3) until model year

2027 for connected vehicle manufacturers that are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia to sell connected vehicles with VCS hardware and/or covered software. Moreover, to address concerns about the resources small businesses are able to devote to compliance, BIS is proposing a general authorization that would permit certain small businesses to engage in otherwise prohibited transactions. BIS also emphasizes that this rule would narrowly target the specific automotive systems that pose the greatest risk when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of certain foreign adversaries. As such, the rule would not broadly prohibit the import of connected vehicle technologies from foreign adversary nations, nor would it require market participants to alter supply chains for low-risk or unconnected components.

BIS believes that the implementation timeline strikes an appropriate balance between minimizing significant disruptions to the connected vehicles supply chain and mitigating the national security risk posed by foreign adversary involvement in the connected vehicles supply chain. Given the relatively limited amount of foreign adversary linked hardware and software in U.S. vehicles today, the software prohibitions proposed in this rule would address the most immediate threats to U.S. national security while allowing industry time to come into compliance with the prohibitions on VCS Hardware.

#### **IV. Risks Associated With Vehicle Connectivity Systems and Automated Driving Systems When Designed, Developed, Manufactured, or Supplied by Persons Owned by, Controlled by, or Subject to the Jurisdiction or Direction of the PRC and Russia**

Following consideration of comments received on the ANPRM, and further consideration of the risks and vulnerabilities associated with various ICTS components that are critical to the operation of CVs, BIS proposes to focus its rule on two integral ICTS systems—VCS and ADS—when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of two foreign adversary entities—the PRC and Russia. Below, BIS further explains its understanding of the undue and unacceptable risks associated with these particular systems, and these particular foreign adversaries, and seeks public comment on the systems and foreign

adversaries addressed in the proposed rule.

#### *a. Vulnerabilities Associated With Vehicle Connectivity Systems and Automated Driving Systems*

##### **1. Vehicle Connectivity Systems**

The term VCS encompasses hardware and software systems—such as the telematics control unit (TCU), cellular modems and antennas, and other automotive components—that integrate various radio frequency communication technologies and enable Connected Vehicles to access external data sources, facilitate vehicle-to-vehicle communication, and provide enhanced services to users through seamless connectivity options. For example, as the primary automotive VCS component, a TCU acts as the primary interface between the internal network and external communication channels. It collects data from onboard sensors such as GPS, accelerometers, gyroscopes, BMS, and other ECUs via wired networks like CAN bus, LIN, FlexRay, Automotive Ethernet, K-Line, as well as wireless protocols such as Bluetooth and Wi-Fi. Some systems use cameras and microphones to facilitate facial recognition of drivers, or to respond to voice commands of drivers. Once gathered, the TCU converts this internal data into radio frequency signals suitable for transmission over the chosen wireless protocol. In other words, as the vast array of sensors on a connected vehicle collect information about a driver's location, speed, voice patterns, battery state of charge, or other vehicle diagnostic and operational information, the TCU converts that data into a format that can be transmitted to systems outside the vehicle and then enables that transmission.

While the increased degree of vehicle connectivity offers benefits to both consumers and manufacturers, it also increases risks to consumers and manufacturers due to the number of access points into the internal vehicle network, each of which may present multiple new software vulnerabilities for adversaries to exploit. See National Renewable Energy Laboratory, "Vehicle Cybersecurity Threats and Mitigation Approaches," (Aug. 2019), <https://www.nrel.gov/docs/fy19osti/74247.pdf>. Such compromise of VCS software could occur at various points of the software development lifecycle, including tool development, source code repositories, open-source dependencies, software updates, and shipment interdiction. For instance, Upstream's 2024 Global Automotive Cybersecurity Report documented a case

where security researchers installed malicious software on the VCS by performing a simulated jailbreak attack of an OEM's VCS using a voltage fault injection on the chip-maker's processor. This malicious software unlocked vehicle manipulating features such as acceleration and heated seats, provided access to private user data such as a user's phonebook and calendar entries, and enabled decryption of encrypted Non-Volatile Memory Express (NVMe) storage, manipulation of the car's identity, and extraction of the vehicle-unique credential used for authenticating and authorizing the OEM's internal service network. *See Upstream, 2024 Global Automotive Cybersecurity Report* (Feb. 2024), <https://upstream.auto/reports/global-automotive-cybersecurity-report/>. By compromising software or its dependencies, malign actors may surveil, disrupt, damage, or otherwise exploit the data or systems of those who use the software. *See National Counterintelligence and Security Center, "Software Supply Chain Attacks,"* (Mar. 2021), [https://www.dni.gov/files/NCSC/documents/supplychain/Software\\_Supply\\_Chain\\_Attacks.pdf](https://www.dni.gov/files/NCSC/documents/supplychain/Software_Supply_Chain_Attacks.pdf).

The threat of such a cyber operation by malicious actors can grow significantly when firmware or hardware components are intentionally designed with vulnerabilities. Access to the hardware supply chain for VCS provides an avenue for threat actors to manipulate or insert, with malicious intent, hardware, or firmware modules into telematics hardware components such as modems, Systems on Chip (SoC), Printed Circuit Boards (PCB), central processing units, and antennae. Manipulating or modifying hardware and associated firmware in the supply chain could also allow foreign adversaries to insert a backdoor, granting them control over the VCS. *See Cybersecurity and Infrastructure Security Agency, Defending Against Software Supply Chain Attacks* (April 2021), [https://www.cisa.gov/sites/default/files/publications/defending\\_against\\_software\\_supply\\_chain\\_attacks\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf), and National Counterintelligence and Security Center, "Software Supply Chain Attacks," (Apr. 2023), <https://www.dni.gov/files/NCSC/documents/supplychain/Software-Supply-Chain-Attacks.pdf>. For instance, cellular and satellite telecommunications transceivers are pivotal connectivity components in the VCS, utilizing radio frequency (RF) energy to facilitate the transmission and reception of data

between a vehicle and the external world. If these transceivers are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, such actors would have the means and capability to introduce vulnerabilities that could be exploited to intercept and/or compromise the information exchanged between the connected vehicle and the external world.

## 2. Automated Driving Systems

The complexity of ADS software, the large foundation of data sources, and the driving responsibilities inherent to ADS render it a valuable target for exploitation. An ADS encompasses the upper end of the spectrum of autonomy levels that dictate the vehicle's independence and the extent of driver intervention required. As defined by the SAE J3016, autonomy levels range from Level 0 (no automation) where the driver controls all aspects of driving, to Level 5 (full automation) where the vehicle can operate independently under all conditions without human intervention. Levels 1 and 2 offer driver assistance through systems that control either steering or acceleration and braking, while Levels 3 through 5 (which generally comprise ADS) progressively increase the system's responsibility for driving tasks, with Level 4 requiring the ability to complete all driving functions within defined operational design domains (ODDs). As the autonomy level increases, the reliability and safety of the ADS become increasingly reliant on the system's operational performance, safety protocols, and cybersecurity measures. *See Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, SAE International, (Apr. 2021), [https://www.sae.org/standards/content/j3016\\_202104/](https://www.sae.org/standards/content/j3016_202104/).

An ADS must be able to execute Dynamic Driving Tasks (DDTs) within specific ODDs. DDTs include critical tasks such as steering, braking, acceleration, and Object and Event Detection, Classification and Response (OEDR). OEDR enables an ADS to perceive and respond to surrounding objects and events, a responsibility that shifts progressively from the driver to the ADS itself as the degree of vehicle autonomy increases. *See Edward Griffor, David Wollman, and Christopher Greer "Automated Driving System Safety Measures Part 1: Operating Envelope Specification," NIST Special Publication 1900-301* (2021), <https://nvlpubs.nist.gov/>

*nistpubs/SpecialPublications/NIST.SP.1900-301.pdf*.

An ADS relies on a large foundation of connected information sources for decisions and outputs which in turn could create inherent vulnerabilities. As a result, the complex software systems that drive decisions for an ADS are valuable targets for malicious actors to exploit. Software-based threats to Connected Vehicles equipped with an ADS include manipulation of sensors to create phantom objects; manipulation of ADS software to detect, capture, and retain information about specific geographic areas or other sensitive data; or other manipulation of sensor fusion processing software that could lead to faulty and dangerous vehicle decision making, to include unauthorized control over the Connected Vehicle. *See National Counterintelligence and Security Center, "Autonomous Automotive Vehicle Supply Chain Risk,"* (2022), <https://www.dni.gov/files/NCSC/documents/supplychain/autonomous-vehicles-placemat-2022-D9A54B50-.pdf>.

A compromised ADS creates opportunities for data exfiltration and unauthorized vehicle manipulation due to the direct access it has to the internal vehicle network (IVN). The IVN controls the communication framework within a Connected Vehicle, overseeing the ECUs responsible for engine control, traction control, door locks, climate control, battery management, powertrain, airbags, cameras, and radar functionalities. These ECUs also communicate via overlaid communication networking protocols such as a CAN bus, Local Interconnect Network (LIN), and ethernet. *See Anastasios Giannaros, et al. "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain and Future Directions," Journal of Cybersecurity and Privacy 3.3* (2023). Because ADS interacts with ECUs through the IVN, a compromised ADS has the capability to execute functions that affect nearly all of a Connected Vehicle's software and hardware components. For example, an update to an ADS could alter the outputs the ADS makes to a body control unit, enabling the ADS to erroneously and dangerously open a vehicle's door while in motion. Moreover, because many Connected Vehicles maintain their own networks and actively scan their operating environment for other proximate networks, an ADS can also potentially be used to impact the IVN of other vehicles or transportation infrastructure networks through vehicle-to-vehicle communication. *See National*

Counterintelligence and Security Center, *Autonomous Automotive Vehicle Supply Chain Risk*, (Apr. 2022), <https://www.dni.gov/files/NCSC/documents/supplychain/autonomous-vehicles-placemat-2022-D9A54B50-.pdf>, and Patrick Wagner, Nikolai Puch, and David Emeis, "Cybersecurity risk analysis of an automated driving system," *Fraunhofer Institute AISEC*, (Oct. 2023), <https://publica.fraunhofer.de/entities/publication/4d66e81e-3570-4c49-9f8c-8c9967a34ca6/details>.

Given the significant processing power and complex decision-making ability of an ADS, the risks arising from ADS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary extend beyond the IVN itself and can include risks to the fidelity and integrity of data that flows to downstream or adjacent transportation infrastructure. Foreign adversaries can corrupt ADS data by exploiting existing vulnerabilities in ADS connectivity environments (see section IV(b) below). As such, direct access to an ADS afforded to a malicious actor through the design, development, manufacture, or supply of ADS software has the potential to cause severe adverse consequences to U.S. national security and U.S. persons.

#### *b. Threats Associated With the PRC and Russia*

The design, development, manufacture, or supply of certain VCS and ADS components by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia poses undue or unacceptable risks to national security and U.S. persons. The PRC and Russia have adopted political, legal, and regulatory regimes that enable their governments to exercise direct and indirect ownership, control, or influence over entities in the connected vehicle supply chain. Unlike other foreign adversaries, the PRC and Russia also have certain current and anticipated industrial capabilities and expertise that uniquely position them within the global automotive market to pose an outsized risk, particularly when paired with the vulnerabilities present within certain connected vehicle systems.

##### *1. PRC*

The PRC's role in the U.S. connected vehicle supply chain presents undue and unacceptable risks. The PRC has a large and growing automotive sector

with strong connections to non-PRC, including U.S., automakers providing it potential increased access to the U.S. automotive market. Further, the PRC's automotive sector has historical and ongoing links to the PRC military and is influenced by pervasive government intervention, including through legal and regulatory structures that increase government oversight of and control over PRC-based companies and their foreign subsidiaries. See Du Xiaoying and Wang Siyi, "Dongfeng plays pivotal role in supporting China's military," *China Daily*, (Sept. 25, 2015), [https://www.chinadaily.com.cn/cndy/2015-09/25/content\\_21976945.htm](https://www.chinadaily.com.cn/cndy/2015-09/25/content_21976945.htm), and Matthew Funaiolo et al., "China Accelerates Construction of 'Ro-Ro' Vessels, with Potential Military Implications," Center for Strategic and International Studies, (Oct. 2023), <https://chinapower.csis.org/analysis/china-construct-ro-ro-vessels-military-implications/>. Moreover, the PRC possesses advanced cyber espionage capacities that it exercises through both state and non-state cyber actors exacerbating such risks.

First, the size and scale of state control in the PRC auto sector poses outsized risks, increasing the vectors by which the national security threats associated with Connected Vehicles can enter the United States. The PRC automotive sector has played an important role in its domestic industrial policy since 1986, when the sector was first named a "pillar industry" in the Seventh Five-Year Plan. The Fourteenth Five-Year Plan, the latest strategic framework for the PRC, continues to prioritize the technology innovation and sustainable development of the automobile market, including new energy vehicles and connected vehicle software and hardware systems. See Ben Murphy, "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," Center for Security and Emerging Technology, (May 2021), [https://cset.georgetown.edu/wp-content/uploads/t0284\\_14th\\_Five\\_Year\\_Plan\\_EN.pdf](https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf). For many years, the state has pursued a number of policies and practices to further its industrial policy objectives in the automotive sector, including mandatory joint venture requirements, foreign equity restrictions, massive subsidies and other financial support measures, and various other preferences and discriminatory policies and practices. The PRC automotive sector's growth was also led in part by several prominent state-

owned firms that began as military equipment suppliers (e.g., Chang'an Automobile, Changhe, Hunan Changfeng Motor) or have since risen to become prominent state-owned firms (e.g., GAC Group, Chery Automobile Co.). See Mattias Holweg, Jianxi Luo, and Nick Oliver, *The past, present and future of China's automotive industry: a value chain perspective*, *International Journal of Technological Learning, Innovation and Development* 2 (Feb. 2009), <https://www.pure.ed.ac.uk/ws/portalfiles/portal/7765689/Oliver.pdf>. In recent years, this growth and development has led to a massive surge in domestic vehicle production, with Chinese vehicle production increasing by 1.5 times over the 15-year span between 2008 and 2023. Indeed, in 2023, the PRC alone was responsible for nearly 33 percent of global passenger vehicle production. See VDA, *Global passenger vehicle production in 2023, by country [Graph]*, (Retrieved July 23, 2024), <https://www.statista.com/statistics/277055/global-market-share-of-regions-on-auto-production/>, and OICA & Statista, *China's share in global vehicle production from 2008 to 2021 [Graph]*, (Mar. 17, 2022), <https://www.statista.com/statistics/233942/chinas-share-of-global-production-capacity-of-the-automobile-industry/>. Amid this significant growth in the PRC's domestic auto industry, Chinese automakers, both state-owned and private firms, have leveraged their significant state-backed support, including subsidies, to fuel a global expansion that has seen Chinese automakers establishing foreign operations in countries like South Africa, the Netherlands, Thailand, Japan, and Brazil, among others, increasing the risks stemming from PRC auto manufacturing in third countries. This expansion, combined with recent investment announcements, has spurred concerns that Chinese automakers may soon seek to further expand into the United States either through exports or the establishment of additional manufacturing facilities. Some PRC-based companies have announced plans to establish manufacturing facilities in Mexico, which could enable them to receive favorable trade terms contained in the U.S.-Mexico-Canada Agreement (USMCA). Such a significant position within the global auto sector greatly expands the number of potential nexus points between PRC connected vehicle suppliers and U.S. automakers and U.S. consumers, including indirectly through auto manufacturers in third countries.

Second, the military linkage between the PRC government and the automotive sector continues to the current day with the PRC's military-civil fusion strategy—which seeks to, among other goals, exploit investment and innovation within the PRC's private sector to achieve military modernization goals—and has prioritized specific information and communication technologies that are integral to connected vehicle supply chains (e.g., telecommunications, artificial intelligence). See Ben Murphy, "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," Center for Security and Emerging Technology (May 2021), [https://cset.georgetown.edu/wp-content/uploads/10284\\_14th\\_Five-Year\\_Plan\\_EN.pdf](https://cset.georgetown.edu/wp-content/uploads/10284_14th_Five-Year_Plan_EN.pdf). Strategies to achieve these goals include mandating collaboration between PRC-based companies and the military and establishing public and private firms as vectors to facilitate technology transfer, industrial espionage, and intellectual property theft that would be advantageous for the PRC military. See Office of the Dir. of Nat'l Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, (Feb. 6, 2023), <https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>.

Third, even beyond military-civil fusion, the role of the PRC government in the auto sector has only grown as government intervention in the market increases, including through direct ownership of prominent industry participants, the purchasing of so-called "golden shares" to gain significant levels of influence within otherwise private firms, embedding Chinese Communist Party (CCP) representatives within corporate boards and management, and the forceful application, or threat thereof, of the PRC's expanding security laws, including its digital era legal structure. See Lingling Wei, "China's New Way to Control Its Biggest Companies: Golden Shares," *Wall Street Journal* (Mar. 2023), <https://www.wsj.com/articles/xi-jinpings-subtle-strategy-to-control-chinas-biggest-companies-ad001a63>. Laws promulgated in recent years provide the PRC government increased oversight and control over PRC-based companies and their foreign subsidiaries, providing a lever for influence over corporate operations that further exacerbates the threat that the PRC poses to U.S. national security. These laws require PRC-based

companies, wherever located, to comply with certain access and information requests upon demand from the PRC, and therefore could be used by the PRC to obtain business or other data from PRC-based companies involved in the connected vehicle supply chain. Companies operating under these laws frequently highlight the lack of transparency, consistency, clarity, and predictability of the enforcement of these laws, publicly stating that PRC laws relating to cybersecurity, data storage, or cryptography are not subject to the same degree of judicial accountability as they might be in other jurisdictions. In particular, BIS notes the PRC may utilize a suite of national security laws (e.g., *Counter-Espionage Law of the People's Republic of China* [promulgated by the Standing Committee of the National People's Congress, Nov. 1, 2014, amended Apr. 26, 2023, effective July 1, 2023]; *National Security Law of the People's Republic of China* [promulgated by the Standing Committee of the National People's Congress, July 1, 2015, effective July 1, 2015]; *National Intelligence Law of the People's Republic of China* [promulgated by the Standing Committee of the National People's Congress, June 27, 2017, effective June 28, 2017, amended Apr. 27, 2018]; *Anti-Terrorism Law of the People's Republic of China* [promulgated by the Standing Committee of the National People's Congress, Dec. 27, 2015, effective Jan. 1, 2016, amended Apr. 27, 2018]) to compel companies, including those in the connected vehicle supply chain, to support national security efforts—which are more broadly defined in the PRC than in the United States—or military agents upon request, including in some cases through the creation of backdoors and security vulnerabilities in products sold abroad, and in many cases, the PRC prohibits companies from disclosing that such a request was made. See U.S. Department of Homeland Security, "Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China," (Dec. 2022), [https://www.dhs.gov/sites/default/files/publications/20\\_1222\\_data-security-business-advisory.pdf](https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf). Additionally, PRC authorities have established a regulatory system that effectively allows them to stockpile cyber vulnerabilities. Entities subject to these regulations, including automotive systems manufacturers, are required to report vulnerabilities upon discovery to PRC authorities before patching them. See Cyberspace Administration of China,

"Provisions on the Management of Security Vulnerabilities of Network Products," (Jul. 2021), [https://www.cac.gov.cn/2021-07/13/c\\_1627761607640342.htm](https://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm). This requirement drastically increases the ability of the PRC government and PRC-backed cyber actors to take action against the United States using connected hardware and its associated software by creating an accessible library of known and potentially unpatched vulnerabilities. And fourth, the PRC has demonstrated a high level of competency in cyber malfeasance. The recent Volt Typhoon action exemplified how PRC cyber actors preposition themselves across U.S. critical infrastructure and military assets in order to, at a potential future date, launch an attack and impede U.S. decision making, induce social panic, and interfere with the deployment of U.S. military forces. See Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," (Feb. 2024), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>. A 2022 Annual Report to Congress by the U.S.-China Economic and Security Review Commission found that the PRC's ability and willingness to "weaponize" its own industries, particularly its cybersecurity industry, grants the country an asymmetric advantage over the United States; an argument that was further supported in reporting earlier this year that detailed the methods by which known government-affiliated cyber threat groups utilize private firms to carry out their attacks. See U.S.-China Economic and Security Review Commission, "2022 Annual Report to Congress," (Nov. 2022), [https://www.uscc.gov/sites/default/files/2022-11/2022\\_Annual\\_Report\\_to\\_Congress.pdf](https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf); Christian Shepherd et al., "Leaked files from Chinese firms show vast international hacking efforts," *The Washington Post* (Feb. 22, 2024), <https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoan/>. Additionally, a 2012 report from United States Senate Permanent Select Committee on Intelligence examining the national security risks posed by the PRC-based companies Huawei and ZTE specifically argued that there are numerous opportunities for PRC-based threat actors to insert malicious hardware or software components into ICTS products throughout the product development stage. See Permanent Select Committee on Intelligence, "Investigative Report on the U.S.

*National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*" (Oct. 2012), [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20\(final\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf). This risk has not diminished, as indicated by a study of designed vulnerabilities in products conducted by the Georgetown Security Studies Review, which outlines five years of persistent insertion of malicious code by PRC-based threat actors. See Georgetown Security Studies Review, "Flawed by design electronics with pre-installed malware" (May 2018), <https://georgetownsecuritystudiesreview.org/2018/05/23/flawed-by-design-electronics-with-pre-installed-malware/>. Given the above, the PRC's access to the U.S. connected vehicle supply chain through its growing automotive sector, military-civil fusion and other corporate governance policies, and legal institutions paired with its development of mature cyber espionage capabilities have increased the risk that the PRC could alter the systems in, or obtain and manipulate information to or about, market participants who use connected vehicle ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC.

## 2. Russia

The Russian state has prioritized the growth of its automotive manufacturing industry, instituted a legal and regulatory framework to compel company data sharing with the state, and maintained a long history of malicious cyber operations against the U.S. Under these circumstances, there is an increasing likelihood that Russia emerges as a supplier of connected vehicles technologies for the U.S. market, providing the Russian government a means of exploiting U.S. connected vehicles. Moreover, incorporating Russian hardware or software into the U.S. connected vehicle supply chain poses undue and unacceptable risks to U.S. critical infrastructure and U.S. persons.

