ALLIANCE FOR AUTOMOTIVE INNOVATION

October 28, 2024

Elizabeth L.D. Cannon
Executive Director
Office of Information and Communications Technology and Services
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, D.C. 20230

RE: Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

Dear Executive Director Cannon:

The Alliance for Automotive Innovation ("Auto Innovators") welcomes the opportunity to provide input to the Bureau of Industry and Security ("BIS") on its *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles* Notice of Proposed Rulemaking ("NPRM"). We appreciate the thoughtful, consultative, and deliberative process that BIS has led in developing this NPRM and look forward to further engagement with BIS as it finalizes this rule.

Auto Innovators represents the full auto industry, including the manufacturers producing most vehicles sold in the U.S., equipment suppliers, battery producers, semiconductor makers, technology companies, and autonomous vehicle developers. Our mission is to work with policymakers to realize a cleaner, safer, and smarter transportation future and to maintain U.S. competitiveness in cutting-edge automotive technology. Representing approximately 5 percent of the country's GDP, responsible for supporting nearly 10 million jobs, and driving $1 trillion in annual economic activity, the automotive industry is the nation's largest manufacturing sector.

We are fully committed to the national security of the U.S. and share the goals of this rulemaking. We are dedicated to working with BIS to develop a final rule that appropriately mitigates the undue or unacceptable risks associated with information and communications technologies and services (ICTS) designed, developed, manufactured, or supplied by foreign adversaries in connected vehicles in the U.S.

We recognize that this rulemaking marks the first time that BIS has utilized the authority provided to it under Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," to promulgate regulations that categorically prohibit certain transactions involving particular technologies. It is essential that BIS maintain its consultative approach to this

consequential and precedential rulemaking. It is also critical that BIS remain committed to developing a reasonable and practicable final rule that does not disrupt the auto industry in a way that is unnecessary for or disproportionate to its important national security goals. The observations and recommendations provided below are intended to assist BIS in striking this crucial balance.

KEY RECOMMENDATIONS

We commend BIS for a thoughtful and thorough proposed rule. The NPRM reflects a tailored approach to transactions that may pose risks to U.S. national security. For example, the NPRM's proposals to narrow the applicability to connected vehicles and vehicle connectivity system hardware from specific foreign adversary countries and to exclude automated driving system hardware are appropriate and appreciated.

The NPRM also clearly reflects efforts by BIS to understand and, where appropriate, accommodate the unique and complex nature of automotive supply chains. However, there are some areas within the proposed rule where adjustments or clarifications could further facilitate implementation and advance our shared national security goals. In particular, in the final rule, we recommend that BIS: (1) resolve definitional ambiguities; (2) reduce unintended impacts of the software prohibition; (3) ensure sufficient time to transition supply chains; and (4) protect proprietary and confidential business information.

(1) Resolve definitional ambiguities

The NPRM creates significant new compliance obligations for connected vehicle manufacturers and vehicle connectivity system hardware importers. It also indirectly imposes substantial new requirements on developers of vehicle connectivity system software and automated driving system software that supply software to connected vehicle manufacturers serving the U.S. market. To foster transparency and predictability with respect to compliance with, and enforcement of, this new rule, BIS and industry should be aligned in their understanding of the scope of the rule. At present, several terms or concepts outlined in the NPRM would benefit from additional clarity.

- Automated Driving System: BIS proposes to define "Automated Driving System" as "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)." The NPRM explains that this definition corresponds to automation levels 3, 4, and 5 as defined by SAE International standard J3016 and is intended to exclude Advanced Driver Assistance Systems (ADAS).

  We welcome the specific references to automation levels from SAE J3016 and the exclusion of ADAS. For clarity, we request that the specific references to J3016 and the clarifications relating to ADAS be incorporated in the definition contained within the regulatory text as follows:

  > "*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). The term Automated Driving System is used specifically to describe a Level 3, 4, or 5 driving automation system, as defined by SAE International standard J3016. The term Automated Driving System does not include a Level 1 or Level 2 driving automation system or the hardware and software that perform the dynamic driving task in such a system."