First, while Russia has historically been less active in the global automotive sector than the PRC, the Russian government has recently sought to revitalize its own domestic auto manufacturing industry following the exodus of foreign automakers after the imposition of significant additional sanctions in 2022. In 2024 alone, the Russian auto market is projected to experience a 15 percent increase in passenger vehicle sales, marking a noted uptick since the market crashed

following sanctions and some Russian auto manufacturers have continued introducing new models even amid broader economic headwinds. See Reuters, "Russia's 2024 car sales forecast raised to 1.45 mln, units, AEB says," (Jul. 2024), <https://www.reuters.com/business/autos-transportation/russias-2024-car-sales-forecast-raised-145-mln-units-aeb-says-2024-07-03>. The void left by many foreign firms has made Russia a valuable export market for Chinese auto manufacturers seeking to expand their presence globally with some Chinese auto brands seizing significant market share from Russian competitors accounting for almost 56 percent of domestic auto sales in August 2023. See Gleb Stolayrov and Alexander Marrow, "Exclusive: Chinese car sales boom in Russia levels off amid shaky local recovery," *Reuters* (Nov. 2023), <https://www.reuters.com/business/autos-transportation/chinese-car-sales-boom-russia-levels-off-amid-shaky-local-recovery-2023-11-24/>. In Russia, the revitalization of the domestic economy, in particular the domestic auto sector, has become a key focus of the government since the imposition of sanctions in recent years. The Russian government has released several plans pointing to a prioritization of the development of its domestic automotive market with a particular focus on research and development for new technology, including autonomous vehicles and V2X vehicle connectivity systems. See Russian Federation, *Order of the Government of the Russian Federation of December 28, 2022 No. 4261-r On Approval of the Strategy for the Development of the Automotive Industry of the Russian Federation until 2035* (Jan. 4, 2023), <https://www.garant.ru/products/ipo/prime/doc/405963861/#1000> and See Russian Federation, *Order of the Government of the Russian Federation of August 23, 2021 No. 2290-r On Approval of the Concept for the Development of Electric Vehicle Production and the Transport Strategy of 2030*, (2023), <http://static.government.ru/media/files/bW9wGZ2rDs3BkeZHf7ZsaxnlbJzQbJf7t.pdf>. The development of these interlocking national transportation and automotive industry strategies involved stakeholders from domestic automakers, technology sectors, and the Russian government, illustrating a coordinated effort across the Russian state and its domestic automotive industry. In order to extend the reach of the state into the Russian auto industry, in February 2024, Russia established a state-owned corporation named Rosavto that will act

as liaison between government and industry and will develop production plans for vehicles and automotive spare parts, oversee the development of new models and technologies, and manage order distribution, legislative initiatives, and workforce training. See Eugene Gerden, "New State Corporation to Oversee Russian Auto Industry," *Wards Auto* (Feb. 2024), <https://www.wardsauto.com/regulatory/new-state-corporation-to-oversee-russian-auto-industry>. Concerted efforts by the Russian government to grow the domestic Russian automotive industry increase the likelihood that Russian-manufactured VCS hardware or covered software will enter the U.S. connected vehicle supply chain, which, as described below, would present an undue or unacceptable risk to U.S. national security.

Second, like the PRC, the Russian government employs a suite of laws that enable it to compel domestic companies with overseas operations to provide data gleaned through foreign ventures or to surrender similar operational assets to the Russian state. These laws (e.g., Russian Law Federal Security Service No. 40-FZ, "Operational-Investigative Activity" No. 144-FZ, 2014 Amdt. to No. 97-FZ) provide the Russian government direct control over Russian corporations' activities and facilities, including data or customer information, and mandate that companies cooperate with assisting counterintelligence actions as requested by the state, including the Federal Security Service of the Russian Federation (FSB). The FSB can, in some cases, mandate that companies allow the FSB to install equipment on their infrastructure or collect data. Firms that are required to facilitate this surveillance or intrusion activity can also be required to actively obfuscate such requests and must provide the state with any information essential to the decryption of any communications captured. Together, these laws enable the Russian state to collect and exploit sensitive data on or about U.S. persons via Russian businesses and, should Russian companies become more prominent in the connected vehicle supply chain, create a pathway by which the Russian government could secure wide-ranging access to the vast amounts of data collected and processed by Connected Vehicles in the United States. See internet Governance, "Report of Peter B. Maggs," (Dec. 2017), <https://www.internetgovernance.org/wp-content/uploads/12-7-Exhibit-AR-Part-6-Maggs-report.pdf>. Public reports have consistently raised concerns about



Russian government laws concerning data collection, citing a lack of appropriate safeguards to prevent misuse, to include judicial or public oversight. More broadly, reports have repeatedly documented the uneven application of the rule of law, lack of judicial accountability, recurrent violations of judicial proceedings, and challenges with judicial independence. See Justin Sherman, "Russia is weaponizing its data laws against foreign organizations," Brookings, (Sept. 2022), <https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/>; Evgeni Moyakine and A. Tabachnik, "Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived legislation in the age of modern technology," *Computer Law & Security Review* 40, (Apr. 2021), <https://www.sciencedirect.com/science/article/pii/S0267364920301175>.

Third, apart from the access codified in Russia's legal framework, the country has a longstanding pattern of utilizing cyber operations to gain illicit access to systems that advance the strategic ends of Russian authorities. For example, in December 2020 the company SolarWinds announced it was the target of a two-year-long cyber operation perpetrated by Russian hackers in the Russian Foreign Intelligence Services (SVR). See U.S. Securities and Exchange Commission, "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures," (Oct. 2023), <https://www.sec.gov/newsroom/press-releases/2023-227>. The perpetrators of the SolarWinds supply chain attack used a software update to deliver its malware to the platform's users after Russian intelligence services obtained covert access to the computer systems on which the platform was installed and ultimately impacted more than 18,000 users, including more than 100 companies and nine U.S. Government agencies. This attack credibly demonstrates how Russian actors can infiltrate global enterprise systems via software updates and exemplifies how they could similarly leverage software as a means to exploit connected vehicles in the United States. Additionally, a 2023 Cyber Security Advisory suggests that exploitation of information technology firms and their software will continue to be a persistent tactic leveraged by the Russian government to collect intelligence. See Joint Cyber Security Advisory, "Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE

Globally" (Dec. 2023), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a>. BIS has further identified Kaspersky Lab as an example of how Russia has leveraged software companies to give it the ability to collect and weaponize the personal information of Americans. See Bureau of Industry and Security, "Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc." (Jun. 2024), <https://www.federalregister.gov/documents/2024/06/24/2024-13532/final-determination-case-no-icts-2021-002-kaspersky-lab-inc>. These political, legal, and regulatory frameworks, combined with the PRC's and Russia's demonstrated capability to exploit ICTS supply chains through malicious cyber activity, exacerbate BIS's concern that the threats posed by these foreign adversaries could be directed at the U.S. connected vehicle supply chain, including integral systems such as VCS and ADS. The persistent connectivity and software-driven capabilities of VCS and ADS, combined with the vast amounts of data that traverse these systems, make them valuable and likely targets for the PRC and Russian governments to compromise.

#### c. Consequences

Taken together, VCS and ADS designed, developed, manufactured, or supplied by persons under the ownership, control, jurisdiction, or direction of the PRC or Russia manifest undue and unacceptable risks to United States national security in several ways. If left unaddressed, the interaction of threats and vulnerabilities could result in the exfiltration of sensitive U.S. persons' data to foreign adversaries or the remote or automated manipulation of Connected Vehicles by the PRC and Russia, among other concerns.

First, the integration of compromised VCS or ADS into a completed vehicle could undermine the reliability of a connected vehicle or its underlying control systems. Compromised components in VCS or ADS could result in increased frequency and severity of connected vehicle malfunctions that could in turn detrimentally impact U.S. national security, including the resiliency of U.S. critical infrastructure, or the safety of U.S. persons.

Given the persistent connectivity of VCS and ADS and the essential functions that they service in the operation of Connected Vehicles, these systems, if compromised and co-opted by an adversary, could serve as a node through which a foreign actor could probe or breach broader ICTS systems within the United States. According to research by Upstream, remote malicious

cyber activities—which rely on network connectivity (e.g., Wi-Fi, Bluetooth, 3/4/5G networks)—have increased significantly in recent years and consistently outnumber malicious cyber activities carried out through physical access to devices since at least 2010, accounting for 95 percent of all malicious cyber activities in 2023. See Upstream, *Upstream's 2024 Global Automotive Cybersecurity Report* (2024), <https://upstream.auto/reports/global-automotive-cybersecurity-report/>. Considering the increasingly sophisticated methodologies employed by foreign adversaries to gain access to critical U.S. cyber infrastructure, compromised VCS and ADS, with their inherent connectivity, would easily present another attack surface for foreign adversaries to exploit. As detailed in the previous analysis of vulnerabilities inherent in VCS, adversaries with access to VCS, such as to telematics systems, could inject malicious code into a vehicle's operational systems. Additionally, such malware could be developed in such a way as to exploit vehicle connectivity to propagate itself across multiple systems as the vehicle travels and connects to those discrete systems. In this way, not only would the ICTS integral to Connected Vehicles be compromised, but vehicle systems could be exploited to spread malware with the intent of harming all ICTS systems to which a vehicle connects. See Anastasios Giannaros, et al. "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain and Future Directions," *Journal of Cybersecurity and Privacy* 3.3 (2023).

Second, as discussed, both VCS and ADS have significant control over and access to critical vehicle functions, including steering, braking, speed control, ignition, and almost all other mechanical functions of the vehicle. Such extensive control over vehicle operations could enable a foreign adversary to use a compromised VCS or ADS component to hamper vehicle functions or even to manipulate a connected vehicle for malicious purposes. As VCS and ADS control or link to integral vehicle functions, a foreign adversary could even exploit compromised VCS or ADS components to impair or disable a connected vehicle while in transit. Disabled, impaired, or otherwise improperly functioning vehicles could result in grave damage or impediment to critical infrastructure within the United States, or in physical harm to U.S. persons. A disabled, impaired, or erratically functioning

Connected Vehicle, or potentially multiple Connected Vehicles all experiencing such problems simultaneously, could result not only in traffic patterns that would effectively block critical transportation arteries, but could cause collisions ultimately damaging transportation features (e.g., roadways, bridges, tunnels) and energy, telecommunications, and similar infrastructure situated near transportation systems. The potential consequences of widespread connected vehicle impairment could be particularly acute if the targets were fleet vehicles operating in support of infrastructure vital to transportation, energy, water, waste, telecommunications, and other essential services.

The risks to the resiliency of critical U.S. infrastructure posed by connected vehicle components designed, developed, manufactured, or supplied by persons that are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia are further compounded by the potential for VCS and ADS to collect data on infrastructure. Advances in VCS and ADS necessitate increasingly cutting-edge sensor suites incorporating radar, LiDAR, camera, sonar, and computer vision to gather information on the surrounding environment for both onboard computing and remote cloud computing to process data in informing vehicle operating decisions. This vast wealth of data, collected over time by multiple vehicles likely contains valuable information such as location data about critical U.S. infrastructure. For example, data gathered from GPS/GNSS systems in a connected vehicle could be cross-referenced and collated with a multitude of other data to produce information about the location, function, and operational trends of various transportation, energy, or other critical infrastructure. A foreign adversary could extract such critical infrastructure data using its control over designers, developers, manufacturers, or suppliers of VCS and ADS components subject to the foreign adversary's ownership, control, jurisdiction, or direction, thereby increasing the risk and precision of attacks on such critical infrastructure.

Finally, given the volume of information collected by vehicles to support VCS and ADS operation, exploitation of these systems could enable an adversary to cull a tremendous amount of data on vehicle movement across the United States. This information could potentially include data generated on or from fleet

vehicles used by emergency response, law enforcement, or the military. This data, and particularly all metadata and derived data that can be drawn from the raw data, can provide considerable insight into fleet size, composition, and capabilities, as well as information on organizational response times and response procedures. Such information would prove valuable to an adversary seeking to disrupt U.S. emergency response operations. Any potential risks to U.S. national security arising from disrupting emergency response activities are further compounded by the potential for an adversary to exploit access to VCS and ADS to leverage the persistent connectivity required for malign operations, including exploits to trigger improper engine shutdown, brake activation, or electrical system deactivation. Any of these actions have serious consequences for U.S. persons' health and safety. The PRC or Russia could use similar methods to target U.S. persons other than institutions, thereby imperiling the safety and security of individual U.S. citizens or residents. VCS and ADS, if corrupted by the producer at the direction of a foreign adversary, could improperly access driver mobile devices to collect, exfiltrate, and exploit personally identifiable information (PII) or even protected health information (PHI). It is also possible that a foreign adversary could use covert access to VCS and ADS to provide false or misleading information to a driver, causing degraded and dangerous vehicle operation conditions. Such tactics could be used either indiscriminately to sow panic and cause disruption, or to intentionally target specific drivers. Additionally, and as noted by the Office of the Director of National Intelligence in the 2024 National Counterintelligence Strategy, foreign adversaries, like the PRC and Russia, view this kind of PII and PHI as particularly valuable as it provides them "not only economic and R&D benefits, but also useful [counterintelligence] information, as hostile intelligence services can use vulnerabilities gleaned from such data to target and blackmail individuals." See The Director of Nat'l Intelligence, *2024 National Counterintelligence Strategy* (Aug. 2024), [https://www.dni.gov/files/NCSC/documents/features/NCSC\\_CI\\_Strategy-pages-20240730.pdf](https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf).

Even when such systems are not subject to compromise, companies owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, if occupying certain positions within the supply chain, may

potentially legally gain access to their users' personal data. For example, one prominent Chinese auto manufacturer with operations in the United States publicly states in its U.S. privacy policy that the personal data it may collect (e.g., identifiers, customer records information, internet or other electronic network activity information, geolocation information, professional or employment-related information) is only stored in the United States "in principle," but goes on to note that personal data "may be transferred to our headquarters in China" for processing and storage. While the incorporation in the U.S. supply chain of VCS hardware and covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia poses one type of risk, transactions involving VCS hardware and covered software pose a separate risk when the connected vehicle manufacturer is, itself, owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, even when the connected vehicle manufacturer is located in the United States. connected vehicle manufacturers have privileged and direct access to all systems in the vehicle, including the VCS hardware and covered software. Not only are VCS hardware and covered software built to the connected vehicle manufacturers' specifications but prior to the sale of a completed connected vehicle, connected vehicle Manufacturers are able to exercise significant levels of control over that VCS hardware and covered software with little to no external oversight prior to the sale of the completed connected vehicle. Based on the foregoing, BIS assesses that ICTS transactions involving VCS hardware or covered software designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of the PRC or Russia—including transactions to supply the VCS hardware or covered software into the United States market as part of the sale of the completed connected vehicle—present undue or unacceptable risks to the national security of the United States within the meaning of E.O. 13873. BIS welcomes comment on the vulnerabilities and risks it has identified.

#### V. Discussion of the Proposed Rule and Request for Comments

BIS proposes a regulation that would—absent a general or specific authorization otherwise—(1) prohibit VCS hardware importers from knowingly importing into the United



States certain hardware for VCS; (2) prohibit connected vehicle manufacturers from knowingly importing into the United States completed connected vehicles incorporating covered software; (3) prohibit connected vehicle manufacturers from knowingly selling within the United States completed connected vehicles that incorporate covered software; and (4) prohibit connected vehicle manufacturers who are persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia from knowingly selling in the United States completed connected vehicles that incorporate VCS hardware or covered software (collectively, "Prohibited Transactions"). These prohibitions would apply to transactions when such VCS hardware or covered software is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

BIS anticipates that this rule would primarily impact market participants who could be considered VCS Hardware Importers or connected vehicle manufacturers, such as OEMs and importers of completed connected vehicles, as well as Tier 1 and Tier 2 suppliers of VCS Hardware. For these entities, three compliance mechanisms—Declarations of Conformity, general authorizations, and specific authorizations—are available, depending on whether the VCS hardware importer or connected vehicle manufacturer wishes to engage in an otherwise prohibited transaction. Importantly, because VCS hardware importers and connected vehicle manufacturers frequently offer many different types of products, any one of the three mechanisms may not be available for their entire business. Rather, depending on the product, VCS hardware importers and connected vehicle manufacturers could be required to use a combination of these three mechanisms to meet their obligations under the rule.

First, Declarations of Conformity would have to be submitted to BIS by VCS hardware importers and connected vehicle manufacturers who have not engaged in a prohibited transaction, unless otherwise specified. Such VCS hardware importers and connected vehicle manufacturers would, in this Declaration of Conformity, certify, once per calendar year or model year (or whenever material changes occur) to BIS that the submitter has not engaged in a prohibited transaction and provide certain information on the import of

VCS hardware and/or the import or sale of completed connected vehicles.

Second, a general authorization could be available for VCS hardware importers and/or connected vehicle manufacturers seeking to engage in an otherwise prohibited transaction, depending on the circumstances. A general authorization would allow the VCS hardware importer and/or connected vehicle manufacturer to engage in the otherwise prohibited transaction, without the need to notify or seek approval from BIS. General authorizations would be available only in a narrow set of circumstances in which the conditions of the otherwise prohibited transaction appropriately mitigate the level of risk associated with the particular transaction. Such conditions would include, for example, when VCS hardware is imported from the PRC or Russia solely for testing purposes, or where the completed connected vehicle that incorporates VCS hardware or covered software from the PRC or Russia will be driven on public roads for fewer than 30 calendar days per year. Those availing themselves of a general authorization would be required to continuously monitor their use of the VCS hardware or completed connected vehicles covered by the General Authorization to ensure the authorization still applies. If a change would render the transaction ineligible for a general authorization, such as a change in the vehicle's use, the VCS hardware importer or connected vehicle manufacturer would be required to apply for a specific authorization and to cease engaging in such transaction unless and until a Specific Authorization is granted. For example, if a completed connected vehicle that incorporates covered software or VCS Hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia is no longer used solely for display, research, or testing, the VCS hardware importer or the connected vehicle manufacturer would be required to seek a specific authorization. Similarly, if the VCS Hardware Importer or connected vehicle manufacturer meets or exceeds total model year production of 1,000 units, or if a completed connected vehicle that incorporates covered software or VCS hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia is to be used on public roadways for 30 or more days in any calendar year, the VCS hardware

importer or connected vehicle manufacturer would be required to seek a specific authorization from BIS.

Lastly, for VCS hardware importers and connected vehicle manufacturers who wish to engage in a prohibited transaction, but do not otherwise qualify for a general authorization, a specific authorization from BIS would be required before they could proceed with the prohibited transaction. A specific authorization would only be available in circumstances where BIS determines, based on the information submitted by the applicant and other collected information, that the otherwise prohibited transaction does not present an undue or unacceptable risk to U.S. national security. However, as a condition of approving the specific authorization, BIS might impose certain requirements and mitigation measures upon the VCS hardware importers and connected vehicles manufacturers seeking to proceed with the prohibited transaction.

VCS hardware importers and connected vehicle manufacturers could appeal to the Under Secretary for Industry and Security (Under Secretary) any decision by BIS to deny an application for a Specific Authorization, suspend or revoke a previously granted specific authorization, or issue a written notification that a VCS hardware importer or connected vehicle manufacturer is ineligible for a general authorization. Further, the regulation would establish a method for VCS hardware importers and connected vehicle Manufacturers to seek guidance from BIS, in the form of advisory opinions, on prospective transactions that may be prohibited. BIS also proposes to establish a process through which BIS may inform VCS hardware importers or connected vehicle manufacturers that certain of their activities could constitute a prohibited transaction.

In proposing this rule, BIS recognizes that Section 203(b) of IEEPA—*i.e.*, the "Berman Amendment"—limits the scope of the authority to regulate or prohibit transactions relating to "information" or "informational materials." In relevant part, the Berman Amendment states that the "authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly . . . the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph

records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and newswire feeds.” 50 U.S.C. 1702(b)(3). Consistent with the statute’s text and purpose, as demonstrated by legislative history and context, as well as judicial interpretations, BIS understands the phrase “information or informational materials” to refer to expressive materials and mediums that may be carrying such expressive content. See, e.g., *United States v. Amirnazmi*, 645 F.3d 564, 586–87 (3d Cir. 2011). Accordingly, the Berman Amendment prevents BIS from regulating, directly or indirectly, the import or export of expressive materials. It does not, however, prevent BIS from imposing a regulation that is aimed at the functional capabilities of technology.

The proposed rule is consistent with the Berman Amendment. Its purpose is to regulate transactions involving certain hardware and software based on functional capabilities that can be exploited by foreign adversaries, not the exchange of ideas and expression that the Berman Amendment protects. As discussed in Section IV, VCS Hardware and covered software process and transmit data such as geolocation information or systems diagnostics reports, which are used to monitor and control the vehicle’s safe operation, and that a foreign adversary could also manipulate in ways that could impair or disable the vehicle’s function, leading to dangerous outcomes that pose a harm to U.S. national security. Similarly, the functional data collected by Covered Software—such as high-definition mapping data of infrastructure and roadways—would pose serious risks to that critical infrastructure if collected and exploited by a foreign adversary. As a result, BIS has determined that the proposed prohibitions in this rule are consistent with the Berman Amendment, which was intended to protect materials involving the free exchange of ideas from regulation under IEEPA. BIS is considering whether and how to address the term “information or informational materials” within the context of the proposed rule and may consider further changes to the final rule to reflect our interpretation of this term. BIS welcomes comment on this issue.

Each section of the proposed rule is discussed below. BIS invites comments on all aspects of this proposed rule.

#### a. Definitions

##### 1. Automated Driving System (ADS)

BIS proposes to define “Automated Driving System” to mean hardware and

software that, collectively, are capable of performing the entire dynamic driving task for a completed connected vehicle on a sustained basis, regardless of whether it is limited to a specific ODD. This definition is consistent with the terminology industry uses for systems that operate at certain advanced levels of autonomy. It is also consistent with definitions issued by NHTSA. Specifically, this definition corresponds to automation levels 3, 4, and 5 as defined by SAE International standard J3016.

##### 2. Completed Connected Vehicle

BIS proposes to define “completed connected vehicle” to mean a connected vehicle that requires no further manufacturing operations to perform its intended function. This definition is consistent with definitions issued by NHTSA. Additionally, for the purposes of this proposed definition, the integration of an ADS into a connected vehicle constitutes a manufacturing operation for a Completed Connected Vehicle. BIS intends this caveat to clarify that a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, whose sole manufacturing or assembly operation is integrating ADS into an otherwise Completed Connected Vehicle, would be subject to the prohibitions in the rule and would need to obtain a Specific Authorization before importing or Selling that completed connected vehicle in the United States.

##### 3. Connected Vehicle

BIS proposes to define “connected vehicle” to mean a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways, that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device. Vehicles operated only on a rail line are not included in this definition. This definition incorporates the suggestions of commenters to the ANPRM, many of whom requested that the definition of connected vehicle specify the types of vehicles that would be covered.

##### 4. Connected Vehicle Manufacturer

BIS proposes to define a “connected vehicle manufacturer” to mean a U.S. person (1) manufacturing or assembling completed connected vehicles in the United States; and/or (2) importing

completed connected vehicles for Sale in the United States.

##### 5. Covered Software

BIS proposes to define “covered software” to mean the software-based components, in which there is a foreign interest, executed by the primary processing unit of the respective systems that are part of an item that supports the function of VCS or ADS at the vehicle level. covered software does not include firmware, which is characterized as software specifically programmed for a hardware device with a primary purpose of controlling, configuring, and communicating with that hardware device. At a minimum, this definition of covered software would include operating systems such as a real-time operating system (RTOS), and general-purpose operating systems. An example of covered software within the ADS is, if included in the system, the machine learning software that performs the functions of object detection, classification, and decision making.

Covered software does not include open-source software. BIS understands open-source software as software that can be freely used, modified, and distributed by anyone, with both access to the source code and the ability to contribute to the software’s development and improvement. Given these qualities of open-source software, it is not designed, developed, manufactured, or supplied by any attributable entity. Therefore, the inclusion of open-source software as a component of covered software is not subject to prohibition. However, if licensed open-source software is modified to create proprietary enterprise software for a specific use not meant for redistribution, the resulting software could be subject to prohibition if the person modifying the open-source software is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. In addition to other aspects of this proposed rule, BIS specifically seeks comment on this definition.

##### 6. FCC ID Number

BIS proposes to define “FCC ID Number” as the unique alphanumeric code identifying a product subject to certification by the Federal Communications Commission (FCC) composed of a (1) grantee code and (2) product code.

##### 7. Foreign Interest

For the purposes of this rule, BIS is considering “foreign interest,” when used with respect to property, as any

interest in property, of any nature whatsoever, whether direct or indirect, by a non-U.S. person. Under this definition, a foreign interest can include, but is not limited to, an interest through ownership, intellectual property, contract—*e.g.*, ongoing supply commitments such as maintenance, any license agreement related to the use of intellectual property—profit-sharing or fee arrangement, as well as any other cognizable interest. This definition is consistent with the definition of “interest” used in the context of Office of Foreign Asset Control sanctions, which are, in relevant part, also established pursuant to the statutory requirements of IEEPA. *See* 31 CFR Chapter V, *and, e.g.*, 31 CFR 510.313, 535.312.

Consistent with IEEPA, BIS proposes to regulate only transactions involving property in which a foreign country or national thereof has any such interest. A transaction would be subject to the prohibitions in the proposed rule only if it involves ICTS, specifically VCS hardware or covered software, that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. VCS hardware importers and connected vehicle manufacturers wishing to engage in transactions that this rule proposes to prohibit would need to qualify for a general authorization or obtain a specific authorization. In order to provide sufficient visibility into the supply chains of VCS Hardware and covered software including to verify that the transaction does not involve VCS Hardware or covered software that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia (*see* Section V(c) of this notice and proposed Section 791.305), BIS is proposing to require that VCS hardware importers and connected vehicle manufacturers that import VCS hardware, or import or sell completed connected vehicles that contain covered software in which there is any other foreign interest, submit an annual Declaration of Conformity containing relevant details about the import or Sale. BIS seeks comment on this regulatory approach, including the necessity and efficacy of requiring Declarations of Conformity with respect to VCS hardware and covered software in which there is a foreign interest, though not a foreign adversary interest. BIS also seeks comment on the availability and efficacy of any

alternative approach that would require a narrower set of VCS hardware importers and completed connected vehicle manufacturers to submit Declarations of Conformity, while still achieving the goals of the Declaration of Conformity requirement and addressing the declared emergency under Executive Order 13873.

With respect to VCS hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, BIS proposes to regulate the importation of VCS hardware, making VCS hardware importers responsible for compliance.

With respect to Covered Software, based on discussions with connected vehicle manufacturers, automotive suppliers, and other stakeholders, BIS has come to understand that typically, ADS and VCS software are designed or developed to a connected vehicle manufacturer's specifications. ADS and VCS software is frequently designed, developed, or supplied by foreign persons, and those persons frequently retain a legally cognizable interest in the underlying software, even after it has been integrated into the connected vehicle. For example, foreign software developers may earn profits from use of their software; retain data access and sharing rights to the software; or have obligations to maintain and update the software. Such arrangements are among the types of interests that BIS contemplates as giving rise to an obligation to submit a Declaration of Conformity or, if the software designer, developer, or supplier is a person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, to qualify for a General Authorization or seek a Specific Authorization under the proposed rule. BIS therefore proposes to regulate covered software by regulating the importation or sale of completed connected vehicles, making connected vehicle Manufacturers responsible for compliance. BIS seeks comment on this understanding of foreign interests in covered software as well as other arrangements in which foreign designers, developers, or suppliers of covered software retain a cognizable legal interest in the software after it is integrated into a connected vehicle.

Finally, in addition to the general regulations related to VCS hardware and covered software described above, with respect to connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, BIS additionally proposes to

regulate VCS hardware and covered software by regulating the sale of completed connected vehicles that incorporate VCS hardware or covered software. In this circumstance, BIS understands from extensive engagement with connected vehicle manufacturers and automotive suppliers that persons who own, control, or direct the operations of the connected vehicle manufacturer would maintain an interest in the vehicle transactions that the connected vehicle manufacturer carries out. For example, this could include, but is not limited to, profit sharing agreements between a parent company and its U.S. subsidiary, or data sharing agreements between the same. BIS understands this to be standard for the automotive industry and would welcome comments on this issue. Additionally, because the PRC and Russian legal regimes discussed in Section IV of this notice could compel a PRC or Russia-based parent company of a connected vehicle manufacturer to provide those governments with information on or access to the operations of the U.S.-based connected vehicle manufacturer, BIS understands that the foreign parent company typically retains a legal right to access the data collected by the U.S. subsidiary, representing a foreign interest in that U.S. subsidiary and its connected vehicle sales.

BIS seeks comment on the nature of foreign interests in transactions related to the connected vehicle supply chain, including as described in the prohibitions outlined herein. BIS also seeks comment as to its understanding of the nature and presence of a Foreign Interest in property subject to the prohibitions described above, as well as whether there are other types of transactions that would involve Foreign Interests, as described above.

#### 8. Hardware Bill of Materials

BIS proposes to define “Hardware Bill of Materials” or HBOM as a comprehensive list of parts, assemblies, documents, drawings, and components required to create a physical product. This term includes information identifying the manufacturer, related firmware, technical information, and descriptive information.

#### 9. Import

BIS proposes to define “import” to mean, with respect to any article, the entry of such article into the United States Customs Territory. It does not include admission of an article from outside the United States into a foreign-trade zone for storage pending further assembly in the foreign-trade zone, or

shipment to a foreign country. This definition only applies to subpart D of 15 CFR part 791.

#### 10. Item

BIS proposes to define “item” as a component or set of components with a specific function at the vehicle level. A system may also be considered an item if it implements a function. This definition is consistent with ISO/SAE Standard 21434.

#### 11. Knowingly

BIS proposes to define “knowingly” to have the same meaning given to “knowledge” in the Export Administration Regulations (15 CFR 772.1). Knowledge of a circumstance (the term may be a variant, such as “know,” “reason to know,” or “reason to believe”) includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person’s willful avoidance of facts.

#### 12. Model Year

Consistent with the definition used by NHTSA, BIS proposes to define “model year” as the year used to designate a discrete vehicle model, irrespective of the calendar year in which the vehicle was actually produced, provided that the production period does not exceed 24 months. Throughout this proposed rule, BIS refers to both calendar year and model year when referring to the import of VCS Hardware, particularly for the submission of Declarations of Conformity (791.305) and the implementation timeline (791.308 (Exemptions)). BIS generally understands that most VCS hardware is imported into the United States already destined for a known, specific model year of vehicle. BIS also understands that some VCS hardware units may be imported without being associated with a specific vehicle model year. As such, the proposed rule provides separate timelines for each of these cases to accommodate business timelines for VCS hardware importers. BIS is particularly interested in comment on this approach.

#### 13. Person Owned by, Controlled by, or Subject to the Jurisdiction or Direction of a Foreign Adversary

BIS proposes to define “person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary” to mean, (a) any person,

wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary; (b) any person, wherever located, who is a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, and is not a United States citizen or permanent resident of the United States; (c) any corporation, partnership, association, or other organization with a principal place of business in, headquartered in, incorporated in, or otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary; or (d) any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs (a) through (c) possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity.

#### 14. Prohibited Transactions

BIS proposes to define “prohibited transactions” as, collectively, the transactions described in §§ 791.302 (Prohibited VCS hardware transactions), 791.303 (Prohibited covered software transactions), or 791.304 (Related prohibited transactions). The term prohibited transactions refers to the prohibitions on the knowing import of VCS hardware into the United States that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, as specified in section 791.302; the knowing Sale within, or import into, the United States of a completed connected vehicle containing covered software that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, as specified in § 791.303; and the knowing Sale of completed connected vehicles that incorporate VCS Hardware or covered software by connected vehicle

Manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, as specified in § 791.304.

#### 15. Sale

BIS proposes to define “sale,” in the context of this subpart, as distributing for purchase, lease, or other commercial operations a new completed connected vehicle for a price, to include the transfer of completed connected vehicles from a connected vehicle manufacturer to a dealer or distributor, as those terms are defined in 49 U.S.C. 30102. This definition also applies to the related terms such as sell or selling. This would include direct-to-consumer sales of completed connected vehicles from the connected vehicle manufacturer to the ultimate purchaser.

#### 16. Software Bill of Materials

BIS proposes to define “Software Bill of Materials” or SBOM as a formal and dynamic, machine-readable inventory detailing the software supply chain relationships between software components and subcomponents, including software dependencies, hierarchical relationships, and baseline software attributes, including author’s name, timestamp, supplier name, component name, version string, component hash, package URL, unique identifier, and dependency relationships to other software components.

BIS understands that this definition generally conforms to industry standards. However, BIS is specifically seeking comment on the feasibility, technical burden, cost, and effectiveness of identifying and disclosing to BIS the listed SBOM attributes.

#### 17. Vehicle Connectivity System

BIS proposes to define “Vehicle Connectivity System” or VCS as a hardware or software item for a completed connected vehicle that has the function of enabling the transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz. This definition would exempt most remote keyless entry fobs and immobilizers and certain internal wireless sensors and relays. VCS software is included in the definition of Covered Software.

#### 18. VCS Hardware

BIS proposes to define “VCS hardware” as the following software-enabled or programmable components and subcomponents that support the function of Vehicle Connectivity Systems or that are part of an item that

supports the function of Vehicle Connectivity Systems: microcontroller, microcomputers or modules, systems on a chip, networking or telematics units, cellular modem/modules, Wi-Fi microcontrollers or modules, Bluetooth microcontrollers or modules, satellite navigation systems, satellite communication systems, other wireless communication microcontrollers or modules, and external antennas. VCS hardware does not include component parts that do not contribute to the communication function of VCS hardware (e.g., brackets, fasteners, plastics, and passive electronics). VCS hardware would include aftermarket devices not contained in a completed connected vehicle at sale but that could be later integrated into or attached to the vehicle to perform VCS functions.

BIS believes this definition appropriately identifies the various components, contained within a TCU or other connected systems of a connected vehicle, that facilitate off-board data transmission, and, thus, are most likely to pose the risks identified in Section IV of this notice. BIS specifically seeks comment on this list of components and the appropriateness of their inclusion to address the national security risks that BIS has identified in this notice.

#### 19. VCS Hardware Importer

BIS proposes to define "VCS hardware importer" as a U.S. person importing VCS hardware for further manufacturing, integration, resale, or distribution. A connected vehicle manufacturer may be a VCS Hardware Importer if VCS hardware has already been installed in a connected vehicle when imported by the connected vehicle manufacturer.

This definition would capture OEMs, and tier 1 and tier 2 suppliers importing VCS hardware into the United States. BIS specifically seeks comment on the scope of this definition, particularly regarding whether it captures the breadth of market participants dealing in VCS Hardware.

#### 20. United States

BIS proposes to define "United States" to mean the United States of America, the States of the United States, the District of Columbia, and any commonwealth, territory, dependency, or possession of the United States, or any subdivision thereof, and the territorial sea of the United States.

#### *b. Prohibitions on Certain Transactions Related to Connected Vehicles*

##### 1. Prohibited Transactions

Under the proposed rule, VCS hardware importers would be

prohibited from knowingly importing into the United States any VCS hardware that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. BIS specifically seeks comment on this approach and whether additional components should be included in or excluded from this prohibition.

Connected vehicle manufacturers would be prohibited from knowingly Selling within the United States, or importing into the United States, completed connected vehicles that incorporate covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

Connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia would also be prohibited from knowingly Selling in the United States completed connected vehicles that incorporate covered software or VCS hardware. As with other connected vehicle manufacturers, connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia participate in the design and development of VCS hardware and covered software, which are generally built to the manufacturers' specifications. However, this prohibition applies even if connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia were not involved in the design or development of the VCS Hardware and Covered Software. Their Sale of those completed connected vehicles constitutes the supply of VCS hardware and covered software and is thus captured by this prohibition. To be clear, BIS anticipates that because of the role connected vehicle manufacturers play in the design and development of the key components in connected vehicles, in many cases, this prohibition will be duplicative of the other prohibitions in this proposed rule. BIS seeks comments on the efficacy of all of the proposed prohibitions detailed above.

As noted above, for the purposes of this proposed rule, BIS defines the term "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" to mean (a) any person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign

adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary; (b) any person, wherever located, who is a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, and is not a United States citizen or permanent resident of the United States; (c) any corporation, partnership, association, or other organization with a principal place of business in, headquartered in, incorporated in, or otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary; or (d) any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs (a) through (c) possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity.

To provide further clarity regarding transactions involving VCS hardware and covered software that would be prohibited, BIS offers the following examples of persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC and Russia:

*Example 1:* Company A, incorporated in the United States, is a wholly owned subsidiary of Company B. Company B is a state-owned enterprise of the PRC or Russia. Because Company B is a state-owned enterprise, Company A would be considered "owned by" the PRC or Russia.

*Example 2:* Company A is a joint venture between Company B and Company C where Company C owns a majority share of Company A. Company B is a corporation incorporated in a third-party jurisdiction. Company C is a state-owned enterprise of the PRC or Russia. Company A would be considered "owned by" the PRC or Russia.

*Example 3:* Company A is majority owned in aggregate by multiple state-owned enterprises and state-owned investment funds of the PRC or Russia. Company A would be considered "owned by" the PRC or Russia.

*Example 4:* Company A, incorporated in the United States, is a subsidiary of

Company B. Company B is a private company incorporated in the PRC or Russia with its principal place of business in the PRC or Russia. Because Company B is subject to the jurisdiction of the PRC or Russia, Company B's subsidiary, Company A, is controlled by an entity subject to the jurisdiction of the PRC or Russia and would be considered "controlled by" and "subject to the direction of" the PRC or Russia.

*Example 5:* Company A is a multinational company where a majority of the voting power is held by Company B, a PRC or Russian government investment fund. Company A would be "controlled by" and "subject to the direction of" the PRC or Russia.

*Example 6:* Company A is a holding company organized in a tax-advantaged jurisdiction. Company A is publicly listed on a stock exchange and its corporate voting structure is characterized by Class A and Class B shares, Class B shares having ten times the voting power of Class A shares. If the aggregate voting power of shareholders subject to the jurisdiction of the PRC or Russia holding either Class A and Class B shares constitutes a majority or a dominant minority of total voting power, then Company A would be "controlled by" and "subject to the direction of" the PRC or Russia.

*Example 7:* Company A, a company that is organized under the laws of the PRC or Russia, owns a minority interest in Company B, a U.S. business. Based on special voting powers vested in that minority interest, Company A maintains certain veto rights that determine important matters affecting Company B, including the right to veto the dismissal of senior executives of Company B. Company B would be considered "controlled by" and "subject to the direction of" Company A, and therefore owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

*Example 8:* Company A is an entity incorporated in a third country and Company B is an entity incorporated in the PRC or Russia. Company A and Company B create a new joint venture, Company C, to design, develop, and manufacture a new product. Company A and Company B own minority shares of the joint venture while Company D, a holding company wholly owned by a PRC citizen, owns the largest minority share. If aggregate voting power of Company B and Company D constitutes majority or dominant minority voting share, Company C would be "controlled by" and "subject to the direction of" the PRC or Russia.

*Example 9:* Company A has eight members on its board of directors. Company A is characterized by a shareholder and corporate governance structure that requires a 75 percent supermajority for any significant business decision. Three of the members of the board are citizens of, and therefore subject to the jurisdiction of, the PRC or Russia. Because these three members make up 37.5 percent of the voting power of the board, they can block any supermajority and therefore determine, direct, or decide important matters affecting Company A. Company A would be "controlled by" or "subject to the direction of" the PRC or Russia.

*Example 10:* The PRC or Russian government, through an investment fund, acquires a 1% special management share in Company A. This share grants the PRC or Russian government the right to appoint a director to the board of Company A and veto certain key business decisions, such as major strategic changes or mergers. This share allows the government to influence Company A's operations and strategy. Company A would be "controlled by" the PRC or Russia.

*Example 11:* Company A maintains its principal place of business in the PRC or Russia. Company A would be "subject to the jurisdiction" of the PRC or Russia.

*Example 12:* Company A is a publicly listed U.S. corporate entity. Company A has a wholly owned subsidiary, Company B, that is organized under the laws of the PRC or Russia and manufactures goods in the PRC or Russia. Because Company B is organized under the laws of the PRC or Russia, Company B would be subject to the jurisdiction of the PRC or Russia. However, Company A is not subject to the jurisdiction of the PRC or Russia by nature of its subsidiary, Company B, being "subject to the jurisdiction" of the PRC or Russia.

*Example 13:* Company A is privately held and incorporated in the United States. One member of Company A's board of directors, Person X, a former chairman of the board of a large PRC corporation, has known ties to the government of the PRC, owns a large minority share of Company A, and has previously made significant investments in other companies founded by Company A's chief executive officer. Person X also facilitated a large minority investment in Company A by the large PRC corporation where they were previously chairman of the board. Person X's professional background indicates that they are directly or indirectly supervised, directed,

controlled, financed, or subsidized by the PRC government. The combination of Person X's close ties to Company A's CEO, Person's X's ownership interest and ability to direct investment from large, highly regulated PRC corporate entities, and Person X's close ties to the PRC government indicate that Company A would be "subject to the direction" of the PRC.

BIS seeks comment on whether the definition of, and examples provided to illuminate, who is a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary," provides sufficient clarity regarding the circumstances under which the rule's prohibitions might apply.

For additional clarity in determining whether a transaction involving VCS hardware or covered software designed, developed, manufactured, or supplied by entities described above would be prohibited under the proposed rule, BIS offers the below examples. In offering these examples, BIS emphasizes that VCS hardware and covered software would not be considered designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, solely based on the country of citizenship of natural persons who are employed, contracted, or otherwise similarly engaged to participate in the design, development, manufacture, or supply of that VCS hardware or covered software:

*Example 14:* A U.S. person has a contractual relationship with a foreign person to import a cellular module, and the cellular module will later be integrated into a VCS for a completed connected vehicle. The U.S. person is, under the proposed rule, a VCS hardware importer. The U.S. person knows the cellular module was manufactured at a facility located in the PRC or Russia and is being imported through a third country. Since the entity manufacturing the module would, at a minimum, be "subject to the jurisdiction" of the PRC or Russia, the import of the module would be a prohibited transaction under the proposed rule, unless it qualifies for a general authorization or a specific authorization from BIS.

*Example 15:* A U.S. person imports a TCU that was assembled in a third country, but that contains a microcontroller that is manufactured in the PRC or Russia and is sold to the third-country assembler of the TCU. The U.S. person knows that the microcontroller was manufactured by an entity located in the PRC or Russia. As the microcontroller is included in the



definition of VCS hardware, the import of the TCU for a completed connected vehicle would be a prohibited transaction under the proposed rule unless it qualifies for a general authorization, or a specific authorization granted by BIS.

*Example 16:* A U.S. person imports a completed connected vehicle, making the U.S. person a connected vehicle manufacturer under the proposed rule's definition. The completed connected vehicle contains a TCU that operates software supporting off-vehicle connectivity above 450 MHz, and that software is designed, developed, or otherwise supplied (in whole or in part) by an entity located in the PRC or Russia. Under the proposed rule, the import of the completed connected vehicle would be prohibited, unless it was authorized by a general authorization or a Specific Authorization.

*Example 17:* A U.S. person who is a connected vehicle manufacturer that manufactures or assembles completed connected vehicles in the United States sells to a dealer within the United States a completed connected vehicle in which the vehicle's ADS software for object detection, classification, and decision making is proprietary software designed, developed, or supplied by an entity in the PRC or Russia. The sale or transfer of the completed connected vehicle would be a prohibited transaction under the proposed rule unless it qualifies for a general authorization or specific authorization granted by BIS.

*Example 18:* A U.S. person who is a connected vehicle manufacturer utilizes foreign VCS and ADS software development teams through various subsidiaries, joint ventures, and contract arrangements, some of which retain servicing obligations, contractual and licensing rights, and other interests in the software they have developed. One of those software development teams is located in the PRC or Russia, and as such, that software team is subject to the jurisdiction of the PRC or Russia. Given the role of PRC or Russian developers in the creation of the VCS or ADS software (covered software), the sale of a completed connected vehicle within the United States that integrates this proprietary covered software, would be a prohibited transaction under the proposed rule, unless it qualifies for a general authorization or specific authorization granted by BIS.

*Example 19:* A U.S. person who is a connected vehicle manufacturer utilizes VCS and ADS software development teams around the world through various subsidiaries, joint ventures, and contract

arrangements. One of those software development teams is comprised of individuals who are PRC or Russian citizens working in a foreign jurisdiction other than the PRC or Russia for a company that is not owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Although the individuals technically meet the definition of "person owned by, controlled by, or subject to the direction of a foreign adversary," the sole fact that PRC or Russian citizens work on the connected vehicle manufacturer's software development would not make the sale of a completed connected vehicle within the United States that integrates this VCS or ADS software a Prohibited Transaction under the proposed rule.

*Example 20:* Company A, which is a wholly owned subsidiary of a foreign corporation in which a PRC or Russian entity owns a controlling interest, imports completed connected vehicles that incorporate covered software and VCS hardware, none of which was originally designed, developed, manufactured, or supplied by an entity owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. In such rare circumstance where Company A did not participate in the design or development of the covered software or VCS hardware, Company A would submit (once per Model Year) a Declaration of Conformity for the import of the completed connected vehicles containing covered software and VCS hardware. However, any subsequent sale by Company A of such completed connected vehicle in the United States would be prohibited. For example, Company A subsequently sells such completed connected vehicles to a dealer in the United States. Because Company A is a person controlled by the PRC or Russia and has direct privileged access to the VCS Hardware and covered software prior to the sale, the knowing sale by Company A of the completed connected vehicle with VCS hardware and covered software would be a prohibited transaction under the proposed rule, and a specific authorization from BIS would be required before engaging in such a transaction.

*Example 21:* Company A, a wholly owned subsidiary of a PRC or Russia corporation manufactures completed connected vehicles in the United States. The completed connected vehicles that Company A manufactures incorporate covered software and VCS hardware provided by Company B, a company that is not owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Because Company A

is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, participated in the design and development of the covered software or VCS hardware, and in any event, has direct and privileged access to its completed connected vehicles—including the incorporated covered software and VCS hardware—Company A's sale of the completed connected vehicles is a prohibited transaction under the proposed rule, and a specific authorization from BIS would be required before engaging in such a transaction.

### c. Compliance

#### 1. Declaration of Conformity

BIS proposes to require VCS Hardware Importers and connected vehicle manufacturers engaged in specified transactions to submit Declarations of Conformity to BIS certifying that they have not engaged in a prohibited transaction. Under the proposed rule, declarants would be responsible for submitting information to BIS, including documentation collected from suppliers of components of VCS hardware and from suppliers of covered software, to verify compliance with the regulations. These requirements include obtaining and analyzing the HBOMs for VCS hardware and the SBOMs for covered software and providing documentation of the steps the declarant took to verify that the transactions comply with the provisions of the rule. In an effort to facilitate compliance, BIS is not currently proposing to mandate particular due diligence requirements but would rather allow VCS hardware importers and connected vehicle Manufacturers to provide evidence of their own efforts tailored to their unique operations. BIS seeks comment on this approach.