- Covered Software: BIS proposes to define "covered software" as "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." The use of the term "supports" in relation to the function of vehicle connectivity systems and automated driving systems creates ambiguity and may lead to an inadvertent misalignment between BIS and industry about what is or is not prohibited. In addition, the terms "primary processing unit" and "vehicle level" are not defined in the proposed rule and may result in some confusion as to what is within the scope of the rule.

  To address this, we recommend that BIS simplify the definition of covered software as follows:

  > "*Covered software* means software, in which there is a foreign interest, executed by the primary processing unit of the Vehicle Connectivity System or Automated Driving System item that directly enables the Vehicle Connectivity System or Automated Driving System function."

  We further recommend that BIS provide a definition of "primary processing unit" to promote a common understanding with industry. For example, BIS could define "primary processing unit" as "a processor configured to operate a real-time operating system or general-purpose operating system."

  We appreciate that the definition of software excludes open-source software. In the NPRM, BIS explains that open-source software is "software that can be freely used, modified, or distributed by anyone, with both access to the source code and the ability to contribute to the software's development and improvement." We recommend that BIS align its definition of "open-source software" with other definitions already in use by the federal government. To this end, BIS should consider aligning with the Cybersecurity and Infrastructure Security Agency (CISA) as the federal agency that is primarily responsible for engaging with industry on cybersecurity matters. In doing so, BIS could reference or duplicate the definition of "open source software" contained in CISA's 2023 Open Source Software Security Roadmap, which provides that:

  > "[Open Source Software] is software for which the human readable source code is made available to the public for use, study, re-use, modification, enhancement, and re-distribution."

Alternatively, BIS could cite to or replicate the definition of "open source software" contained within the *John C. McCain National Defense Authorization Act for Fiscal Year 2019* (Public Law 115-232) which provides that:

> "The term "open source software" means software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and re-distribution by the users of such software."

- Foreign Interest**:** Under the NPRM, a connected vehicle manufacturer is required to submit a Declaration of Conformity if there is a foreign interest in the covered software. BIS proposes to define "foreign interest" as "any interest in property, of any nature whatsoever, whether direct or indirect, by a non-U.S. person." BIS further explains in the NPRM that 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 licensing agreement related to the use of intellectual property – profit-sharing or fee arrangement, as well as any other cognizable interest."

  To help minimize the compliance burden without compromising the national security goals of the rule, we recommend that the definition of foreign interest be modified so that an interest in the software by a person from an allied country be treated the same as an interest in the software by a U.S. person and therefore not subject to the requirement to submit a Declaration of Conformity. BIS could consider referencing Group A countries from its own Export Administration Regulations in determining what countries constitute allied countries.

  We further recommend that the definition of "foreign interest" explicitly focus on whether the prohibited person has a cognizable interest in the property. For additional clarity, we recommend that BIS add the examples from the NPRM into the definition of "foreign interest" in the final rule.

  For example, "foreign interest" could be defined by BIS as:

  > "*Foreign interest*, for purposes of this subpart, means a cognizable interest in property, which includes a direct or indirect interest through ownership, intellectual property, contract, profit-sharing, or fee arrangement, by a person who is neither:
  >
  > (a) a U.S. person; nor
  >
  > (b) a person who is a citizen of an allied country and who is not owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."

- Hardware Bill of Materials**:** BIS proposes to define "Hardware Bill of Materials" (HBOM) as "a comprehensive list of parts, assemblies, documents, drawings, and components required to create a physical product." The NPRM notes that an HBOM would include "information identifying the manufacturer, related firmware, technical information, and descriptive information."

To help ensure alignment between BIS and industry on what specific elements are to be included in an HBOM, we recommend that BIS specifically identify a resource that can serve as an illustrative example to industry. One potential resource for consideration is the *HBOM Framework for Supply Chain Risk Management* developed by the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, a cross-sector body organized and co-chaired by CISA. BIS may also want to consider developing an HBOM model template that vehicle connectivity system hardware importers can leverage when developing their required HBOMs.