The proposed rule generally contemplates that Declarations of Conformity would be submitted in three instances by persons not engaged in prohibited transactions: (1) Declarations submitted by VCS hardware importers; (2) Declarations submitted by connected vehicle manufacturers importing completed connected vehicles containing covered software into the United States; and (3) Declarations submitted by connected vehicle manufacturers selling completed connected vehicles in the United States that they have manufactured or assembled in the United States and which contain covered software, so long as there is a continuing foreign interest in the covered software. Persons required to submit a Declaration of

Conformity need do so once per model year for units associated with a vehicle model year, or calendar year for units not associated with a vehicle model year, and only for the categories of transactions they seek to execute during that period. VCS hardware importers or connected vehicle manufacturers engaging in multiple transactions that require submissions of Declarations of Conformity under separate paragraphs of § 791.305 may, if they prefer, submit a single compiled Declaration of Conformity containing all required information for all transactions. For example, an OEM that manufactures or assembles completed connected vehicles in the United States, imports connected vehicles into the United States, and imports VCS hardware into the United States would be able to submit a single Declaration of Conformity based on vehicle make, model, and trim and VCS hardware that will be imported or manufactured that Model Year.

BIS believes that Declarations of Conformity will be an important tool for advancing the goals of this proposed rule, and addressing the emergency declared in E.O. 13873. Declarations of Conformity will first and foremost provide BIS with a means to verify VCS hardware importers' and completed connected vehicle manufacturers' compliance with the proposed prohibitions. Through extensive engagement with connected vehicle manufacturers and automotive suppliers, BIS has come to understand that connected vehicle supply chains are complex and often opaque, with potentially hundreds of suppliers for a single connected vehicle in a given model year. Such complexity and opacity could result in the incorporation into connected vehicles of VCS hardware and covered software that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries, without the full knowledge of the connected vehicle manufacturer. While connected vehicle manufacturers typically have strong relationships with their immediate suppliers, to include the development of years-long supply contracts that span entire vehicle generations, their understanding of the deeper supply chain (to include who is supplying their suppliers) is substantially weaker. Additionally, while the COVID-19 pandemic and associated supply chain crisis forced connected vehicle manufacturers to more critically evaluate their hardware supply chains, illumination of software

supply chains remains largely unachieved. Consequently, BIS believes that the requirement to submit annual Declarations of Conformity will serve as an important mechanism for ensuring that parties subject to this proposed rule implement the due diligence and other procedures necessary to fully understand the supply chains for their VCS hardware and covered software and thus comply the proposed rule's prohibitions on the incorporation of VCS Hardware or covered software that has been designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

BIS also believes that the collection of annual Declarations of Conformity from connected vehicle manufacturers and VCS hardware importers would facilitate enforcement of the proposed rule, including by allowing BIS to proactively identify red flags and potential violations of the proposed prohibitions. For example, BIS may rely on the broad perspective provided by the Declarations of Conformity from multiple connected vehicle manufacturers and VCS hardware importers to identify previously undetected participation by PRC or Russian designers, developers, manufacturers, or suppliers that are subject to the prohibitions of this proposed rule yet remain entrenched in the U.S. connected vehicle supply chain. Additionally, these Declarations of Conformity would allow BIS to maintain an understanding of technological advancements and changes in the U.S. connected vehicle industry—both in hardware and software—and consequently enable BIS to propose updates to the rule as needed to maximize its effectiveness in mitigating the undue and unacceptable risks posed by the PRC and Russia while minimizing burden on industry.

The sections below explain in greater detail the types of Declaration of Conformity that would be required under the proposed rule. BIS seeks comment on this regulatory approach, including the necessity and efficacy of requiring Declarations of Conformity with respect to VCS hardware and covered software in which there is a Foreign Interest. BIS also seeks comment on the availability and efficacy of any alternative approach that would require a narrower set of VCS Hardware Importers and completed connected vehicle manufacturers to submit Declarations of Conformity, while still achieving the goals of the Declaration of Conformity requirement

and addressing the declared emergency under E.O. 13873.

#### i. Import of VCS Hardware

The Declaration of Conformity described in § 791.305(a)(1) would require VCS hardware Importers to provide information on the specific VCS hardware that the declarant plans to import into the United States for a given model year, or, for units not associated with a model year, a given calendar year. BIS proposes to require the Declaration of Conformity to contain the FCC ID number(s) of the VCS hardware, and, if applicable, any subcomponents in the VCS hardware that also have an FCC ID number. FCC regulations at 47 CFR 2.925 require any electronic device that emits RF waves, including those imported into the United States, to have an FCC ID number, which is used to identify and certify that the device meets the necessary regulatory standards for wireless communication. The proposed rule would additionally require VCS Hardware Importers to report all third-party information technology external endpoints to which the VCS Hardware is programmed to connect, including the country in which said endpoint is located and/or the identity and location of the service provider. This would include any third-party that is not the VCS hardware importer nor the final recipient, such as the connected vehicle manufacturer that integrates the VCS hardware and receives data on an episodic or ongoing basis from the VCS hardware. Additionally, VCS hardware importers would be required to submit an HBOM as part of the Declaration of Conformity. BIS would expect, consistent with the proposed definition for this term, this HBOM to include a comprehensive list of parts and technical information, including the provenance of subcomponents contained within the VCS hardware.

#### ii. Import of Completed Connected Vehicles

The Declaration of Conformity described in section 791.305(a)(2) would require connected vehicle manufacturers that import completed connected vehicles, including U.S.-based OEMs and foreign-headquartered OEMs with operations in the United States, to provide information to BIS on the make, model, and trim (if known) of the imported group of completed connected vehicles and the covered software contained within the completed connected vehicles. BIS proposes to require declarants to submit an SBOM for the covered software related to both VCS and ADS. The



minimum requirements for the SBOM are author's name, timestamp, supplier name, component name, version string, component hash, package URL, unique identifier, and dependency relationships to other software components. Declarants may submit additional SBOM information as evidence demonstrating the covered software is not sourced from PRC or Russian-linked entities. BIS seeks comment on all aspects of this SBOM requirement.

### iii. Manufacture or Assembly of Completed Connected Vehicles for Sale in the United States

Similarly, this proposed rule, as described in section 791.305(a)(3), would require connected vehicle Manufacturers that manufacture or assemble completed connected vehicles for sale in the United States to submit a Declaration of Conformity that includes information on the make, model, and trim of the group of completed connected vehicles and the covered software contained within the completed connected vehicles that the connected vehicle manufacturer will sell for a Model Year. BIS emphasizes that this requirement would apply only to connected vehicle manufacturers whose vehicles incorporate covered software in which there is a foreign interest. Connected vehicle manufacturers who manufacture or assemble completed connected vehicles in the United States and whose vehicles contain no covered software in which there is a foreign interest would not be required to submit a Declaration of Conformity. However, given the global nature of automotive software supply chains, BIS anticipates that nearly all connected vehicle manufacturers of completed connected vehicles for Sale in the United States would be required to submit an annual Declaration of Conformity covering all completed connected vehicles by make, model, and trim to be manufactured for Sale in the United States for each Model Year. As detailed above, this requirement would include the submission of an SBOM for covered software incorporated into the group of completed connected vehicles.

### iv. Procedures To Submit Declarations of Conformity

VCS Hardware Importers and connected vehicle manufacturers submitting a Declaration of Conformity under this rule would be required to submit the Declaration of Conformity to BIS annually, 60 days prior to the first sale or first import of a Vehicle Identification Number (VIN) series of completed connected vehicles

comprised of a single model year, or 60 days prior to the import of VCS hardware covered by the Declaration of Conformity. VCS hardware importers and connected vehicle manufacturers may, at their discretion, submit a combined Declaration of Conformity, or may submit separate Declarations of Conformity (e.g., one Declaration covering import of VCS hardware and another covering import of completed connected vehicles). Declarations of Conformity covering both the import or manufacture of completed connected vehicles and the import of VCS Hardware should be submitted by the earlier of the two reporting dates. connected vehicle manufacturers that would submit a Declaration of Conformity for the import of a group of completed connected vehicles into the United States should not submit a Declaration of Conformity related to the subsequent Sale of that same group of Completed Connected Vehicles. In the event of material changes that impact the content of the Declaration of Conformity, VCS hardware importers or connected vehicle manufacturers would be required to submit an updated Declaration of Conformity and an updated HBOM or SBOM within 30 days of such a change. Such changes may include changes in the suppliers of key subcomponents or functional aspects of the VCS hardware or covered software incorporated in the completed connected vehicle. BIS would make a web portal available on its website (<https://www.bis.gov>) through which VCS Hardware Importers and connected vehicle manufacturers may submit Declarations of Conformity.

### 2. General Authorizations

General Authorizations would allow certain VCS Hardware Importers and connected vehicle manufacturers to engage in otherwise prohibited transactions without the need to notify BIS prior to engaging in the transaction. connected vehicle manufacturers or VCS hardware importers (and entities under common control, including parents) who produce small quantities of completed connected vehicles or VCS hardware, which the proposed rule defines as fewer than 1,000 units in a calendar year, would be eligible for a general authorization. This is in line with requirements for high-volume and low-volume manufacturers found in 49 CFR part 565. BIS specifically seeks comment on this threshold for both completed connected vehicles and VCS Hardware. connected vehicle manufacturers would be eligible for a general authorization if the completed connected vehicle is otherwise subject

to a prohibition but will be used on public roadways fewer than 30 days in any calendar year. For purposes of this general authorization, each use of a completed connected vehicle on public roadways on a distinct calendar day will count toward the 30-day limit, regardless of the duration of a vehicle's use on a particular day. VCS hardware importers and connected vehicle manufacturers would also qualify for a general authorization for otherwise prohibited transactions involving completed connected vehicles incorporating covered software or VCS hardware if the completed connected vehicles are used only for testing display, or research purposes and not on public roads in the United States. Lastly, VCS hardware importers or connected vehicle manufacturers would qualify for a general authorization for the importation of completed connected vehicles incorporating covered software or the importation of VCS Hardware solely for the purposes of repair, alteration, or competition off public roads, and the vehicle or hardware will be reexported from the United States within one year of the time of import.

BIS proposes to allow persons using General Authorizations to self-certify their compliance with the applicable General Authorization. As such, these persons would not need to submit documentation to BIS but would be required to gather and maintain full records for a period of 10 years documenting compliance for all completed connected vehicles and VCS hardware covered by the general authorization. Furthermore, persons availing themselves of a general authorization would be required to continuously monitor for any changes that render a transaction ineligible for continued reliance on the general authorization. A VCS hardware importer or connected vehicle manufacturer that is no longer eligible for a general authorization would need to apply for and receive a specific authorization before engaging in an otherwise prohibited transaction. For example, connected vehicle manufacturers who import a certain model or trim of completed connected vehicles containing covered software that are originally used for display or testing purposes must seek a specific authorization before importing that model or trim of completed connected vehicle for more general use in the United States.

A connected vehicle manufacturer or VCS hardware importer that is a subsidiary, joint venture, affiliate, or other entity subject to the ownership, control, jurisdiction, or direction of the

PRC or Russia would be ineligible for general authorizations and would be required to apply for a specific authorization before engaging in an otherwise prohibited transaction.

### 3. Specific Authorizations

VCS hardware importers and connected vehicle manufacturers wishing to engage in an otherwise prohibited transaction who are ineligible for an exemption or general authorization would have to apply for and receive a specific authorization to engage in the otherwise prohibited transaction. The purpose of specific authorizations is to allow BIS on a case-by-case basis to determine the nature and scope of the undue or unacceptable risk to U.S. national security posed by transactions involving VCS hardware and covered software, including the extent of foreign adversary involvement in the transactions, as well as potential mitigations.

VCS hardware importers and connected vehicle manufacturers must not engage in an otherwise prohibited transaction until BIS grants the application for a specific authorization. If a party engages in a prohibited transaction prior to receiving a specific authorization from BIS, that transaction would constitute a violation of the regulation. Specific authorization requests will be reviewed on a case-by-case basis, and the time to reach a decision on an application for a specific authorization will vary based on the complexity of the case. However, BIS will respond to applicants with a processing update within 90 days of the initial application for a specific authorization, and typically endeavor to provide either a request for more information or a decision within that time period.

Applications for a specific authorization must contain complete information on the proposed transaction, including every party involved, an overview of the covered software and/or the VCS hardware designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, the intended use of the covered software and/or VCS hardware, and documentation to support the information contained in the application. Persons seeking a specific authorization would submit an application via a web portal that would be available on the BIS website. Applicants should take care to submit to BIS only one copy of an application pertaining to each transaction for which they seek specific authorization to avoid

processing delays. BIS may request additional information from an applicant about any matter related to the specific authorization request. In rare situations, as part of its review of an application for specific authorization, BIS may, in its sole discretion, request an oral briefing by the applicant and any other relevant parties. At any point between initial submission of an application for specific authorization and a final decision issued by BIS, an applicant may submit additional information to bolster the application or provide clarity on any aspect thereof.

When reviewing applications for a specific authorization, BIS will consider the factors that may pose undue or unacceptable risks, particularly as they relate to transactions that could result in the exfiltration of connected vehicle or U.S. persons' data, or the remote manipulation or operation of a connected vehicle. Examples of factors that BIS may consider include: the applicant's ability to limit PRC or Russian government access to, or influence over the design, development, manufacture, or supply of the VCS hardware or covered software; security standards used by the applicant and if such standards can be validated by BIS or a third-party; and other actions or proposals the applicant offers to implement as a way to mitigate undue or unacceptable risk.

BIS's decision regarding any application for specific authorization will apply only to the specific parties and transaction outlined in the application and described in the decision notice. Additionally, the decision notice from BIS to the applicant(s) may contain any conditions that must be met by the parties for a transaction to be authorized. Such conditions, which are subject to revision by BIS, may include technical controls (e.g., software validation) or operational controls (e.g., physical and logical access monitoring procedures), that are either permanent or temporary. These controls will focus on the supply chain element that involves a link to a foreign adversary to mitigate any undue or unacceptable risk posed by the transaction. For connected vehicle manufacturers owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, a specific authorization may include a requirement that all VCS hardware and covered software be assembled and integrated into the connected vehicle in the United States. In the approval letter for specific authorization, BIS will determine the effective date and duration of the authorization on a case-by-case basis.

While applicants denied authorizations would not be precluded from submitting new applications for specific authorizations with regard to different transactions (involving different parties and/or different covered software or VCS hardware), BIS will reconsider a previously denied application for a specific authorization only if the applicant demonstrates a material change in circumstances.

### 4. Exemptions

Transactions by VCS hardware importers and connected vehicle manufacturers would be exempt from the proposed prohibitions for a limited period. BIS proposes a shorter implementation period for transactions involving covered software and proposes a longer implementation period for transactions involving VCS hardware to allow market participants adequate time to establish alternative supply chains if necessary. This reflects BIS's understanding, and numerous public comments underscoring, that hardware supply chains for Connected Vehicles are complex and require multiple years to alter. VCS hardware importers would be permitted to engage in otherwise prohibited transactions involving VCS Hardware and would also be exempt from a requirement to submit a Declaration of Conformity for transactions not otherwise prohibited so long as: (1) for VCS hardware units not associated with a vehicle model year, the import of the VCS hardware takes place prior to January 1, 2029; or (2) the VCS hardware is integrated into a connected vehicle (completed or incomplete) or destined for a connected vehicle with a model year prior to 2030. Beginning January 1, 2029, any VCS hardware importer seeking to engage in a transaction subject to the VCS hardware prohibitions in § 791.302 (other than the import of a connected vehicle with a model year prior to 2030) would be required to obtain a specific authorization if the transaction is not otherwise permitted by a general authorization. Furthermore, VCS hardware importers seeking to import VCS hardware beginning on January 1, 2029, or VCS Hardware in completed connected vehicles or that is destined for connected vehicles starting with Model Year 2030, would be required to submit an annual Declaration of Conformity to BIS, unless obligated to seek a Specific Authorization. Connected vehicle manufacturers would be permitted to engage in otherwise Prohibited Transactions involving covered software designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to

the jurisdiction or direction of the PRC or Russia, so long as the completed connected vehicle that is imported or sold is of a model year prior to 2027. Beginning Model Year 2027 (as imported into or sold in the United States), any connected vehicle manufacturer seeking to engage in a prohibited transaction involving covered software specified in section 791.303 would be required to obtain a specific authorization if the transaction is not otherwise permitted by a general authorization. Furthermore, connected vehicle manufacturers would be required to submit an applicable Declaration of Conformity for imports or Sales of all completed connected vehicles beginning in Model Year 2027. Connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia would be permitted to engage in otherwise prohibited transactions so long as the completed connected vehicle that is Sold is of a Model Year prior to 2027. Beginning Model Year 2027 (as Sold in the United States), these particular connected vehicle manufacturers seeking to engage in a prohibited transaction specified in § 791.304 would be required to obtain a specific authorization if the transaction is not otherwise permitted by a general authorization.

#### 5. Appeals

BIS proposes to create a mechanism by which any person whose application for a specific authorization is denied, whose specific authorization is suspended or revoked, or who has received a written notification of ineligibility for a general authorization may appeal that decision to the Under Secretary. Appeals must be submitted in writing by email or mail to the Office of the Under Secretary within 45 days of the date on the notice of the adverse administrative action by BIS. The appeal must detail how the party submitting the appeal has been directly and adversely affected by BIS's action, and the reasons that BIS's action should be reversed or otherwise modified. The Under Secretary, at his or her discretion, may delegate to the Deputy Under Secretary for Industry and Security or another BIS official the review of appeals, including arranging, at the official's discretion, informal hearings with relevant parties regarding the appeal.

Appellants may submit supplementary information in support of their appeal, whether *sua sponte* or at the request of the Under Secretary or the designated official, but, though the Under Secretary or designated official

generally would not consider additional information submitted *sua sponte* more than 30 days after submission of the original appeal. If the Under Secretary or designated official requests supplementary information, appellants will have no more than 30 calendar days to respond to the request. Appellants may also request an in-person informal hearing in writing at the time of submission. A hearing is not required, and the Under Secretary or designated official may, at his or her discretion, grant or deny a request for an informal hearing.

#### 6. Advisory Opinions

In response to public comments regarding the ANPRM, BIS proposes to include a mechanism for BIS to issue advisory opinions, similar to the process outlined in the Export Administration Regulations (EAR). BIS anticipates this process will provide connected vehicle manufacturers, VCS hardware importers, and other interested parties with greater clarity about how to comply with the proposed rule on an as-needed basis. As with the EAR, BIS emphasizes that advisory opinions provided under this proposed rule would in no way serve as evidence that the ICTS transaction addressed in the opinion is not subject to the jurisdiction of another U.S. Government agency. BIS may publish on its website an advisory opinion that may be of broad interest to the public, with redactions where necessary to protect Confidential Business Information. To solicit an advisory opinion from BIS, persons would be required to submit a written request to BIS by email or through a portal that will be available on the BIS website. BIS will not accept advisory opinion requests submitted by mail. A request for an advisory opinion must contain contact information for the submitter as well as all current information on the prospective transaction to assist BIS in making a determination. This would include technical details on the involved VCS hardware or covered software, information on the completed connected vehicle (if applicable), the SBOM and/or HBOM for the covered software and/or VCS hardware, and any other supporting materials that the submitter assesses will assist BIS in determining if the transaction may be prohibited by this rule. Persons seeking an advisory opinion are encouraged to submit as much pertinent information as possible in the initial request for an advisory opinion, but BIS may request more information as needed to formulate its opinion. BIS will only consider advisory opinion requests for

actual, not hypothetical, prospective transactions in which all parties, as opposed to anonymous parties, are identified. Additionally, parties may only rely on an advisory opinion when engaging in a transaction if the original Advisory Opinion request contained complete and accurate information and only so long as such information remains accurate following the issuance of the Advisory Opinion.

#### 7. "Is-Informed" Notices

BIS could notify connected vehicle manufacturers or VCS hardware importers, either through direct letters or through a **Federal Register** notice meant to inform a broader set of persons, that a transaction involving certain covered software, VCS hardware, or entities requires a specific authorization because it would constitute a Prohibited Transaction according to the terms of this proposed rule. Any person who engages in a transaction covered by an "Is-Informed" notice without first receiving a Specific Authorization from BIS would have knowledge that such transaction is prohibited and would therefore be in violation of the rule. Is-Informed notices may only be delivered by or at the direction of the Under Secretary or a BIS employee designated by the Under Secretary.

#### 8. Recordkeeping and Reporting Requirements

BIS proposes to require connected vehicle manufacturers and VCS hardware importers to maintain complete records related to any transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required by this rule, for a period of ten years. This recordkeeping requirement applies regardless of whether the transaction is subject to a general authorization, specific authorization, or whether the connected vehicle manufacturer or VCS hardware importer has not yet sought an authorization. BIS would expect said records to include all information pertinent to a general authorization or submitted when applying for a Specific Authorization, as well as business records related to the execution of the transaction, such as contracts, import records, bills of sale, relevant correspondence, and all other files specified in sections 791.312 and 791.313 to assess compliance with the rule.

All connected vehicle manufacturers and VCS hardware importers would be required to submit records when requested by BIS related to any transaction for which a Declaration of

Conformity, general authorization, or specific authorization would be required by this rule, whether or not said transaction was carried out under a general authorization, specific authorization, or without an authorization from BIS. As such, BIS would be allowed to request business records, before, during, or after the transaction in question has taken place.

#### *d. Enforcement*

##### *1. Penalties*

IEEPA authorizes this rulemaking. Thus, persons who violate, attempt to violate, conspire to violate, or knowingly cause a violation of this rule, if finalized, may be subject to civil and/or criminal penalties under IEEPA (50 U.S.C. 1705), depending on the circumstances of the violation. Potential violations of this proposed rule that would be subject to penalties include engaging in a prohibited transaction without an applicable general authorization or specific authorization, or failure to abide by the conditions enumerated in a specific authorization. Willfully providing false or fictitious information to the U.S. Government may be subject to criminal fines, imprisonment, or both. A civil penalty may be imposed on any person who violates, attempts to violate, conspires to violate, or causes a violation of any authorization, order, regulation, or prohibition issued under IEEPA.

Under the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, the specific maximum civil penalty will be adjusted by notice in the *Federal Register* effective each calendar year by the Office of the Secretary of the Department of Commerce. At the time of publishing of this proposed rule, the maximum civil penalty for violations of IEEPA is \$368,136 per violation and the maximum criminal penalty is \$1,000,000.

Under the proposed rule, should BIS have reason to believe that a violation has occurred and intends to issue a civil monetary penalty, it will inform the alleged violator through a written notice of the intent to impose a penalty ("Pre-Penalty Notice"). BIS will generally transmit the Pre-Penalty Notice electronically but may additionally issue a mailed notice. The recipient of a Pre-Penalty Notice may respond in writing to BIS to provide additional information or otherwise contest the penalty. BIS must receive this response within 30 days of the transmission of the original pre-penalty notice. A response to a pre-penalty notice does not constitute a formal appeal, but it allows the recipient of the pre-penalty

notice to contest facts set forth by BIS in the pre-penalty notice, provide exculpatory evidence, or otherwise respond to the pre-penalty notice. BIS may seek to initiate settlement discussions in the pre-penalty notice or may conduct separate outreach following transmission of the pre-penalty notice. Recipients of a pre-penalty notice may additionally request to initiate settlement discussions in their response to BIS or may conduct separate outreach to do so.

Following the delivery of the pre-penalty notice and after considering any responses from the alleged violator, BIS will inform the alleged violator in writing as to whether it has found that a violation in fact occurred. Should BIS find that a violation has indeed taken place and no settlement has been reached, BIS will issue a final penalty notice to the violator specifying the violation and determining the specific civil monetary penalty to be imposed. This penalty may not be appealed following the procedures in section 791.309, but is a final agency action that the violator may contest in the appropriate U.S. District Court.

Should a violator fail to pay the penalty as specified in the final penalty notice or fail to make alternative payment arrangements approved by BIS, BIS may refer the matter to the Department of Treasury for administrative collection or to the Department of Justice for collection via civil suit in U.S. District Court.

##### *2. Finding a Violation*

Under the proposed rule, there may be cases in which BIS determines that a violation has taken place but that a civil monetary penalty is not appropriate. In such cases, BIS would issue a finding of violation that identifies the violation. The finding of violation could also contain an administrative response other than a civil monetary penalty, such as an order to cease and desist from conduct or activities that are prohibited by the proposed rule. Consistent with the procedures listed above regarding a pre-penalty notice, recipients of a finding of violation may file a response within 30 days contesting the facts of the finding of violation and/or providing information relevant to BIS's determination of whether a violation has occurred. BIS will consider any new information and inform the party in writing whether a violation has or has not occurred. A recipient that does not respond within 30 days of receipt of the finding of violation will be deemed to have waived the right to respond. Any action taken in a finding of violation

issued by BIS constitutes a final agency action that is not subject to appeal following the procedures in section 791.309.

##### *3. Severability*

BIS intends for the provisions of this proposed rule, as finalized to be severable from each other. If a court holds that any provision in a final 15 CFR part 791, subpart D, is invalid or unenforceable, BIS intends that the remaining provisions of a final 15 CFR part 791, subpart D, as relevant, would continue in effect to the greatest extent possible. In addition, if a court holds that any such provision is invalid or unenforceable as to a particular person or circumstance, BIS intends that the provision would remain in effect as to any other person or circumstance. Depending on the circumstances and the scope of the court's order, BIS believes that the remaining provisions of a final rule likely could continue to function sensibly independent of any provision or application held invalid or unenforceable. For example, the prohibitions related to transactions involving VCS Hardware could continue to apply as intended, even if a court finds that the prohibitions on transactions involving ADS are invalid. Similarly, the proposed rule could be applied with respect to relevant hardware and software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC, even if a court finds its application with respect to relevant hardware and software from Russian-linked persons is invalid.

#### *e. Classification*

##### *1. Executive Order 12866*

Executive Order 12866, as reaffirmed by Executive Order 13563 and amended by Executive Order 14094, directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributed impacts, and equity). This proposed rule has been designated a significant regulatory action by the Office of Information and Regulatory Affairs (OIRA) under section 3(f)(1) of Executive Order 12866, as amended by Executive Order 14094.

##### *2. Unfunded Mandates Reform Act of 1995*

This proposed rule would not produce a federal mandate (under the regulatory provisions of title II of the

Unfunded Mandates Reform Act of 1995) for state, local, and tribal governments or the private sector.

### 3. Executive Order 13132 (Federalism)

This proposed rule does not contain policies having federalism implications requiring preparations of a Federalism Summary Impact Statement.

### 4. Executive Order 12630 (Governmental Actions and Interference With Constitutionally Protected Property Rights)

This proposed rule does not contain policies that have takings implications.

### 5. Executive Order 13175 (Consultation and Coordination With Indian Tribes)

The Department has analyzed this proposed rule under Executive Order 13175 and has determined that the action would not have a substantial direct effect on one or more Indian tribes, would not impose substantial direct compliance costs on Indian tribal governments, and would not preempt tribal law.

### 6. National Environmental Policy Act

The Department has reviewed this rulemaking action for the purposes of the National Environmental Policy Act (42 U.S.C. 4321, *et seq.*). It has been determined that this proposed rule would not have a significant impact on the quality of the human environment.

### 7. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501, *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond nor be subject to a penalty for failure to comply with a collection of information subject to the requirements of the PRA, unless that collection has obtained OMB approval and displays a currently valid Office of Management and Budget (OMB) Control Number.

This proposed rule will create new information collection requirements, which are subject to review and approval by OMB under the PRA. Specifically, this proposed rule would require connected vehicle manufacturers and VCS hardware importers to submit annual Declarations of Conformity certifying that their import of VCS hardware and/or import or manufacture of completed connected vehicles does not involve hardware or software subject to the prohibitions in this proposed rule. Additional requirements for the Declarations of Conformity include supplying technical information regarding the hardware or software in question and providing a

Bill of Materials for applicable software, hardware, or both.

Moreover, entities seeking specific authorizations from BIS to engage in otherwise prohibited transactions will have to file information with the Department, submissions of which are also subject to the PRA. Applications for a specific authorization would require, but are not limited to, a description of the nature of the otherwise prohibited transaction(s). For entities that are covered by a General Authorization, a self-certification, without need to notify BIS, would be required (*see* Section VI of the NPRM). BIS proposes to require connected vehicle manufacturers and VCS hardware importers to maintain complete records related to any transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required by this rule for a period of ten years, consistent with IEEPA's statute of limitations. These records would include any transaction for which the connected vehicle manufacturer or VCS hardware importer has not yet sought an authorization. BIS expects said records to include all information submitted in applications, as well as business records related to the execution of any ICTS transaction subject to the rule, such as contracts, import records, bills of sale, and all other files BIS may deem pertinent in assessing compliance with this proposed rule. Lastly, entities seeking an advisory opinion from BIS would have to file information with the Department, though this is an optional process for parties looking for additional clarity on proposed transactions. BIS anticipates that this collection would be largely similar to its program in administering 15 CFR 748.3, as it would require similar information and the process for submission is analogous. BIS seeks comment on how many entities would request an advisory opinion in order to better understand the associated costs.

BIS estimates that the initial burden placed on applicable entities would be 180 to 240 hours. This estimate takes into account the one-time initial cost (in hours) per entity to comply with the rule, including reading and understanding the rule's provisions. Every subsequent year, BIS anticipates that the total annual cost burden (in hours) for applicable entities to implement the rule would be 100 to 500 hours.

BIS assesses that there are 42 to 281 entities potentially impacted by the proposed rule and that the initial cost burden for these entities is between \$30,964 and \$38,554. This estimate takes into account the one-time initial

cost per entity to comply with the rule, including reading and understanding the rule's provisions. Every subsequent year, BIS anticipates that the total annual cost burden for applicable entities to implement the rule will be \$16,133 to \$80,667 a year (average of operations manager, engineer, and lawyer hourly salaries in Table 2 [ $\$484/\text{hour}/3 = \$161.33$ ] \* [100 and 500 hours]). The annual cost burden placed on impacted entities includes (but is not limited to) producing the necessary HBOMs and SBOMs and documenting due diligence efforts. These hour and cost estimates are subject to variations among responsible entities due to application type. Declarations of Conformity will need to be submitted annually at minimum, while Specific Authorizations will need to be updated on an as-needed basis.

The estimated annual federal salary cost to the U.S. Government is \$1,130,000 [500 Declaration of Conformity/Specific Authorization notifications per year \* two staff at a GS-13 salary ( $\$113/\text{hour} * 2 = \$226/\text{hour}$ ) \* average of 10 hours each to review each notification]. The \$113 per staff member per hour cost estimate for this information collection is consistent with the GS-scale salary data for a GS-13 Step 1 (<https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2024/DCB.pdf>) multiplied by a factor of 2 to include the cost of benefits and overhead.

The total estimated annual cost to the U.S. Government is \$1,437,982.00. The calculation is as follows: Federal Employee Salaries (2 full-time employees) [\$1,130,000.00] + Federal Government Overhead @20% [\$226,000.00] + Legal Support (GS-15 Step 1 salary (multiplied by 2 to include the cost of benefits and overhead) @ 25%) [\$81,982.00] = \$1,437,982.00.

BIS requests comments on the information collection and recordkeeping requirements associated with this proposed rule. These comments will help BIS:

i. Evaluate whether the information collection is necessary for the proper performance of our agency's functions, including whether the information will have practical utility;

ii. Evaluate the accuracy of our estimate of the burden of the information collection, including the validity of the methodology and assumptions used;

iii. Enhance the quality, utility, and clarity of the information to be collected; and

iv. Minimize the burden of the information collection on those who are to respond (such as through the use of

appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses).

#### 8. Regulatory Flexibility Act

In compliance with Section 603 of the Regulatory Flexibility Act (RFA), 5 U.S.C. 601–612, the Department has prepared an initial regulatory flexibility analysis (IRFA) for this proposed rule. The IRFA describes the economic impacts the proposed action may have on small entities. The Department seeks comments on all aspects of the IRFA.

1. *A description of the reasons why action by the agency is being considered.* Connected Vehicles contain a growing number of connected components. While these components provide greater safety and convenience through features like Wi-Fi, Bluetooth, cellular telecommunication, and satellite connectivity, the incorporation of progressively complex hardware and software systems enabling vehicle connectivity has also increased the attack surfaces through which malign actors may exploit vulnerabilities to gain access to a vehicle. ICTS integral to Connected Vehicles present an undue or unacceptable risk to U.S. national security when those systems are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Furthermore, the PRC and Russia are able to leverage legal and regulatory regimes to compel private companies subject to their jurisdiction, including carmakers and vehicle suppliers, to cooperate with state security and intelligence services. Cooperation can include providing data, logical access, encryption keys, and other vital technical information, as well as by installing backdoors or bugs on equipment or in software updates, ultimately making vehicle equipment exploitable by foreign adversaries. Such privileged access potentially enables the PRC and Russia to exfiltrate sensitive data collected by Connected Vehicles through their components and allow remote manipulation for vehicles driven by U.S. persons.

2. *A succinct statement of the objectives of, and legal basis for, the proposed rule.* The Department is proposing this rule pursuant to authority under the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701, *et seq.*), the National Emergencies Act (NEA) (50 U.S.C. 1601, *et seq.*), and Section 301 of Title 3, United States Code, and in accordance with E.O. 13873, “Securing

the Information and Communications Technology and Services Supply Chain,” 84 FR 22689 (May 17, 2019), which delegated to the Secretary of Commerce (Secretary) certain authorities provided to the President by IEEPA, the NEA, and Section 301 of Title 3 of the United States Code. In accordance with the National Emergencies Act, the President has declared each year since E.O. 13873 was published that the national emergency declared in E.O. 13873 regarding the ICTS supply chain continues to remain in effect.

To address identified risks to national security from ICTS transactions, E.O. 13873 directs the Secretary (in consultation with other agency heads identified in E.O. 13873) to review any ICTS transaction, defined as any 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, where the transaction involves any property in which a foreign country or national has any interest. When the Secretary, in consultation with the appropriate agency heads, finds that an ICTS transaction or class of ICTS transactions pose undue risks (including of sabotage, subversion, or catastrophic effects on the security and resiliency of U.S. critical infrastructure), or unacceptable risks to national security or the security and safety of U.S. persons, the Secretary may identify the ICTS transaction as prohibited by Section 1 of E.O. 13873 or impose mitigation measures on the ICTS transaction or class of ICTS transactions reviewed. E.O. 13873 additionally provides that the Secretary issue rules establishing criteria by which particular technologies or market participants may be categorically included in or categorically excluded from prohibitions established pursuant to the E.O.

3. *A description of and, where feasible, an estimate of the number of small entities to which the proposed rule will apply.* BIS anticipates that the entities primarily responsible for compliance with this regulation will be connected vehicle manufacturers and VCS hardware importers. BIS assesses, based on publicly available information, that the U.S. connected vehicle market is dominated by a small set of manufacturers, few of which would be considered “small entities” under the Small Business Administration’s definitions. The Small Business Administration small business size standard for NAICS 336110: Automobile and Light Duty Motor Vehicle Manufacturing and NAICS 336120:

Heavy Duty Truck Manufacturing is 1,500 employees or fewer. However, BIS has limited data on how many of these suppliers engage in covered software and VCS hardware transactions, and therefore cannot estimate how many of these suppliers qualify as small entities. BIS specifically seeks comments on the number of suppliers engaged in covered software and VCS Hardware transactions in the United States, as well as the percentage of those entities that might or could qualify as small entities.

4. *A description of the projected reporting, recordkeeping, and other compliance requirements of the proposed rule, including an estimate of the classes of small entities that will be subject to the requirement and the type of professional skills necessary for preparation of the report or record.* As stated above, connected vehicle manufacturers and VCS hardware importers will bear the majority of the proposed rule’s compliance costs. BIS estimates that the recordkeeping and compliance burden placed on responsible small entities would involve operations managers, engineers, and lawyers. On an annual basis, these entities will need to, at minimum and if applicable, submit a Declaration of Conformity certifying that their import of VCS hardware and/or import or manufacture of completed connected vehicles does not involve hardware or software subject to the prohibitions in this proposed rule. The Declaration of Conformity would also include technical information regarding the hardware or software in question and a Bill of Materials for applicable software, hardware, or both.

BIS proposes to require connected vehicle manufacturers and VCS hardware importers to maintain complete records related to any transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required by this rule, for a period of ten years, consistent with IEEPA’s statute of limitations. These records would be expected to assist BIS’s enforcement efforts for the prohibitions in the proposed rule. The required records would include those related to any transaction that is subject to a general authorization (including records of any entities producing fewer than 1,000 connected vehicle or VCS hardware units in a calendar year), any transaction that is subject to a specific authorization, and any transaction involving covered software or VCS Hardware for which the connected vehicle manufacturer or VCS hardware importer has not yet sought an



authorization. BIS expects such records to include all information submitted in applications, as well as business records related to the execution of any ICTS transaction subject to the rule, such as contracts, import records, bills of sale, and all other files BIS may deem pertinent in assessing compliance with this proposed rule.

Because small entities could avail themselves of a general authorization, the maintenance of records in support of such authorization would be the only compliance requirement. These records would serve as the small entities' self-certification, which does not need to be submitted to BIS. A general authorization would allow the VCS hardware importer and/or connected vehicle manufacturer to engage in the otherwise prohibited transaction, without the need to notify or seek approval from BIS. General Authorizations would be available only in a narrow set of circumstances in which the conditions of the otherwise prohibited transaction appropriately mitigate the level of risk associated with the particular transaction. Such conditions would include, for example, when VCS hardware is imported from the PRC or Russia solely for testing purposes, or where the completed connected vehicle that incorporates VCS hardware or covered software from the PRC or Russia will not be driven on public roads for more than 30 calendar days per year. Those availing themselves of a general authorization would be required to continuously monitor their use of the VCS hardware or completed connected vehicles covered by the general authorization to ensure the authorization still applies. If a change would render the transaction ineligible for a general authorization, such as a change in the vehicle's use, the VCS hardware importer or connected vehicle manufacturer would be required to apply for a specific authorization and to cease engaging in such transaction unless and until a specific authorization is granted. For example, if a completed connected vehicle that incorporates covered software or VCS Hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia is no longer engaged in display, research, or testing, the VCS hardware importer or the connected vehicle manufacturer would be required to seek a specific authorization. Similarly, if the VCS Hardware Importer or connected vehicle manufacturer exceeds total model year production of 1,000 units, or

if a completed connected vehicle that incorporates covered software or VCS hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia is to be used on public roadways for 30 or more days in any calendar year, the VCS hardware importer or connected vehicle manufacturer would be required to seek a specific authorization from BIS.

5. *An identification, to the extent practicable, of all relevant Federal rules that may duplicate, overlap, or conflict with the proposed rule.* This rulemaking does not duplicate or conflict with any Federal rules.

6. *A description of any significant alternatives to the proposed rule that accomplish the stated objectives of Executive Order 13984 and Executive Order 14110 and applicable statutes and that would minimize any significant economic impact of the proposed rule on small entities.* The Department has proposed what it believes to be "the least restrictive means necessary [by] tailor[ing] the prohibition to address the undue or unacceptable risk" (see 15 CFR part 791.109(c)) and believes that the proposed rule will materially address significant risks for the United States or U.S. persons while balancing the overall compliance costs of the rule and minimizing the impact on small entities. Below is a description of alternatives considered by the Department; the Department invites comment on these alternatives.

*No-action alternative:* While the alternative of taking no action would be less costly for connected vehicle manufacturers and VCS hardware importers, the no-action alternative is not preferred because the risks presented by foreign adversary involvement in the ICTS of the U.S. connected vehicle market could lead to catastrophic negative events for U.S. national security, including the security of U.S. critical infrastructure, and U.S. persons.

*More stringent alternatives:* The Department considered several more stringent regulatory approaches, including regulating additional connected vehicle component systems not included in this proposed rule. For example, the Department considered the risks posed by various connected vehicle component systems, including ADS, telematics, battery management systems (BMS), automated driver assistance systems (ADAS), vehicle operating systems (OS), and satellite or cellular telecommunication systems. The Department currently believes the

best approach to address the risks posed by connected vehicles and connected vehicle components from foreign adversary nations is to focus the scope of the NPRM on PRC- and Russian-supplied VCS hardware (which encompasses both telematics and satellite or cellular telecommunication systems) and covered software. Other systems under consideration, such as ADAS, seem to have a low risk of data exfiltration or, in the case of vehicle OS, would involve regulation that is expected to be extremely burdensome on industry.

*Preferred alternative:* The proposed rule is the preferred alternative. BIS assesses that the regulatory approach outlined in this proposed rule would have the highest net benefit for connected vehicle manufacturers, VCS hardware importers, and consumers. BIS currently believes the provisions in the proposed rule are also to be, for the reasons articulated above and in the NPRM's preamble, "the least restrictive means necessary. . .to address the undue or unacceptable risk" presented by covered software and VCS hardware in connected vehicles.

#### List of Subjects in 15 CFR Part 791

Business and industry, Communications, Computer technology, Critical infrastructure, Executive orders, Foreign persons, Investigations, National security, Penalties, Technology, Telecommunications.

Elizabeth L.D. Cannon,

*Executive Director, Office of Information and Communications Technology and Services, Bureau of Industry and Security, United States Department of Commerce.*

For the reasons set out in the preamble, 15 CFR part 791, is proposed to be amended as follows:

#### PART 791—SECURING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SUPPLY CHAIN

■ 1. The authority citation for part 791 continues to read as follows:

Authority: 50 U.S.C. 1701*et seq.*; 50 U.S.C. 1601*et seq.*; E.O. 13873, 84 FR 22689; E.O. 14034, 86 FR 31423.

■ 2. Amend part 791 by adding subpart D, consisting of § 791.300 through § 791.319, to read as follows:

#### Subpart D—ICTS Supply Chain: Connected Vehicles

Sec.

791.300 Purpose and scope.

791.301 Definitions.

791.302 Prohibited VCS hardware transactions.

- 791.303 Prohibited covered software transactions.
- 791.304 Related prohibited transactions.
- 791.305 Declaration of Conformity.
- 791.306 General authorizations.
- 791.307 Specific authorizations.
- 791.308 Exemptions.
- 791.309 Appeals.
- 791.310 Advisory opinions.
- 791.311 "Is-Informed" notices.
- 791.312 Recordkeeping.
- 791.313 Reports to be furnished on demand.
- 791.314 Penalties.
- 791.315 Pre-penalty notice; settlement.
- 791.316 Penalty imposition.
- 791.317 Administrative collection; referral to United States Department of Justice.
- 791.318 Finding of violation.
- 791.319 Severability.

#### Subpart D—ICTS Supply Chain: Connected Vehicles

##### § 791.300 Purpose and scope.

The inclusion in Connected Vehicles of certain ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of certain foreign adversaries poses undue or unacceptable risks to U.S. national security. To address these undue or unacceptable risks, it is the purpose of this subpart to:

(a) Prohibit ICTS transactions that involve certain software and hardware that, are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China (PRC) or the Russian Federation (Russia), as defined in § 791.4 and that enable connected vehicle Automated Driving Systems or Vehicle Connectivity Systems, as defined in this subpart;

(b) Implement compliance mechanisms such as Declarations of Conformity to ensure that no Prohibited Transactions, as defined in this subpart, have occurred;

(c) Provide general authorizations and a mechanism for specific authorizations for certain transactions that are otherwise prohibited by this subpart, but where any undue or unacceptable risks to national security can be reasonably mitigated, based on defined criteria and conditions; and

(d) Incentivize connected vehicle manufacturers, VCS hardware importers, and related suppliers to adopt measures to help secure the U.S. ICTS supply chain for connected vehicles.

##### § 791.301 Definitions.

The following definitions apply only to this subpart, 15 CFR part 791 subpart

D. For additional definitions applicable to all of part 791, *see* 15 CFR 791.2. If a term is defined differently in this subpart than in 15 CFR 791.2, the definition listed in this section will apply to this subpart.

*Automated Driving System* means hardware and software that, collectively, are capable of performing the entire dynamic driving task for a completed connected vehicle on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD).

*Completed connected vehicle* means a connected vehicle that requires no further manufacturing operations to perform its intended function. For the purposes of this subpart, the integration of an Automated Driving System into a connected vehicle constitutes a manufacturing operation for a completed connected vehicle.

*Connected vehicle* means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways, that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device. Vehicles operated only on a rail line are not included in this definition.

*Connected vehicle manufacturer* means a U.S. person

(1) Manufacturing or assembling completed connected vehicles in the United States; and/or

(2) Importing completed connected vehicles for sale in the United States.

*Covered software* means the software-based components, in which there is a foreign interest, executed by the primary processing unit of the respective systems that are part of an item that supports the function of Vehicle Connectivity Systems or Automated Driving Systems at the vehicle level. Covered software does not include firmware, which is characterized as software specifically programmed for a hardware device with a primary purpose of controlling, configuring, and communicating with that hardware device. Covered software also does not include open-source software that can be freely used, modified, and distributed by anyone, with both access to the source code and the ability to contribute to the software's development and improvement unless that open-source software has been modified for proprietary purposes and not redistributed or shared.

*FCC ID Number* means the unique alphanumeric code identifying a product subject to certification by the Federal Communications Commission composed of a:

- (1) Grantee code; and
- (2) Product code.

*Foreign interest*, for purposes of this subpart, means any interest in property of any nature whatsoever, whether direct or indirect, by a non-U.S. person.

*Hardware Bill of Materials (HBOM)* means a comprehensive list of parts, assemblies, documents, drawings, and components required to create a physical product, including information identifying the manufacturer, related firmware, technical information, and descriptive information.

*Import* means, in the context of this subpart, with respect to any article, the entry of such article into the United States Customs Territory. It does not include admission of an article from outside the United States into a foreign-trade zone for storage pending further assembly in the foreign-trade zone or shipment to a foreign country.

*Item* means a component or set of components with a specific function at the vehicle level. A system may also be considered an item if it implements a function.

*Knowingly* means having knowledge of a circumstance (the term may be a variant, such as "know," "reason to know," or "reason to believe"), to include not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts.

*Model year* means the year used to designate a discrete vehicle model, irrespective of the calendar year in which the vehicle was actually produced, provided that the production period does not exceed 24 months.

*Prohibited transactions* mean, collectively, the transactions described in 791.302 (Prohibited VCS Hardware Transactions), 791.303 (Prohibited Covered Software Transactions), or 791.304 (Related Prohibited Transactions) of this subpart.

*Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary* means:

(1) Any person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly



supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary;

(2) Any person, wherever located, who is a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, and is not a United States citizen or permanent resident of the United States;

(3) Any corporation, partnership, association, or other organization with a principal place of business in, headquartered in, incorporated in, or otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary; or

(4) Any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs (a) through (c) possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity.