Finally, to align with industry's general understanding of the core elements of a traditional HBOM, we suggest that BIS remove the specific references to "documents" and "drawings" in the definition of HBOM and instead maintain focus on parts, assemblies, and components.

- Person Owned By, Controlled By, or Subject to the Jurisdiction or Direction of a Foreign Adversary: In the NPRM, BIS proposes to define "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" to mean: "(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 (1) through (4) 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."

  We welcome the illustrative examples provided by BIS in the NPRM but request additional clarity with respect to (1) and (4) to ensure alignment between industry and BIS and support the industry's good faith intent to comply. For example, it is not clear what constitutes "direction or control" by a foreign adversary or what is meant by a "dominant minority."

  Specifically, we recommend that BIS incorporate objective criteria into the definition. One option is to align with the criteria proposed by the U.S. Department of Justice in its recent Notice of Proposed Rulemaking on *Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons*. In doing so, BIS could also incorporate the more conservative thresholds implemented in the Department of Energy's *Final Interpretive Guidance on the Definition of*

Foreign Entity of Concern relating to Section 40207 of the *Bipartisan Infrastructure Law* and specify that the following persons would be considered persons "owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary":

(1) An entity that is 25 percent or more owned, directly or indirectly, by a foreign adversary, or that is organized or chartered under the laws of, or has its principal place of business in, a country controlled by a foreign adversary;

(2) An entity that is 25 percent or more owned, directly or indirectly, by an entity described in (a) or a person described in (3), (4), or (5);

(3) Any person that is an employee or contractor of a foreign adversary or of an entity that is described in (1), (2), or (5);

(4) Any person who is primarily a resident in the territorial jurisdiction of a foreign adversary; or

(5) Any person, wherever located, who otherwise acts as an agent, representative, or employee of a foreign adversary or any person who acts in any other capacity at the order, request, or direction of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, financed, or subsidized in whole or in majority part by a foreign adversary.

In addition to providing objective criteria to facilitate compliance, a decision to leverage the Department of Justice's proposed definition can help address the fact that many connected vehicle manufacturers, vehicle connectivity system hardware importers, and vehicle connectivity system and automated driving system software suppliers have facilities and operations in non-foreign adversary nations throughout the world that may be involved in the design, development, and manufacture of vehicles or components for the U.S. market. It can also provide additional clarity to industry that the involvement of any person from China or Russia in the development of vehicle connectivity system hardware, vehicle connectivity system software, or automated driving system software does not automatically make the import of that hardware or the import or sale of a connected vehicle that integrates that software a prohibited transaction.

- Software Bill of Materials: BIS proposes to define "Software Bill of Materials" 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."

  To provide further clarity on the specific elements to be included in the SBOM, we recommend that BIS identify a resource that can serve as an illustrative example to industry. Options for consideration include *The Minimum Elements For a Software Bill of Materials*

issued by the National Telecommunications and Information Administration in July of 2021 or the Informational Report on SBOMs that will soon be released by the Automotive Information Sharing and Analysis Center (Auto-ISAC). BIS may also want to consider developing an SBOM model template that connected vehicle manufacturers can use when developing their SBOMs.

- Vehicle Connectivity System: In the NPRM, BIS proposes to define a "Vehicle Connectivity System" 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."

  It is our understanding from the NPRM that BIS does not intend to capture within the definition of "Vehicle Connectivity Systems" other systems (e.g., power supply) that lack an independent wireless connection but may exchange data with a "Vehicle Connectivity System." In fact, BIS specifically states in the NPRM that it "has chosen to focus on the systems that ultimately facilitate the transmission of data both to and from the vehicle" and not systems that are "generally lacking their own data link, instead relying on communication through a VCS." To ensure a shared understanding between BIS and industry, we recommend that the definition of "Vehicle Connectivity System" be modified to reflect this important point.