*Sale* means, in the context of this subpart, distributing for purchase, lease, or other commercial operations a new completed connected vehicle for a price, to include the transfer of completed connected vehicles from a connected vehicle manufacturer to a dealer or distributor, as those terms are defined in 49 U.S.C. 30102. This definition also applies to the related terms such as *Sell* or *Selling*.

*Software Bill of Materials (SBOM)* means a formal and dynamic, machine-readable inventory detailing the software supply chain relationships between software components and subcomponents, including software dependencies, hierarchical relationships, and baseline software attributes, including author's name, timestamp, supplier name, component name, version string, component hash package URL, unique identifier, and dependency relationships to other software components.

*Vehicle Connectivity System (VCS)* means a hardware or software item for a completed connected vehicle that has the function of enabling the transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz.

*VCS hardware* means the following software-enabled or programmable components and subcomponents that

support the function of Vehicle Connectivity Systems or are part of an item that supports the function of Vehicle Connectivity Systems: microcontroller, microcomputers or modules, systems on a chip, networking or telematics units, cellular modem/modules, Wi-Fi microcontrollers or modules, Bluetooth microcontrollers or modules, satellite navigation systems, satellite communication systems, other wireless communication microcontrollers or modules, and external antennas. VCS hardware does not include component parts that do not contribute to the communication function of VCS hardware (e.g., brackets, fasteners, plastics, and passive electronics).

*VCS hardware importer* means a U.S. person importing VCS hardware for further manufacturing, integration, resale, or distribution. A connected vehicle manufacturer may be a VCS hardware importer if VCS hardware has already been installed in a connected vehicle when imported by the connected vehicle manufacturer.

*United States* means the United States of America, the States of the United States, the District of Columbia, and any commonwealth, territory, dependency, or possession of the United States, or any subdivision thereof, and the territorial sea of the United States.

#### **§ 791.302 Prohibited VCS hardware transactions.**

(a) VCS hardware importers are prohibited from knowingly importing VCS hardware that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

(b) In the context of this subpart, VCS hardware will not be considered to be designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, solely based on the country of citizenship of natural persons who are employed, contracted, or otherwise similarly engaged to participate in the design, development, manufacture, or supply of the VCS hardware.

#### **§ 791.303 Prohibited covered software transactions.**

(a) Connected vehicle manufacturers are prohibited from knowingly importing into the United States completed connected vehicles that incorporate covered software, designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

(b) Connected vehicle manufacturers are prohibited from knowingly selling in the United States completed connected vehicles that incorporate covered software, designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

(c) In the context of this subpart, covered software will not be considered to be designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, solely based on the country of citizenship of natural persons who are employed, contracted, or otherwise similarly engaged to participate in the design, development, manufacture, or supply of the Covered Software.

#### **§ 791.304 Related prohibited transactions.**

Connected vehicle manufacturers who are persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, are prohibited from knowingly selling in the United States completed connected vehicles that incorporate VCS hardware or covered software.

#### **§ 791.305 Declaration of Conformity.**

(a) *Requirements*—(1) *Import of VCS hardware*: A VCS hardware importer may not import VCS Hardware as part of a transaction that is not otherwise prohibited by this subpart without first submitting to the Bureau of Industry and Security (BIS) a Declaration of Conformity, unless otherwise specified by this subpart. The Declaration of Conformity shall include:

- (i) The name and address of VCS hardware importer;
- (ii) A certification that the declarant has not knowingly engaged in a prohibited VCS hardware transaction;
- (iii) The FCC ID Number associated with the VCS hardware and, if applicable, of the subcomponents contained therein;
- (iv) A list of third-party external endpoints to which the VCS hardware connects, including the country where each endpoint is located and/or the identity and location of the service provider;
- (v) If known, the make, model, and trim of the completed connected vehicles for which the VCS hardware is intended;
- (vi) A HBOM for the VCS hardware that is the subject of the Declaration of Conformity;

(vii) Documentation of the VCS hardware importer's due diligence efforts, to include independent or hired third-party research, to ensure the VCS

hardware listed in the HBOM is not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(viii) If applicable, an indication of whether the submission is an update to a prior Declaration of Conformity and the date of the last submission;

(ix) Identifying information for an individual point of contact (including name, email address, and phone number); and,

(x) Any additional material information the VCS hardware importer would like to submit.

(2) *Import of completed connected vehicles:* A connected vehicle manufacturer may not import completed connected vehicles containing covered software as part of a transaction that is not otherwise prohibited by this subpart without first submitting to BIS a Declaration of Conformity, unless otherwise specified by this subpart. The Declaration of Conformity shall include:

(i) The name and address of the connected vehicle manufacturer;

(ii) A certification that the declarant has not knowingly engaged in a prohibited covered software transaction;

(iii) The make, model, trim, and Vehicle Identification Number (VIN) series applicable to the completed connected vehicles;

(iv) A SBOM for the covered software that is the subject of the Declaration of Conformity. At a minimum, the SBOM must include author's name, timestamp, supplier name, component name, version string, component hash, package URL, unique identifier, and dependency relationships to other software components.

(v) Documentation of the connected vehicle manufacturer's due diligence efforts, to include independent or hired third-party research, to ensure that the covered software listed in the SBOM is not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(vi) If applicable, an indication of whether the submission is an update to a prior Declaration of Conformity and the date of the last submission;

(vii) Identifying information for an individual point of contact (including name, email address, and phone number); and

(viii) Any additional material information the connected vehicle manufacturer would like to submit.

(3) *Sale of completed connected vehicles manufactured in the United States:* Connected vehicle

manufacturers that manufacture or assemble completed connected vehicles in the United States that incorporate covered software as part of a transaction that is not otherwise prohibited by this subpart, may not sell completed connected vehicles in the United States without first submitting to BIS a Declaration of Conformity, unless otherwise specified by this subpart. If there is no Foreign Interest in the covered software that is incorporated in completed connected vehicles manufactured or assembled in the United States, the connected vehicle manufacturer need not submit a Declaration of Conformity. If submitting a Declaration of Conformity, it shall include:

(i) The name and address of the connected vehicle manufacturer;

(ii) A certification that there is a foreign interest in the covered software that is incorporated in the completed connected vehicles that will be sold in the United States;

(iii) A certification that the declarant has not knowingly engaged in a prohibited covered software Transaction;

(iv) The make, model, trim, and VIN series applicable to the completed connected vehicles;

(v) A SBOM for the covered software that is the subject of the Declaration of Conformity. At a minimum, the SBOM must include author's name, timestamp, supplier name, component name, version string, component hash, package URL, unique identifier, and dependency relationships to other software components.

(vi) Documentation of the connected vehicle manufacturer's due diligence efforts, to include independent or hired third-party research, to ensure the covered software listed in the SBOM is not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(vii) If applicable, an indication of whether the submission is an update to a prior Declaration of Conformity and the date of the last submission;

(viii) Identifying information for an individual point of contact (including name, email address, and phone number); and

(ix) Any additional material information the connected vehicle manufacturer would like to submit.

(b) *Procedures to submit Declarations of Conformity.* Connected vehicle manufacturers and VCS Hardware Importers shall submit Declarations of Conformity annually as specified in this section and any time there is a material

change that makes a prior Declaration of Conformity or associated HBOM or SBOM no longer accurate.

(1) Connected Vehicles Manufacturers seeking to import or manufacture for Sale in the United States a completed connected vehicle containing covered software shall submit a Declaration of Conformity 60 days prior to the first import or first sale of each model year of completed connected vehicles, grouped by make, model, and trim.

(2) VCS hardware importers seeking to import any VCS hardware shall submit a Declaration of Conformity 60 days prior to the first import of VCS hardware for each model year for units associated with a vehicle model year, or calendar year for units not associated with a vehicle model year. VCS hardware importers may submit a single Declaration of Conformity detailing all VCS Hardware models that will be imported in the Model Year or calendar year.

(3) Entities that are both connected vehicle manufacturers and VCS hardware importers may, but are not required to, submit a single compiled Declaration of Conformity detailing all required information specified in 791.305 of this subpart. Any compiled Declaration of Conformity shall be submitted 60 days prior to the first import or first sale of the model year of completed connected vehicles or 60 days prior to the first import of VCS hardware, whichever occurs first.

(4) Declarants must notify BIS of any material change in the contents of a previously submitted Declaration of Conformity by submitting a revised Declaration of Conformity within 30 days following any such changes.

(c) Declarations of Conformity must be delivered to BIS using an official electronic reporting option as specified by BIS on its website (<https://www.bis.gov>).

(d) *Connected vehicle introduced by means of a fraudulent or false declaration.* Any person who engages in a prohibited VCS hardware transaction or a prohibited covered software transaction and submits a false or fraudulent Declaration of Conformity made without reasonable cause to believe the truth of the declaration, may incur penalties as defined in § 791.314.

#### § 791.306 General authorizations.

(a) VCS hardware importers and connected vehicle manufacturers may qualify for a general authorization if they meet the stated requirements or conditions to engage in otherwise prohibited transactions. Persons availing themselves of any general authorization are required to maintain

records documenting each otherwise prohibited transaction for a period of 10 years as specified in § 791.312.

(b) *General course of procedure.* VCS hardware importers and connected vehicle manufacturers may self-certify, without need to notify BIS, that they meet the requirements for one or more of the following general authorizations:

(1) The connected vehicle manufacturer or VCS hardware importer and entities under common control, including parents, engaging in an otherwise prohibited transaction produces a total model year production of completed connected vehicles containing covered software or total model year production of VCS hardware is less than 1,000 units;

(2) The completed connected vehicle that incorporates covered software or VCS hardware will be used on public roadways on fewer than 30 calendar days in any calendar year;

(3) The completed connected vehicle that incorporates covered software or the VCS hardware will be used solely for the purpose of display, testing, or research, and will not be used on public roadways; or

(4) The completed connected vehicle that incorporates covered software or the VCS hardware is imported solely for purposes of repair, alteration, or competition off public roads and will be reexported within one year from the time of import;

(c) *Change in use.* In the event of any change in the use of a completed connected vehicle or VCS hardware associated with a general authorization, a VCS hardware importer or connected vehicle manufacturer availing itself of a general authorization must determine if it still qualifies for the general authorization or if it must apply for a specific authorization.

(d) *Inspection.* VCS hardware importers and connected vehicle manufacturers availing themselves of a general authorization are subject to audit and inspection by BIS.

(e) *Restrictions.* VCS Hardware importers and connected vehicle manufacturers shall not avail themselves of any general authorization if any one or more of the following apply:

(1) BIS has notified the VCS hardware importer or connected vehicle manufacturer that it is not eligible for a general authorization.

(2) The VCS Hardware Importer or connected vehicle manufacturer is a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

#### § 791.307 Specific authorizations.

(a) BIS may provide Specific Authorizations permitting a VCS hardware importer or connected vehicle manufacturer to engage in otherwise prohibited transactions. Persons receiving a specific authorization are required to maintain records for a period of 10 years as required in § 791.312 and submit reports and statements in accordance with the instructions specified in each specific authorization.

(b) *General course of procedure.* Prohibited transactions subject to this subpart, and that are not otherwise permitted under an exemption or a general authorization, may be permitted under a specific authorization. It is the policy of BIS not to grant applications for specific authorizations for transactions that are permitted by a general authorization.

(c) *Applications for specific authorizations.* Applications for specific authorizations shall include, at a minimum, a description of the nature of the otherwise prohibited transaction(s), including the following:

(1) The identity of the parties engaged in the transaction, including relevant corporate identifiers and information sufficient to identify the ultimate beneficial ownership of the transacting parties;

(2) An overview of the VCS hardware or covered software that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(3) If known, the make, model, and trim of the completed connected vehicle in which the VCS hardware or covered software will be integrated;

(4) The intended function of the VCS hardware or covered software;

(5) Documentation to support the information contained in the application, including ISO/SAE 21434 Threat Analysis and Risk Assessments, to include an assessment on the applicant's ability to limit PRC or Russian government access to, or influence over the design, development, manufacture or supply of the VCS hardware or covered software; security standards used by the applicant with respect to the VCS hardware or covered software; other actions and proposals such as technical controls (*i.e.*, software validation) or operational controls (*i.e.*, physical and logical access monitoring procedures), the applicant intends to take to mitigate undue or unacceptable risk; and

(6) Any other information that BIS may request after receipt of the initial application for a Specific Authorization.

(d) *Application submission procedures.* A VCS hardware importer or connected vehicle manufacturer who seeks to engage in an otherwise prohibited transaction must submit an application for specific authorization in writing prior to engaging in the transaction and await a decision from BIS prior to engaging in the transaction. This application must be delivered to BIS using an official electronic reporting option as specified by BIS on its website (<https://www.bis.gov>).

(e) *Additional conditions.* Only one application for a specific authorization should be submitted to BIS for each otherwise prohibited transaction; multiple parties submitting an application for a specific authorization for the same transaction may result in processing delays.

(f) *Information to be supplied.* An applicant may be required to furnish additional information as BIS deems necessary to assist in making a decision. The applicant may present additional information concerning an application for a specific authorization at any time before BIS makes its decision with respect to the application.

(g) *Review and decisions.* Applications for specific authorization will be reviewed on a case-by-case basis and determine conditions to be applied to each specific authorization as may be needed to mitigate any risk that arises as a result of the otherwise prohibited transaction. Such review may include an evaluation of the risks and potential mitigation measures proposed by the applicant for the particular transaction, including, but not limited to, risks of data exfiltration from, and remote manipulation or operation of, the connected vehicle; the extent and nature of foreign adversary involvement in the design, development, manufacture, or supply of the VCS hardware or covered software; the applicant's ability to limit PRC or Russian government access to, or influence over the design, development, manufacture or supply of the VCS hardware or covered software; security standards used by the applicant and if such standards can be validated by BIS or a third-party; other actions and proposals the applicant intends to take to mitigate undue or unacceptable risk. BIS will advise each applicant of the decision respecting the filed application.

(h) *Processing period.* BIS shall respond to any application for a specific authorization with a status update and a request for additional information or documents, if any, within 90 days after receipt of the application.

(i) *Scope.* (1) Unless otherwise specified in the authorization, a specific

authorization permits the transaction only:

- (i) Between the parties identified in the specific authorization;
- (ii) With respect to the otherwise prohibited transaction(s) described in the authorization; and
- (iii) If the conditions specified in the specific authorization are satisfied. The applicant must inform any other parties identified in the specific authorization of the authorization's scope and specific conditions.

(2) Any specific authorization obtained based on a false or misleading representation in the application or in any document submitted in connection with the application under this section shall be deemed void as of the date of issuance, and the applicant may incur penalties as specified in § 791.314.

(3) As a condition for the issuance of any specific authorization, the applicant may be required to file reports with respect to the otherwise prohibited transactions authorized by the specific authorization in such form and at such times and places as may be prescribed in the specific authorization or otherwise communicated to the applicant by BIS. Reports should be sent in accordance with the instructions provided in the applicable specific authorization.

(j) *Effect of denial.* BIS's denial of a specific authorization may be appealed as described in § 791.309 and does not preclude parties from filing an application for a specific authorization for a separate otherwise prohibited transaction. The applicant may at any time request, by written correspondence, reconsideration of the denial of an application based on new material facts or changed circumstances.

(k) *Effect of specific authorization.* (1) No specific authorization issued under this subpart, or otherwise issued by BIS, permits or validates any prohibited transaction effected prior to the issuance of such specific authorization unless specifically provided for in the specific authorization.

(2) No regulation, ruling, instruction, or authorization permits any prohibited transaction under this subpart unless the regulation, ruling, instruction or Authorization is issued by BIS and specifically refers to this subpart. No regulation, ruling, instruction, or authorization referring to this subpart shall be deemed to permit any prohibited transaction prohibited by any provision of this subpart unless the regulation, ruling, instruction, or authorization specifically refers to such provision. Any specific authorization permitting any otherwise prohibited transaction has the effect of removing

those prohibitions from the transaction, but only to the extent specifically stated by the terms of the specific authorization. Unless the specific authorization otherwise specifies, such an authorization does not create any right, duty, obligation, claim, or interest in, or with respect to, any property that would not otherwise exist under ordinary principles of law.

(3) Nothing contained in this subpart shall be construed to supersede the requirements established under any other provision of law or to relieve a person from any requirement to obtain an authorization from another department or agency of the U.S. Government in compliance with applicable laws and regulations subject to the jurisdiction of that department or agency.

(l) *Amendment, modification, or rescission.* Except as otherwise provided by law, any Specific Authorization or instructions issued thereunder may be amended, modified, or rescinded by BIS at any time.

#### § 791.308 Exemptions.

(a) VCS hardware importers may engage in prohibited transactions described in § 791.302 without an authorization as required under §§ 791.306 and 791.307, and are exempt from submitting Declarations of Conformity with respect to all other transactions, as described in § 791.305 provided that:

(1) For VCS Hardware units not associated with a vehicle model year, the import of the VCS hardware occurs prior to January 1, 2029; or

(2) The VCS hardware is associated with a vehicle model year prior to 2030 or the VCS hardware is imported as part of a connected vehicle with a model year prior to 2030.

(b) Connected vehicle manufacturers may engage in prohibited transactions described in § 791.303 without authorization as required under §§ 791.306 or 791.307 and are exempt from submitting Declarations of Conformity with respect to all other transactions, as described in § 791.305, provided that the completed connected vehicle that incorporates covered software described in § 791.303(a)(1) was manufactured prior to Model Year 2027.

(c) Connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia may engage in prohibited transactions described in section 791.304 without Authorization as required under §§ 791.306 or 791.307, and are exempt from submitting Declarations of Conformity to all other

transactions, provided that the completed connected vehicle that incorporates VCS hardware and/or covered software was manufactured prior to Model Year 2027.

#### § 791.309 Appeals.

(a) *Scope.* Any person directly and adversely affected by any of the listed administrative actions taken by BIS pursuant to this subpart may appeal to the Under Secretary for reconsideration of that administrative action. Only the following types of administrative actions are subject to the appeals procedures described in this subpart:

- (1) Denial of an application for specific authorization;
- (2) Suspension or revocation of an issued specific authorization; or
- (3) Determination of ineligibility for a general authorization.

(b) *Designated appeals reviewer and coordinator.* The Under Secretary may delegate to the Deputy Under Secretary of Commerce for Industry and Security or to another BIS official the authority to review and decide the appeal, and to exercise any other function of the Under Secretary under this section. In addition, the Under Secretary may designate any employee of BIS to be an appeals coordinator to assist in the review and processing of an appeal under this subpart.

(c) *Appeals procedures.* An appeal under this subpart must be submitted to the Under Secretary by email or at the following address: Bureau of Industry and Security, U.S. Department of Commerce, Room 3898, 14th Street and Pennsylvania Avenue NW, Washington, DC 20230 not later than 45 days after the date appearing on the written notice of administrative action. The appeal must include a full written statement in support of the appellant's position. The appeal must include a precise statement of the reasons that the appellant believes that the administrative action has a direct and adverse effect and should be reversed or modified. The Under Secretary or the designated official may request additional information that would be helpful in resolving the appeal and may accept additional submissions. The Under Secretary or the designated official will not ordinarily accept any submission filed sua sponte more than 30 days after the filing of the appeal.

(d) *Request for informal hearing.* In addition to the written statement submitted in support of an appeal, an appellant may request, in writing, at the time an appeal is filed, an opportunity for an informal hearing. A hearing is not required, and the Under Secretary or the designated official may grant or deny a

request for an informal hearing at the Under Secretary or the designated official's sole discretion. Any hearings will be held in the District of Columbia unless the Under Secretary or the designated official determines, based upon good cause shown, that another location would be preferable.

(e) *Informal hearing procedures.* If a hearing request is granted, the Under Secretary or the designated official may provide an opportunity for the appellant to make an oral presentation at an informal hearing based on the materials previously submitted by the appellant or made available by the Department. The Under Secretary or the designated official may require that any facts in controversy be covered by an affidavit or testimony given under oath or affirmation. The rules of evidence prevailing in courts of law do not apply, and all evidentiary material deemed by the Under Secretary or the designated official to be relevant and material to the proceeding, and not unduly repetitious, will be received and considered. The Under Secretary or the designated official has the authority to limit the number of people attending the hearing, to impose any time or other limitations deemed reasonable, and to determine all procedural questions. A transcript of an informal hearing shall not be made, unless the Under Secretary or the designated official determines that the national interest or other good cause warrants it, or the appellant requests a transcript. If the appellant requests, and the Under Secretary or the designated official approves the taking of, a transcript, the appellant will be responsible for paying all expenses related to production of the transcript. Any person designated by the Under Secretary to conduct an informal hearing shall submit a written report containing a summary of the hearing and recommended action to the Under Secretary.

(f) *Decisions.* In addition to the documents specifically submitted in connection with the appeal, the Under Secretary or the designated official may consider any recommendations, reports, or other relevant documents available to BIS in determining the appeal, but shall not be bound by any such information, nor prevented from considering any other relevant information, or consulting with any other person or groups, in making a decision. The Under Secretary or the designated official may adopt any other procedures deemed necessary and reasonable for considering an appeal, including by providing the appellant with an interim or proposed decision and offering the appellant an opportunity to provide

comments. The Under Secretary or the designated official shall decide an appeal within a reasonable time after receipt of the appeal. The decision shall be issued to the appellant in writing and contain a statement of the reasons for the action and address any arguments contrary to the decision presented by the appellant. The decision of the Under Secretary or the designated official shall be final.

(g) *Effect of appeal.* Acceptance and consideration of an appeal shall not affect any administrative action, pending or in effect, unless the Under Secretary or the designated official, upon request by the appellant and with opportunity for a response, grants a stay.

#### **§ 791.310 Advisory opinions.**

(a) VCS hardware importers and connected vehicle manufacturers may request an advisory opinion from BIS as to whether a prospective transaction is subject to a prohibition in this subpart. The entire transaction that is the subject of the advisory opinion request must be an actual, as opposed to hypothetical, transaction and involve disclosed, as opposed to anonymous, parties to the transaction.

(b) Advisory opinion requests must be made in writing, and may be delivered to BIS by email, through the BIS website, or by any other means that BIS may prescribe.

(c) Persons submitting advisory opinion requests are encouraged to provide as much information as possible to assist BIS in making a determination, to include the following information:

(1) The name, title, and telephone and email address of the person to contact;

(2) The submitter's complete address comprised of street address, city, state, country, and postal code;

(3) All available information identifying the parties to the prospective transaction;

(4) Complete information regarding the VCS hardware and/or covered software and any descriptive literature, brochures, technical specifications, or papers that provide sufficient technical detail to enable BIS to verify whether the prospective transaction would constitute a prohibited transaction as defined in this subpart;

(5) For connected vehicle manufacturers: the make, model, and trim level, or other identifying information number of the completed connected vehicle;

(6) For VCS hardware Importers: the identification of the system; and, if known, the make, model, and trim of the group of completed connected vehicles for which the equipment is intended;

(7) An SBOM and/or an HBOM; and  
(8) Any other information that the submitter believes to be material to the prospective transaction.

(d) Each person that submits an advisory opinion request shall provide any additional information or documents that BIS may thereafter request in its review of the matter.

(e) Each advisory opinion can be relied upon by the requesting party or parties to the extent the disclosures made pursuant to this subpart were accurate and complete and to the extent the disclosures continue accurately and completely to reflect circumstances after the date of the issuance of the advisory opinion. An advisory opinion will not restrict enforcement actions by any agency other than BIS. It will not affect a requesting party's obligations to any other agency or under any statutory or regulatory provision other than those specifically discussed in the Advisory Opinion.

(f) BIS may publish on its website an advisory opinion that may be of broad interest to the public, with redactions where necessary to protect confidential business information.

#### **§ 791.311 "Is-Informed" notices.**

(a) BIS may inform VCS hardware importers or connected vehicle manufacturers either individually by specific notice or, for larger groups, through a separate notice published in the *Federal Register*, that a specific authorization is required because an activity could constitute a prohibited transaction.

(b) Specific notice that a specific authorization is required may be given only by, or at the direction of, the Under Secretary or a BIS official designated by the Under Secretary.

#### **§ 791.312 Recordkeeping.**

Except as otherwise provided, VCS hardware importers and connected vehicle manufacturers shall keep a full and accurate record of each transaction engaged in for which a Declaration of Conformity, general authorization, or specific authorization would be required under sections 791.305, 791.306, or 791.307, regardless of whether these transactions are effected pursuant to a general authorization, specific authorization, or otherwise, and such record shall be available for examination for at least 10 years after the date of such transactions.

#### **§ 791.313 Reports to be furnished on demand.**

(a) VCS hardware importers and connected vehicle manufacturers are required to furnish under oath, in the

form of reports or as otherwise specified by BIS, from time to time and at any time as may be required by BIS, complete information relative to any transaction involving the import of VCS hardware or the import or Sale of completed connected vehicles incorporating covered software, regardless of whether such transaction is effected pursuant to an authorization or otherwise, subject to the provisions of this subpart. BIS may require that such reports include the production of any books, contracts, letters, papers, or other hard copy or electronic documents relating to any transactions, in the custody or control of the persons required to make such reports. BIS may, through any person or agency, conduct investigations, hold hearings, administer oaths, examine witnesses, receive evidence, take depositions, and require by subpoena the attendance and testimony of witnesses and the production of any books, contracts, letters, papers, and other hard copy or electronic documents relating to any matter under investigation, regardless of whether any report has been required or filed in connection therewith.

(b) For purposes of paragraph (a) of this section, the term "document" includes any written, recorded, or graphic matter or other means of preserving thought or expression (including in electronic format), and all tangible things stored in any medium from which information can be processed, transcribed, or obtained directly or indirectly, including correspondence, memoranda, notes, messages, contemporaneous communications such as text and instant messages, letters, emails, spreadsheets, metadata, contracts, bulletins, diaries, chronological data, minutes, books, reports, examinations, charts, ledgers, books of account, invoices, air waybills, bills of lading, worksheets, receipts, printouts, papers, schedules, affidavits, presentations, transcripts, surveys, graphic representations of any kind, drawings, photographs, graphs, video or sound recordings, and motion pictures or other film.

(c) Persons providing documents to BIS pursuant to this section must submit documents electronically. Acceptable formats include Portable Document Format (PDF) and Microsoft Excel. Files with embedded, encrypted, or password protected content will not be accepted.

#### **§ 791.314 Penalties.**

(a) Section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) (IEEPA) is applicable to

violations of the provisions of any general authorization, Specific authorization, regulation, order, directive, instruction, or prohibition issued by or pursuant to the direction or authorization of the Secretary of Commerce (Secretary) pursuant to this subpart or otherwise under IEEPA.

(1) A civil penalty not to exceed the amount set forth in section 206 of IEEPA may be imposed on any person who violates, attempts to violate, conspires to violate, or causes a violation of any exemption, general authorization, specific authorization, regulation, order, directive, instruction, or prohibition issued under this subpart.

(2) A person who willfully commits, willfully attempts to commit, willfully conspires to commit, or aids or abets in the commission of a violation of any exemption, general authorization, specific authorization, regulation, order, directive, instruction, or prohibition issued under this subpart is subject to criminal penalties and may, upon conviction, be fined not more than \$1,000,000, or if a natural person, be imprisoned for not more than 20 years, or both.

(b) The civil penalties provided in IEEPA are subject to adjustment pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990 (Pub. L. 101-410, as amended, 28 U.S.C. 2461 note).

(c) The criminal penalties provided in IEEPA are subject to adjustment pursuant to 18 U.S.C. 3571.

(d) Pursuant to 18 U.S.C. 1001, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the U.S. Government, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact; or makes any materially false, fictitious, or fraudulent statement or representation; or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry shall be fined under title 18, United States Code, imprisoned, or both.

(e) Violations of this subpart may also be subject to other applicable laws.

#### **§ 791.315 Pre-penalty notice; settlement.**

(a) *When required.* If BIS has reason to believe that there has occurred a violation of any provision of this subpart or a violation of the provisions of any exemption, general authorization, specific authorization, regulation, order, directive, instruction, or prohibition issued by or pursuant to the direction or authorization of the Secretary pursuant to this subpart or otherwise under

IEEPA and determines that a civil monetary penalty is warranted, BIS will issue a pre-penalty notice informing the alleged violator of BIS's intent to impose a monetary penalty. A Pre-Penalty Notice shall be in writing and issued electronically to the alleged violator. The pre-penalty notice may be issued whether or not another agency has taken any action with respect to the matter.

(b) *Response—(1) Right to respond.* An alleged violator may respond to a Pre-Penalty Notice in writing to BIS.

(2) *Deadline for response.* A response to a Pre-Penalty Notice must be made within 30 days as set forth below. The failure to submit a response within 30 days shall be deemed to be a waiver of the right to respond.

(i) *Computation of time for response.* A response to a Pre-Penalty Notice must be electronically transmitted on or before the 30th day after the date of delivery by BIS.

(ii) *Extensions of time for response.* If a due date falls on a federal holiday or weekend, that due date is extended to include the following business day. Any other extensions of time will be granted, at the discretion of BIS, only upon specific request to BIS.

(3) *Form and method of response.* A response to a pre-penalty notice need not be in any particular form, but it must be typewritten and signed by the alleged violator or a representative thereof, contain information sufficient to indicate that it is in response to the pre-penalty notice, and include the BIS identification number listed on the pre-penalty notice. A digital signature is acceptable.

(4) *Information that should be included in response.* Any response should set forth in detail why the alleged violator either believes that a violation of the provisions of this subpart did not occur and/or why a civil monetary penalty is otherwise unwarranted under the circumstances. The response should include all documentary or other evidence available to the alleged violator that supports the arguments set forth in the response. BIS will consider all relevant materials submitted in the response.

(c) *Settlement.* Settlement discussions may be initiated by BIS, the alleged violator, or the alleged violator's authorized representative.

(d) *Representation.* A representative of the alleged violator may act on behalf of the alleged violator, but any oral communication with BIS prior to a written submission regarding the specific allegations contained in the pre-penalty notice must be preceded by a written letter of representation, unless the pre-penalty notice was served upon



the alleged violator in care of the representative.

**§ 791.316 Penalty imposition.**

(a) If, after considering any written response to the pre-penalty notice and any relevant facts, BIS determines that there was a violation by the alleged violator named in the pre-penalty notice and that a civil monetary penalty is appropriate, BIS may issue a penalty notice to the violator containing a determination of the violation and the imposition of the monetary penalty.

(b) The issuance of the penalty notice shall constitute final agency action. The violator may seek judicial review of that final agency action in federal district court.

**§ 791.317 Administrative collection; referral to United States Department of Justice.**

In the event that the violator does not pay the penalty imposed pursuant to this subpart or make payment arrangements acceptable to BIS, the matter may be referred for administrative collection measures by the Department of the Treasury or to the United States Department of Justice for appropriate action to recover the penalty in a civil suit in a federal district court.

**§ 791.318 Finding of Violation.**

(a) *When issued.* (1) BIS may issue an initial finding of violation that identifies a violation if BIS:

(i) Determines that there has occurred a violation of any provision of this subpart, or a violation of the provisions of any exemption, general authorization, specific authorization, regulation, order, directive, instruction, or prohibition issued by or pursuant to the direction or authorization of the Secretary pursuant to this subpart or otherwise under IEEPA;

(ii) Considers it important to document the occurrence of a violation; and

(iii) Concludes that an administrative response is warranted but that a civil monetary penalty is not the most appropriate response.

(2) An initial finding of violation shall be in writing and may be issued whether or not another agency has taken any action with respect to the matter.

(b) *Response*—(1) *Right to respond.* An alleged violator may contest an initial Finding of Violation by providing a written response to BIS.

(2) *Deadline for response; default determination.* A response to an initial Finding of Violation must be made within 30 days as set forth in paragraphs (b)(2)(i) and (ii) of this section. The failure to submit a response within 30 days shall be deemed to be a waiver of the right to respond, and the initial Finding of Violation will become final and will constitute final agency action. The violator may seek judicial review of that final agency action in federal district court.

(i) *Computation of time for response.* A response to an initial finding of violation must be electronically transmitted on or before the 30th day after the date of delivery by BIS.

(ii) *Extensions of time for response.* If a due date falls on a federal holiday or weekend, that due date is extended to include the following business day. Any other extensions of time will be granted, at the discretion of BIS, only upon specific request to BIS.

(3) *Form and method of response.* A response to an initial finding of violation need not be in any particular form, but it must be typewritten and signed by the alleged violator or a representative thereof, contain information sufficient to indicate that it is in response to the initial finding of violation, and include the BIS identification number listed on the initial finding of violation. A digital signature is acceptable.

(4) *Information that should be included in response.* Any response

should set forth in detail why the alleged violator either believes that a violation of the provisions of this subpart did not occur and/or why a finding of violation is otherwise unwarranted under the circumstances. The response should include all documentary or other evidence available to the alleged violator that supports the arguments set forth in the response. BIS will consider all relevant materials submitted in the response.

(c) *Determination*—(1) *Determination that a finding of violation is warranted.* If, after considering the response, BIS determines that a final finding of violation should be issued, BIS will issue a final finding of violation that will inform the violator of its decision. Any action taken in a final finding of violation shall constitute final agency action. The violator has the right to seek judicial review of that final agency action in federal district court.

(2) *Determination that a finding of violation is not warranted.* If, after considering the response, BIS determines a finding of violation is not warranted, then BIS will inform the alleged violator of its decision not to issue a final finding of violation.

**§ 791.319 Severability.**

If any provision of this subpart is held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, or stayed pending further agency action or judicial review, the provision is to be construed so as to continue to give the maximum effect to the provision permitted by law, unless such holding will be one of utter invalidity or unenforceability, in which event the provision will be severable from this part and will not affect the remainder thereof.

[FR Doc. 2024–21903 Filed 9–23–24; 8:45 am]

BILLING CODE 3510–33–P

# Department of Commerce

Bureau of Industry and Security

15 CFR Part 7

[Docket No. 240227-0060]

Securing the Information and Communications Technology and Services

Supply Chain: Connected

Advance notice of proposed rulemaking

3/1/2024



to amend the current version of that order, FAA Order JO 7400.11H, dated August 11, 2023, and effective September 15, 2023. These updates would be published subsequently in the next update to FAA Order JO 7400.11. That order is publicly available as listed in the ADDRESSES section of this document.

FAA Order JO 7400.11H lists Class A, B, C, D, and E airspace areas, air traffic service routes, and reporting points.

### The Proposal

The FAA is proposing to amend 14 CFR part 71 by establishing Class E airspace extending upward from 700 feet above the surface to within a 6.4-mile radius of The Sigurd Anderson Airport, Webster, SD.

The FAA is proposing this action due to the development of new public instrument procedures at this airport and to support IFR operations.

### Regulatory Notices and Analyses

The FAA has determined that this proposed regulation only involves an established body of technical regulations for which frequent and routine amendments are necessary to keep them operationally current. It, therefore: (1) is not a “significant regulatory action” under Executive Order 12866; (2) is not a “significant rule” under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979); and (3) does not warrant preparation of a regulatory evaluation as the anticipated impact is so minimal. Since this is a routine matter that will only affect air traffic procedures and air navigation, it is certified that this proposed rule, when promulgated, will not have a significant economic impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

### Environmental Review

This proposal will be subject to an environmental analysis in accordance with FAA Order 1050.1F, “Environmental Impacts: Policies and Procedures” prior to any FAA final regulatory action.

### List of Subjects in 14 CFR Part 71

Airspace, Incorporation by reference, Navigation (air).

### The Proposed Amendment

In consideration of the foregoing, the Federal Aviation Administration proposes to amend 14 CFR part 71 as follows:

## PART 71—DESIGNATION OF CLASS A, B, C, D, AND E AIRSPACE AREAS; AIR TRAFFIC SERVICE ROUTES; AND REPORTING POINTS

■ 1. The authority citation for 14 CFR part 71 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g); 40103, 40113, 40120; E.O. 10854, 24 FR 9565, 3 CFR, 1959–1963 Comp., p. 389.

### § 71.1 [Amended]

■ 2. The incorporation by reference in 14 CFR 71.1 of FAA Order JO 7400.11H, Airspace Designations and Reporting Points, dated August 11, 2023, and effective September 15, 2023, is amended as follows:

*Paragraph 6005 Class E Airspace Areas Extending Upward From 700 Feet or More Above the Surface of the Earth.*

\* \* \* \* \*

### AGL SD E5 Webster, SD [Establish]

The Sigurd Anderson Airport, SD  
(Lat 45°17'35" N, long 94°30'49" W)

That airspace extending upward from 700 feet above the surface within a 6.4-mile radius of The Sigurd Anderson Airport.

\* \* \* \* \*

Issued in Fort Worth, Texas, on February 27, 2024.

Martin A. Skinner,  
Acting Manager, Operations Support Group,  
ATO Central Service Center.

[FR Doc. 2024–04317 Filed 2–29–24; 8:45 am]

BILLING CODE 4910–13–P

## DEPARTMENT OF COMMERCE

### Bureau of Industry and Security

### 15 CFR Part 7

[Docket No. 240227–0060]

RIN 0694–AJ56

### Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

**AGENCY:** Bureau of Industry and Security, U.S. Department of Commerce.

**ACTION:** Advance notice of proposed rulemaking.

**SUMMARY:** In this advance notice of proposed rulemaking (ANPRM), the Department of Commerce’s (Department) Bureau of Industry and Security (BIS) seeks public comment on issues and questions related to transactions involving information and communications technology and services (ICTS) that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or

subject to the jurisdiction or direction of foreign countries or foreign non-government persons identified in the Department’s regulations, pursuant to the Executive Order (E.O.) entitled “Securing the Information and Communications Technology and Services Supply Chain,” and that are integral to connected vehicles (CVs), as defined herein. This ANPRM will assist BIS in determining the technologies and market participants that may be most appropriate for regulation pursuant to the E.O.

**DATES:** Comments must be received on or before April 30, 2024.

**ADDRESSES:** All comments must be submitted by one of the following methods:

- *The Federal eRulemaking Portal:* <https://www.regulations.gov> at docket number BIS–2024–0005.

- *Email directly to: connected vehicles@bis.doc.gov.* Include “RIN 0694–AJ56” in the subject line.

- *Instructions:* Comments sent by any other method, to any other address or individual, or received after the end of the comment period, may not be considered. For those seeking to submit confidential business information (CBI), please clearly mark such submissions as CBI and submit by email, as instructed above. Each CBI submission must also contain a summary of the CBI, clearly marked as public, in sufficient detail to permit a reasonable understanding of the substance of the information for public consumption. Such summary information will be posted on [regulations.gov](https://www.regulations.gov).

### FOR FURTHER INFORMATION CONTACT:

Marc Coldiron, U.S. Department of Commerce, telephone: 202–482–3678. For media inquiries: Jeremy Horan, Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce: [OCPA@bis.doc.gov](mailto:OCPA@bis.doc.gov).

### SUPPLEMENTARY INFORMATION:

#### I. Authorities

On May 15, 2019, the President issued E.O. 13873, “Securing the Information and Communications Technology and Services Supply Chain,” pursuant to the President’s authority under the Constitution and the laws of the United States, including the International Emergency Economic Powers Act (IEEPA), the National Emergencies Act (50 U.S.C. 1601, *et seq.*), and Section 301 of Title 3, United States Code. E.O. 13873 declares a national emergency regarding the ICTS supply chain, finding that “the unrestricted acquisition or use in the United States of information and communications

technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.” The E.O. further notes that “[t]his threat exists both in the case of individual acquisitions or uses of such technology or services, and when acquisitions or uses of such technologies are considered as a class.”

In accordance with the National Emergencies Act, the President has declared each year since E.O. 13873 was published that the national emergency continues in effect. *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain*, 85 FR 29321 (May 14, 2020); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain*, 86 FR 26339 (May 13, 2021); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain*, 87 FR 29645 (May 13, 2022); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain*, 88 FR 30635 (May 11, 2023).

To address identified risks to national security from ICTS transactions, E.O. 13873 grants the Secretary of Commerce (Secretary) (in consultation with other agency heads identified in the E.O.) the authority to review and, if necessary, impose mitigation measures on or prohibit any ICTS transaction, which includes any 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. In order to require mitigation for or to prohibit an ICTS transaction or class of transactions, the Secretary, in consultation with other agency heads, must first determine that the ICTS transaction or class of transactions at issue: (1) involves ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the

jurisdiction or direction of a foreign adversary, which the E.O. defines 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 United States persons;” and (2) poses:

A. an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;

B. an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or

C. otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

These factors are collectively referred to as “undue or unacceptable risks.”

E.O. 13873 additionally provides the Secretary with the authority to issue rules establishing criteria by which particular technologies or market participants may be categorically included in or categorically excluded from prohibitions established pursuant to the E.O. To date, the Department has not pursued or used this authority to regulate ICTS transactions on a category- or class-wide basis. Furthermore, E.O. 13873 grants the Secretary the authority to identify a mechanism and relevant factors for the negotiation of mitigation measures that would allow approval of an otherwise prohibited transaction.

## II. Background

### a. Purpose

Pursuant to the authority delegated to the Secretary under E.O. 13873, BIS is considering proposing rules that would prohibit certain ICTS transactions or classes of ICTS transactions by or with persons who design, develop, manufacture, or supply ICTS integral to CVs and are owned by, controlled by, or subject to the jurisdiction or direction of foreign governments or foreign non-government persons identified at 15 CFR 7.4 (hereinafter referred to as “15 CFR 7.4 entities”). BIS is also considering proposing measures that would allow market participants to engage in otherwise prohibited transactions or classes of transactions if the undue or unacceptable risks of those ICTS transactions can be sufficiently mitigated using measures that are monitorable.

The purpose of this ANPRM is to gather information to support BIS’s potential development of a rule regarding ICTS integral to CVs. In particular, BIS seeks public input on certain definitions and its assessment of how a class of transactions involving ICTS integral to CVs, when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity, could present undue or unacceptable risks to U.S. national security. These include risks related to threats from 15 CFR 7.4 entities, capabilities of CVs that may increase the likelihood of vulnerabilities, and consequences to U.S. persons and critical infrastructure if these vulnerabilities are exploited or intentionally inserted by 15 CFR 7.4 entities. BIS solicits input on the ICTS most integral to CVs and most vulnerable to compromise, as well as input on mechanisms to address identified risks through potential design, implementation standards and protocols, manufacturing integrity protection systems and procedures, or prohibitions.

BIS recognizes the benefits of CV technologies and does not imply through this ANPRM that technologies such as vehicle-to-everything (V2X) communications are generally unsafe for use in the United States. Indeed, these new vehicles often provide safer, more fuel-efficient travel. However, E.O. 13873 is focused on risks that ICTS transactions might present to national security. Therefore, this ANPRM, which is being issued pursuant to the authorities granted under E.O. 13873, seeks public comment on potential means to narrowly address involvement by persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities in the design, development, manufacture, or supply of ICTS integral to CVs where that involvement may create undue or unacceptable risk to U.S. national security.

Additionally, BIS seeks comment on whether to create a process for the public to request approval to engage in an otherwise prohibited transaction by demonstrating that a particular transaction adequately addresses the risk to U.S. national security. BIS encourages public feedback to help inform the rulemaking process, particularly regarding transactions where ICTS supply chains may be impacted by any proposed rule.

### b. Definitions

As an initial matter, BIS is interested in receiving comments on the applicable

definition for *connected vehicle* or *CV* within the context of transactions involving ICTS incorporated into such vehicles. BIS could define a *connected vehicle* as an automotive vehicle that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device. Such a definition would likely include automotive vehicles, whether personal or commercial, capable of global navigation satellite system (GNSS) communication for geolocation; communication with intelligent transportation systems; remote access or control; wireless software or firmware updates; or on-device roadside assistance.

CVs also integrate hardware that enables connectivity within the vehicle and/or external connectivity with devices, networks, applications, and services outside the vehicle. CV safety applications are designed to increase situational awareness and reduce traffic accidents through vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and increasingly, V2X communications, as contemplated in a series of Department of Transportation workshops focusing on V2X communications titled “Saving Lives with Connectivity.” See Bill Canis, Cong. Research Serv., R46398, *Motor Vehicle Safety: Issues for Congress* 8 (2021), <https://sgp.fas.org/crs/misc/R46398.pdf>; U.S. Dep’t of Transp., ITS V2X Communications Summit (2023), [https://www.its.dot.gov/research\\_areas/emerging\\_tech/html/ITS\\_V2X\\_CommunicationSummit.htm](https://www.its.dot.gov/research_areas/emerging_tech/html/ITS_V2X_CommunicationSummit.htm).

BIS arrived at this definition by reviewing existing definitions for connected vehicles from trade associations and leading research publications including the Connected Vehicle Reference Implementation Architecture, U.S. Department of Transportation’s Intelligent Transportation Systems Joint Program Office, Institute of Electrical and Electronics Engineers research, and Society of Automotive Engineers standards.

Various terms exist across industry and the U.S. Government to refer to vehicles that exhibit the connected features explained above. In addition to input on the term *connected vehicle*, BIS is seeking comment on alternative terminology that might better correspond to the definition of *connected vehicle* discussed above. Such terminology could include

“networked vehicles,” “intelligent connected vehicles,” “software-defined vehicles,” or “connected autonomous vehicles.”

This ANPRM seeks comment on the definitions to use for a rule regarding transactions involving ICTS integral to CVs, and specifically:

1. In what ways, if any, should BIS elaborate on or amend the potential definition of *connected vehicle* stated above? If amended, how will the revised definition enable BIS to better address national security risks arising from classes of transactions involving ICTS integral to CVs?

2. Is the term *connected vehicles* broad enough to include autonomous vehicles and related equipment, electric vehicles, or other alternative power sources and related technologies? Does a better term exist to describe the broader scope?

3. Are there other commonly used definitions for CVs that BIS should consider when defining a class of ICTS transactions, including definitions from industry, civil society, and foreign entities? If so, why would those definitions be more appropriate for the purposes of a rule?

#### *c. Risks Associated With Connected Vehicles*

The automotive industry is constantly undergoing innovation and change, and as communications and broadband technology advance, so do the technologies used in automobiles. Particularly relevant for the purposes of this ANPRM, new technology has fueled a rise in interconnectivity and autonomous capabilities in new vehicles. An automobile’s value is no longer determined only by the engine, steering system, and other traditional automotive parts. Increasingly, an automobile is a compilation of on-board computers; sensors; cameras; batteries; and various other categories of ICTS software or hardware tied together through automotive software systems. Over time, vehicle connections to the internet will evolve even further and new communication technology will advance vehicle capabilities. These technological advances will continue to rely on significant data collection not only about the vehicle and its myriad components, but also the driver, the occupants, the vehicle’s surroundings, and nearby infrastructure. Moreover, CVs allow for information to be gathered and shared to address both individual and societal transportation needs. These technologies may expose the vehicles, and the sectors they support, to new cyber-enabled attack vectors and vulnerabilities, with the potential to

create novel and potentially profound risks to national security and public safety. Cyber-enabled vulnerabilities can be exacerbated if the ICTS integral to CVs is designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity.