  BIS further explains in the NPRM that its proposed definition would exempt most keyless entry fobs and immobilizers and certain internal wireless sensors and relays. While we appreciate and share the goal of excluding certain low-risk communication from the definition of "Vehicle Connectivity System," we are not confident that the delineation of communications below and above 450 MHz adequately achieves that goal. There is automotive-related communication above 450 MHz that we do not believe BIS intended to cover in the rule, including ultra-wideband-enabled key fobs using spectrum above 6 GHz and automotive radar using 77 GHz spectrum. To address this, we recommend that BIS consider explicitly excluding these two specific use cases from the definition of "Vehicle Connectivity Systems."

  For example, "Vehicle Connectivity System" could be defined as follows:

  > "*Vehicle Connectivity System (VCS)* means a hardware or software item installed in or on a completed connected vehicle that is dedicated to the function of enabling the transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz. VCS does not include a hardware or software item that:
  >
  > (1) supplies or manages power for the VCS;

(2) simply exchanges data with a VCS without impacting the ability of the VCS to transmit, receive, convert, or process radio frequency communications;

(3) enables the transmission, receipt, conversion, or processing of ultra-wideband communications for key fobs at a frequency over 6 GHz; or

(4) enables the transmission, receipt, conversion, or processing of automotive radar communications at a frequency of 77 GHz."

- VCS Hardware: BIS proposes to define "VCS hardware" as "software-enabled or programmable components and subcomponents that support the function of Vehicle Connectivity System or are part of an item that supports the function of Vehicle Connectivity Systems." The NPRM further identifies specific items that BIS would consider to be "VCS hardware," including "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." BIS also explains in the NPRM that "VCS hardware" does not include component parts that do not contribute to the communication function of VCS hardware and specifically references "brackets, fasteners, plastics, and passive electronics" as examples.

  There is still some vagueness as to what other component parts would be considered by BIS to "not contribute to the communication function of VCS hardware" and what electronics would be considered by BIS to be "passive electronics." We recommend that BIS modify the definition of "VCS hardware" to clarify that it applies only to components or subcomponents that are for installation in or on a connected vehicle and that directly enable, rather than support, the vehicle connectivity system function. We further recommend that BIS modify the definition of "VCS hardware" to make clear that only components or subcomponents that are software-enabled or programmable are included.

  For example, BIS could define "VCS hardware" as follows:

  > "*VCS hardware* means the following components and subcomponents for installation in or on a connected vehicle that directly enable the function of Vehicle Connectivity Systems or that are part of an item that directly enables the function of Vehicle Connectivity Systems if those components or subcomponents are software-enabled or programmable: 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 components or subcomponents that do not contribute to the communication function of Vehicle Connectivity Systems (e.g., brackets, fasteners, plastics, and passive electronics or antennas) or that are not software-enabled or programmable."

(2) Reduce unintended impacts of the software prohibition

Software that directly enables vehicle connectivity, such as cellular technology, was developed years ago and may very well have included persons who, under this rule, would have been considered persons under the ownership, control, or direction of a foreign adversary. Determining retroactively whether such a person was *ever* involved in the development of software, particularly with respect to software that is not specific or unique to vehicle connectivity systems or automated driving systems, is nearly impossible. Since connected vehicle manufacturers or relevant software suppliers may be unable to verify that no persons under the ownership, control, or direction of a foreign adversary were involved in the development of previously-developed software, it is conceivable that – under the NPRM as drafted – connected vehicle manufacturers may no longer be able to offer some basic connectivity options in their vehicles. Such an outcome would be incredibly disruptive to the automotive industry and its consumers in the U.S. and almost certainly not intended by BIS.

For this reason, we recommend that any software prohibitions apply prospectively and not to legacy vehicle connectivity system software developed prior to the effective date of the final rule. We also recommend that the rule not apply to automated driving system software if that software was developed prior to the effective date of the final rule, but only if the connected vehicle manufacturer can demonstrate that: (a) no foreign adversary maintains access to or control of that software; and (b) it has used industry best practices to conduct a full and comprehensive review of the software after such time that any foreign adversary had any access to or control of it.

(3) Ensure sufficient time to transition supply chains

As we noted in our comments to the ANPRM, the automotive supply chain that has developed to support increasingly sophisticated and advanced vehicles is one the world's largest and most complex. This, combined with the fact that vehicle systems undergo at least three to four years of engineering, testing, and validation before production, means that components cannot be easily swapped or altered to source from a different supplier. The timeline proposed by BIS in the NPRM for vehicle connectivity system hardware (MY 2030) will prove challenging for some connected vehicle manufacturers and vehicle connectivity system hardware importers. BIS should consider providing modestly more time (i.e., at least one additional year) for some manufacturers to either identify alternative suppliers or allow for their current suppliers to come into compliance if needed and to conduct the testing and validation that is required before new hardware components are integrated into production vehicles.

In addition, vehicle models do not generally undergo major redesigns every model year. Rather, it is only every four to six years that a manufacturer will undertake a major redesign of a vehicle model. Major redesigns occur when vehicle models are completely or nearly completely reengineered. In the interim, a particular vehicle model may experience only a minor refresh, which includes smaller changes such as updated headlights, new wheel designs, or new paint color options. vehicle connectivity system technologies and suppliers remain largely unchanged when a vehicle model undergoes only a refresh.

While the timelines proposed in the NPRM may provide time for manufacturers to identify new suppliers or to allow for current suppliers to come into compliance for new vehicle models or major redesigns of existing vehicle models, it is likely not sufficient for vehicle models that will already be in production when the rule takes effect but are not scheduled to undergo a major redesign until after MY 2030 (or MY 2031, if BIS adjusts the timeline as suggested above). To address this, we suggest that BIS make clear that the prohibitions apply only to vehicle models undergoing a major redesign in or after MY 2030 (or MY 2031, if BIS adjusts the timeline). Alternatively, BIS could phase-in the prohibition so that it applies to approximately 1/3 of a manufacturer's vehicles in year one, 2/3 of the manufacturer's vehicles in year two, and all of a manufacturer's vehicles in year 3. This should minimize production disruption and allow manufacturers and their suppliers to more easily accommodate adjustments at such time that vehicle models undergo a major redesign.

(4) Protect proprietary and confidential business information

The NPRM proposes that a connected vehicle manufacturers be required to submit to BIS a Software Bill of Materials (SBOM) for covered software as part of its Declaration of Conformity and that a connected vehicle manufacturer and a vehicle connectivity system hardware importer be required to submit to BIS a Hardware Bill of Materials (HBOM) as part of its Declaration of Conformity. Some information, including information about specific suppliers, contained within an SBOM or HBOM is decidedly proprietary in a highly competitive auto industry. To protect and preserve the proprietary nature of this supplier information, we recommend that the connected vehicle manufacturer or the vehicle connectivity system hardware importer be required to certify as part of its Declaration of Conformity that an SBOM or HBOM has been developed but not be required to submit the SBOM or HBOM to BIS as part of its Declaration of Conformity. Rather, the pertinent portions of the SBOM or HBOM would be made available to BIS upon request in connection with an audit or investigation and, in these instances, handled as confidential business information.

BIS should also consider taking a similar approach for some of the other elements of the proposed Declaration of Conformity. In particular, a list of third-party external endpoints for vehicle connectivity system hardware components and the documentation of due diligence may be other items that are required but not submitted automatically to BIS as part of the Declaration of Conformity and instead be made available to BIS upon request in connection with an audit or investigation.

Finally, to ensure that such confidential information is protected from disclosure or release, BIS should develop a submission system with proper firewalls and cybersecurity protections for any SBOM, HBOM, or other proprietary information that is submitted to it and should delete any proprietary information after an audit or investigation is complete.

ADDITIONAL RECOMMENDATIONS

In addition to the key recommendations outlined above, we make the following additional recommendations to BIS for its consideration.