#### *i. Threat From 15 CFR 7.4 Entities*

E.O. 13873 defines the term “foreign adversary” to mean 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 U.S. persons. In the rules implementing the E.O. at 15 CFR 7.4(a), the Secretary has identified the following as foreign adversaries: the People’s Republic of China, including the Hong Kong Special Administrative Region (PRC); Republic of Cuba; Islamic Republic of Iran; Democratic People’s Republic of Korea; Russian Federation; and Venezuelan politician Nicolás Maduro (Maduro Regime).

The incorporation of ICTS products and services used in the United States from persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities’ can offer a direct entry point to sensitive U.S. technology and data and bypass measures intended to protect U.S. persons’ safety and security. This may allow actors with insider access to gain entry to the systems the ICTS connects to and ultimately engage in malicious cyber activity. Consequently, this exploitation may result in undue risks to ICTS and critical infrastructure in the United States and unacceptable risks to national security.

The PRC presents a particularly acute and persistent threat to the United States ICTS supply chain. According to the Office of the Director of National Intelligence, the PRC likely represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks. See Off. of the Director of Nat’l Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* 10 (2023), <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>. The PRC is almost certainly capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States and has conducted cyber espionage operations that have compromised telecommunications firms, providers of managed services, and broadly used software. *Id.* At 10. In short, the PRC has

engaged in a pattern of hacking and cyber intrusion that demonstrates the PRC's intent to compromise and exploit U.S. ICTS supply chains and critical infrastructure, threatening U.S. national security.

The PRC's legal structure also gives broad authority to the state to co-opt private companies to pursue its objectives. A host of laws give the PRC government the authority to compel companies located in the PRC, including automakers and their suppliers, to cooperate with PRC intelligence and security services. The PRC's 2021 Data Security Law, for example, makes all private data available to the PRC state when it is needed for "national security." See National People's Congress, *Data Security Law of the People's Republic of China*, Art. 35, [http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209\\_385109.html](http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html). The PRC's 2017 National Intelligence Law imposes affirmative obligations on entities and persons subject to the PRC's jurisdiction to cooperate with intelligence agencies—Article 17 allows PRC intelligence officials to take control of a private organization's facilities, including its communications equipment. See National People's Congress, *National Intelligence Law (as amended, 2018)*, [http://www.npc.gov.cn/npc/c2/c30834/201905/t20190521\\_281475.html](http://www.npc.gov.cn/npc/c2/c30834/201905/t20190521_281475.html). The PRC's 2015 National Security Law obliges citizens and private companies to provide security and military agencies with all "necessary support and assistance." See State Council of the People's Republic of China, *National Security Law*, Art. 77(5), [https://www.gov.cn/zhengce/2015-07/01/content\\_2893902.htm](https://www.gov.cn/zhengce/2015-07/01/content_2893902.htm). Beyond legal obligations, companies established in the PRC may be required to create internal Chinese Communist Party (CCP) committees that can exercise influence over corporate decisions. See National People's Congress, *Company Law of the People's Republic of China*, Art. 19, [https://www.npc.gov.cn/zgrdw/npc/xinwen/2018-11/05/content\\_2065671.htm](https://www.npc.gov.cn/zgrdw/npc/xinwen/2018-11/05/content_2065671.htm).

The combination of legal authorities and opaque CCP influence make private companies that are subject to the PRC's jurisdiction susceptible to requests from intelligence and military officials. PRC officials can compel PRC firms to provide the PRC government with data, logical access, encryption keys, and other vital technical information, as well as to install backdoors or bugs in equipment which create security flaws easily exploitable by PRC authorities. U.S. Dep't of Homeland Security, *Data*

*Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the Peoples Republic of China* 2 (2020), [https://www.dhs.gov/sites/default/files/publications/20\\_1222\\_data-security-business-advisory.pdf](https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf). Original equipment manufacturers (OEMs) for vehicles in the PRC, due to the vast amounts of data generated by their products, are notable targets for government access. According to open-source reporting, over 200 automakers that operate in the PRC are legally obligated to transmit real-time vehicle data, including geolocation information, to government monitoring centers. See Erika Kinetz, *In China Your Car Could Be Talking To The Government*, Associated Press News (Nov. 29, 2018), <https://apnews.com/article/4a749a4211904784826b45e812cfff4ca>. This pervasive data sharing, which provides the PRC government with detailed information on the behaviors and habits of individuals, is indicative of a broader approach to co-opting private companies—one that raises significant concerns about how the PRC government might exploit the growing presence of PRC OEMs and manufacturers of ICTS integral to CVs in foreign markets. The combination of these factors uniquely elevates BIS's concern regarding PRC participation in the ICTS supply chain for CVs in the United States.

BIS seeks to better understand the role of persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities, particularly the PRC, in the ICTS supply chain for CVs, and the leverage these entities might exert as a result. In particular, the ANPRM seeks comments on the following issues:

4. Please describe the ICTS supply chain for CVs in the United States. Particularly useful responses may include information regarding:

a. categories of ICTS, such as software or hardware, that are integral to CVs operating in the United States;

b. market leaders for each distinct phase of the supply chain for ICTS integral to CVs (such as design, development, manufacturing, or supply) including, but not limited to: OEMs, tier one, tier two, and tier three suppliers, and service providers;

c. geographic locations where software (such as the vehicle operating system), hardware (such as light detection and ranging (LiDAR) sensors), or other ICTS components integral to CVs in use in the United States are designed, developed, manufactured, or supplied;

d. involvement in any sector or sub-sector of the U.S. ICTS supply chain for CVs by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity; and

e. geographic locations where data from CVs in use in the United States is transmitted, stored, or analyzed.

5. Are there ICTS integral to CVs for which persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity are sole source suppliers? To what extent do OEMs of CVs in use in the United States rely upon suppliers wholly or partially owned by a company based in or under the control of a 15 CFR 7.4 entity?

6. In what ICTS hardware or software for CVs do persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity maintain a technological advantage over U.S. and other foreign counterparts and how may this dynamic evolve in the coming years?

7. How, and to what degree, does CV automotive software connect to GNSS systems that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity? for geolocation and other functions?

8. How might a disruption to the supply of ICTS components for CVs in use in the United States, including hardware and software, from persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity affect OEMs of CVs in use in the United States and ICTS suppliers? Where possible, please specify which disruptions to component supply would be particularly detrimental.

9. To what extent can OEMs procure alternative sources of ICTS integral to CVs that do not constitute ICTS from persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities?

10. Please describe the relationship between OEMs of CVs in use in the United States and their ICTS suppliers. Particularly useful responses may include the type of information that is shared between OEMs of CVs in use in the United States and their ICTS suppliers in the normal course of business, how this information is shared, what access or administrative privileges are typically granted, and if suppliers have any capability for remote access or ability to provide firmware or software updates.

11. What risks might be posed by aftermarket ICTS integrated onboard CVs and interfaced with vehicle systems, such as tracking devices, cameras, and wireless-enabled

diagnostic interfaces? Should aftermarket automotive systems or components be considered integral to CV operation?

12. To what extent are ICTS components of CVs designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity present in critical infrastructure sectors? Are there instances of municipal, state, or federal funding for procurement of such 15 CFR 7.4 entities' ICTS integral to CVs for use in critical infrastructure sectors?

13. What other instances exist where persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity, are integrated into the ICTS supply chain for CVs?

#### ii. Capabilities of Connected Vehicles May Increase the Likelihood of Vulnerabilities 15 CFR 7.4 Entities Could Exploit

CVs and the components that enable their functionality present opportunities for exploitation by 15 CFR 7.4 entities via insider access, which could potentially result in severe consequences to U.S. persons and critical infrastructure. Increasing the number and scope of wireless connected components in a vehicle also increases the attack surfaces through which a malicious actor can gain initial entry. As CVs gain new and different connectivity capabilities, design, implementation, and operational protocols need to be added to address new attack surfaces and maintain the confidentiality, integrity, and availability of the data that traverse any one functional system. As demonstrated in controlled environments, attack vectors can be exploited and may provide access to other functional systems within a CV. Moreover, once one subsystem has been compromised, depending on the nature of the vulnerability and the design of the vehicle network architecture, the attacker might have the ability to move laterally and eventually gain access to other functional automotive systems. While integrated functionality may provide seamless communication, comfort, and operability for the consumer, it is possible that unauthorized remote access to a particular sensor system could be escalated to vehicle systems and operations, potentially resulting in injury, loss of life, and disruption to critical infrastructure networks.

Preliminarily, BIS has identified the following capabilities associated with CVs that may increase the likelihood of vulnerabilities that 15 CFR 7.4 entities could exploit:

**Data Collection:** CVs rely on the collection and integration of broad and varied data to improve the vehicle's functionality and safety. This data, which can encompass vehicle-level data (e.g., driver behavior, vehicle status, geolocation, biometrics, driver mobile phone data) and environmental-level data (e.g., detailed mapping data, object detection, traffic patterns), are extracted through various onboard systems and sensors. The Advanced Driver-Assistance System (ADAS) of a CV, for example, typically relies on a combination of sensors—radar, LiDAR, ultrasonic, audio, and video—that are constantly collecting and processing data. CVs now collect data inside the cockpit as well. Consumer and commercial CVs increasingly incorporate driver monitoring systems (DMS) to ensure the driver remains alert and fully able to take control of the car should autonomous systems fail, and to ensure commercial truck drivers remain on schedule. More sophisticated DMS feature driver-facing cameras—including eye tracking, facial recognition, and microphones—collect potentially sensitive information about drivers and passengers. This increases the sensitivity of the data that CVs collect, potentially providing 15 CFR 7.4 entities with access to biometric information in addition to environmental data.

**Connectivity:** CVs are connected to and can communicate with a range of external sources, including the OEM and third-party service providers, as well as in-car devices like smart phones. In an increasing subset of vehicles, telematics systems connect the vehicle with cloud-based services to provide onboard systems with external data streams (e.g., geolocation, streaming service, assistance service, emergency notification) and underlie many of a CV's core functionalities. V2X systems, when widely implemented, will support the broadcast and reception of messages that enable safety alerts and mobility advisories. Providing broadcast (radio) communication capabilities that facilitate driver assistance capabilities may open cybersecurity vectors that need to be addressed to ensure broadcast message integrity and authenticity through design, standards, implementation and manufacturing protocols, and to prevent possible message and transmission misbehavior.

Further, interconnectivity in the software or hardware components may amplify risks posed by ICTS integral to CVs that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR

7.4 entity. For example, OEMs enable communication with their vehicle after sale even when a customer does not subscribe to services, including by providing software updates and refinements, as well as by enabling or disabling subscription-based features. This access by the OEM to the CV provides numerous opportunities for 15 CFR 7.4 entities that own, control, or have the ability to exert jurisdiction or direction over the OEM, to insert vulnerabilities allowing for future backdoor attacks and other malicious behavior. Additionally, individually connected components and sensors are capable of transmitting data separately from the vehicle's broader communications suite, including receiving over the air (OTA) updates without the knowledge or consent of the vehicle owner or OEM. BIS seeks to better understand the capabilities associated with technical trends—both current and future—in CV design and the ICTS components therein. In particular, the ANPRM seeks further comment on the following:

14. What is the full scope of data collection capabilities in CVs and the aggregation and scale of data that CVs could collect on U.S. persons, entities, geography, and infrastructure? Who has authorized access to, or control of, data collected by CVs?

15. What types of remote access or control do OEMs have over their CVs? Please describe what software or other mechanisms allow for such remote access or control by the OEM to occur.

16. What cybersecurity concerns may arise from linkages between sensors in CVs? To what extent can individual sensors and components communicate OTA independently from the CV's Operating System (OS)?

17. What standards, best practices, and industry norms are used to secure the interconnection between vehicles and charging infrastructure? How are battery management systems (BMS) integrated into a vehicle's automotive software systems, and how are they protected from malware?

18. How do manufacturers supplement existing cybersecurity standards and best practices such as the National Highway Traffic Safety Administration's *Cybersecurity Best Practices for the Safety of Modern Vehicles* at each step of the CV supply chain, including design, manufacturing, and operation?

a. Particularly useful responses will be specific about the types of programs and practices used such as test and verification, bug bounties, white hat programs, or end-to-end encryption to secure the link between vehicle and

server. See Nat'l Highway Traffic Safety Admin., *Cybersecurity Best Practices for the Safety of Modern Vehicles* (2022), <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf>; see also Cybersecurity and Infrastructure Security Agency, *Autonomous Ground Vehicle Security Guide: Transportation Systems Sector* (2021), <https://www.cisa.gov/resources-tools/resources/autonomous-ground-vehicle-security-guide>.

19. Please describe the automotive software development cycle. BIS is particularly interested in learning:

a. The degree to which OEMs license software, as opposed to developing it internally;

b. The extent to which software is developed outside the United States and, if so, where;

c. What measures are taken to ensure software security and integrity during the development cycle;

d. If OEMs partner or co-develop automotive software with any persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity; and

e. The extent to which software that is embedded in hardware (e.g., firmware) is subject to the development cycle described above.

20. Please describe the relationship between CV OEMs and cloud service providers (CSPs). Particularly useful responses may describe what access privileges, controls, and remote capabilities with respect to CV OEM systems are afforded to the CSP. Additionally, what are the common shared responsibility models between a CSP and a CV OEM and how are the communication and systems protected?

21. How do CV OEMs verify the bill of materials and software bill of materials as authentic for vendors and suppliers, specifically regarding OS, telematic systems, ADAS, Automated Driving Systems (ADS), satellite or cellular telecommunication systems, and BMS? If a software bill of materials is required, to what extent does it provide information regarding software vulnerabilities, and how is this information used, stored, and protected?

22. To what extent is software from vendors and suppliers tested and verified to comply with OEM requirements?

23. What vendor-vetting and supply chain security practices do OEMs employ when procuring ICTS integral to CVs?

iii. Consequences

The ability of a 15 CFR 7.4 entity to compel private companies through

applicable legal frameworks, combined with the exploitation of vulnerabilities created by the increase in capabilities of the ICTS integral to CVs, has the potential to create severe and, in certain instances, catastrophic consequences for U.S. persons and critical infrastructure. Through ICTS designed, developed, manufactured, or supplied by persons subject to the ownership, control, jurisdiction, or direction of a 15 CFR 7.4 entity, the intelligence agencies of that entity could obtain access to a wide range of information from companies in the CV ICTS supply chain to exfiltrate, collect, and aggregate sensitive data on U.S. persons. These data include location, traffic patterns, audio and video recordings of the inside and outside of the car, as well as information about the driver's identity, finances, contacts, and home address, which can be collected by CVs themselves or by a passenger's mobile device connected to a CV.

In addition, backdoors embedded in a CV's software could enable a 15 CFR 7.4 entity under certain conditions to obtain control over various vehicle functions that could include the ability to disable the vehicle completely. A group of researchers were able to demonstrate a vulnerability in an OEM's Bluetooth software that allowed access to some vehicle control systems, initiating remote actions such as activating the brakes and turning the steering wheel. See Consumer Watchdog, *Kill Switch: Why Connected Cars Can Be Killing Machines and How to Turn Them Off* 37–40 (2019), <https://consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19.pdf>. A similar ability in the hands of a 15 CFR 7.4 entity that can control or direct an OEM could allow that entity to disable the controls on an individual vehicle while it was being driven or to sabotage entire fleets without having physical access to the vehicles. Finally, because of CVs' connectivity, they could be used to access multiple critical infrastructure systems with which they interact, including telecommunications networks, transportation systems, and the electrical grid. As CV technology advances, vehicles and charging infrastructure may increasingly communicate with these systems to manage traffic flows and grid load. As such, the proliferation of CVs containing vulnerable ICTS from persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity could provide that entity with a platform for launching distributed denial of service attacks against intelligent transportation systems,

satellite or cellular communications hardware, or other critical infrastructure. See Mohammad Ali Sayed, et al., *Electric Vehicle Attack Impact on Power Grid Operation*, 137 Int'l J. Electrical Power & Energy Sys. 107784 (2022), <https://www.science-direct.com/science/article/abs/pii/S0142061521010048>; Numaan Huq, et al., *Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud, and Other Connected Technologies*, Trend Micro Res. (2021), [https://documents.trendmicro.com/assets/white\\_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf](https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf); Anastasios Giannaros, et al., *Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions*, 3 J. of Cybersecurity and Privacy 493 (2023). Given these threats, vulnerabilities, and potential consequences, BIS is considering identifying the following automotive software systems as the ICTS integral to CVs most likely to present undue or unacceptable risks if exploited by 15 CFR 7.4 entities: (i) vehicle OS; (ii) telematics systems; (iii) ADAS; (iv) ADS; (v) satellite or cellular telecommunication systems; and (vi) BMS.

As BIS considers whether and how to regulate these software systems, it seeks additional information, including:

24. Are there ICTS integral to CVs other than those identified in this ANPRM that could present material risks if they were designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction of a 15 CFR 7.4 entity? If so, please discuss how the ICTS could be exploited to pose such a risk.

25. Of the ICTS integral to CVs identified in this ANPRM, which present the greatest risk to safety or security if they are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity?

26. As ADS systems evolve and developers rely on cellular systems to communicate with ADS-enabled vehicles to support overall operational capability (e.g., communications to a fleet management office), what should the U.S. government consider in order to support the development of this technology securely from 15 CFR 7.4 entity malign activity?

### III. Additional Questions for Comment

This ANPRM seeks comment on processes and mechanisms that BIS could implement in a potential rule to authorize an otherwise prohibited ICTS



transaction with the adoption of mitigation measures.

#### *Authorizations and Mitigations*

27. In what instances would granting a temporary authorization to engage in an otherwise prohibited transaction under a proposed rule be necessary and in the interest of the United States to avoid supply chain disruptions or other unintended consequences?

28. What review criteria should BIS implement when considering an application for a temporary authorization?

29. What specific standards, mitigation measures, or cybersecurity best practices should BIS consider when evaluating the appropriateness of a requested authorization?

30. Are there any U.S. government models, such as the Office of Foreign Assets Control's sanctions programs or the Export Administration Regulations, that this program should consider emulating in granting authorizations?

#### *Economic Impact*

31. What economic impacts to U.S. businesses or the public, if any, might be associated with the regulation of ICTS integral to CVs contemplated by this ANPRM? If responding from outside the United States, what economic impacts to local businesses and the public, if any, might be associated with regulations of ICTS integral to CVs?

32. What, if any, anticompetitive effects may result from regulation of ICTS that is integral to CVs as contemplated by this ANPRM? And what, if anything, can be done to mitigate the anticompetitive effects of regulation of ICTS?

33. What types of U.S. businesses or firms (e.g., small businesses) would likely be most impacted by the program contemplated in this ANPRM? If responding from outside the United States, what types of local businesses or firms (e.g., small businesses) would likely be most impacted by the program contemplated in this ANPRM?

34. What actions can BIS take, or provisions could it add to any proposed regulations, to minimize potential costs borne by U.S. businesses or the public? If responding from outside the United States, what actions can BIS take, or what provisions could it add to any proposed regulations, to minimize potential costs borne by local businesses or the public?

35. What new due diligence, compliance, and recordkeeping controls will U.S. persons anticipate needing to undertake to comply with any proposed regulations regarding ICTS integral to

CVs that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities?

Elizabeth L.D. Cannon,  
*Executive Director, Office of Information and Communications Technology and Services.*  
[FR Doc. 2024-04382 Filed 2-29-24; 8:45 am]  
BILLING CODE 3510-33-P

## FEDERAL TRADE COMMISSION

### 16 CFR Part 461

RIN 3084-AB71

#### Trade Regulation Rule on Impersonation of Government and Businesses

**AGENCY:** Federal Trade Commission.

**ACTION:** Supplemental notice of proposed rulemaking; request for public comment.

**SUMMARY:** The Federal Trade Commission (FTC or Commission) requests public comment on its proposal to amend the trade regulation rule entitled Rule on Impersonation of Government and Businesses (Impersonation Rule or Rule) to revise the title of the Rule, add a prohibition on the impersonation of individuals, and extend liability for violations of the Rule to parties who provide goods and services with knowledge or reason to know that those goods or services will be used in impersonations of the kind that are themselves unlawful under the Rule. The Commission believes these changes are necessary and such impersonation is prevalent, based on all comments it received on the Rule and other information discussed in this document. The Commission now solicits written comment, data, and arguments concerning the utility and scope of the proposed revisions to the Impersonation Rule.

**DATES:** Comments must be received on or before April 30, 2024.

**ADDRESSES:** Interested parties may file a comment online or on paper by following the instructions in the Comment Submissions part of the SUPPLEMENTARY INFORMATION section below. Write "Impersonation SNPRM, R207000" on your comment and file your comment online at <https://www.regulations.gov>. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Mail Stop H-144 (Annex I), Washington, DC 20580.

**FOR FURTHER INFORMATION CONTACT:** Claire Wack, [cwack@ftc.gov](mailto:cwack@ftc.gov), (202-326-2836).

**SUPPLEMENTARY INFORMATION:** The Commission invites interested parties to submit data, views, and arguments on the proposed amendments to the Impersonation Rule and, specifically, on the questions set forth in Section VIII of this supplementary notice of proposed rulemaking ("SNPRM"). The comment period will remain open until April 30, 2024. To the extent practicable, all comments will be available on the public record and posted at the docket for this rulemaking on <https://www.regulations.gov>. If interested parties request to present their position orally, the Commission will hold an informal hearing, as specified in section 18(c) of the FTC Act, 15 U.S.C. 57a(c). Any request for an informal hearing must be submitted as a written comment within the comment period and must include: (1) a request to make an oral submission, if desired; (2) a statement identifying the person's interests in the proceeding; and (3) any proposals to add disputed issues of material fact that need to be resolved during the hearing. See 16 CFR 1.11(e). Any comment requesting an informal hearing should also include a statement explaining why an informal hearing is warranted and a summary of any anticipated oral or documentary testimony. If the comment identifies disputed issues of material fact, the comment should include evidence supporting such assertions. If the Commission schedules an informal hearing, either on its own initiative or in response to request by an interested party, the FTC will publish a separate document notifying the public pursuant to 16 CFR 1.12(a) ("initial notice of informal hearing").

### I. Background

#### *A. Trade Regulation Rule on Impersonation of Government and Business*

Published elsewhere in this issue of the *Federal Register* is the Commission's final Trade Regulation Rule entitled "Rule on Impersonation of Government and Business," promulgated under the authority of section 18 of the FTC Act, 15 U.S.C. 57a(b)(2); the provisions of Part 1, Subpart B, of the Commission's Rules of Practice, 16 CFR 1.7-1.20; and the Administrative Procedure Act ("Impersonation Rule" or "Rule"). This authority permits the Commission to promulgate, modify, or repeal trade regulation rules that define with specificity acts or practices that are unfair or deceptive in or affecting