- Specific Authorizations: We support the proposal within the NPRM to establish a mechanism and process through which entities can request a specific authorization to engage in an otherwise prohibited transaction. We understand that these requests will be time-limited and require appropriate mitigation measures. We also appreciate that these requests will be reviewed on a case-by-case basis and may require varying lengths of time depending on the complexity of the case.

  That being said, for product planning purposes, a timely decision by BIS to grant or deny a specific authorization request will be critical for connected vehicle manufacturers, Vehicle Connectivity System hardware importers, and developers of vehicle connectivity system or automated driving system software. For that reason, we recommend that the rule establish a 45-day deadline for BIS to issue a decision on a specific authorization request. We also recommend that the rule provide BIS with the ability to extend its time for issuing a decision beyond the 45-day deadline but only if notice is provided to the requester before the initial 45-day deadline passes.

  The NPRM also notes that, in an approval letter for a specific authorization, BIS will determine the effective date and duration of the authorization, which will be determined on a case-by-case basis. We understand and appreciate the need to provide BIS with some flexibility with respect to these matters. We also recognize the importance of certainty to manufacturers, hardware importers, and software developers for product planning purposes. We therefore recommend that the duration of a specific authorization be for no less than one model year.

  In addition, while we appreciate that there will not be a one-size-fits-all approach to BIS's consideration of specific authorizations, we urge BIS to expand upon and provide additional guidance on the information needed from a connected vehicle manufacturer or vehicle connectivity system hardware importer for BIS to consider and successfully process a specific authorization request. Having a basic starting point for engagement and discussion with BIS on such requests is likely to make the specific authorization process more efficient for both BIS and the requestor.

- General Authorizations: The NPRM proposes several general authorizations which would enable connected vehicle manufacturers and vehicle connectivity system hardware importers to engage in otherwise prohibited transactions.

  This includes a general authorization for connected vehicle manufacturers or vehicle connectivity system hardware importers that produce a total model year production of completed connected vehicles containing covered software or total model year production of vehicle connectivity system hardware that is less than 1,000 units. We support this small volume manufacturer general authorization but seek clarification that the limit applies to production specifically for the U.S. market and not to global production. We also urge BIS to consider raising the unit limit. In doing so, BIS should look to the National Highway Traffic

Safety Administration and its attempts to reduce compliance burdens for and otherwise meet the unique needs of small volume manufacturers in various motor vehicle safety standards.

In addition, if BIS decides to apply the software prohibition retroactively to software developed prior the effective date of the final rule, BIS may want to consider providing a time-limited general authorization for covered software to minimize the need for it to process a significant number of specific authorizations. For example, BIS could allow connected vehicle manufacturers to engage in otherwise prohibited covered software transactions but only to the extent the software: (a) was developed prior to the effective date of the final rule; and (b) will be integrated into a completed connected vehicle prior to MY 2030. In order to qualify for the time-limited general authorization, BIS could require compliance with stringent security requirements, such as: possessing and controlling the relevant source code within the U.S.; verifying that the software is free from vulnerabilities through the use of a recognized vulnerability assessment tool or a vulnerability scan conducted by an independent third party; maintaining cryptographic signatures of the covered software using keys controlled by the connected vehicle manufacturer; complying with ISO/SAE 21434 Threat Analysis and Risk Assessments for the covered software; and ensuring that no person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary had access to or any involvement in the design, development, manufacture, or supply of any modification whatsoever for the covered software after the effective date of the final rule. BIS could require that the connected vehicle manufacturer attest to compliance with these requirements in an annual certification provided to BIS that includes, among other things, technical documentation that demonstrates how the connected vehicle manufacturer is complying.

- Interpretive Guidance: The NPRM proposes to include a mechanism for BIS to issue advisory opinions to connected vehicle manufacturers, vehicle connectivity system hardware importers, and other interested parties on the applicability of the prohibitions. The NPRM notes that BIS will only consider advisory opinion requests for actual, not hypothetical, prospective transactions.

  We appreciate and support this proposed advisory opinion mechanism but expect that more clarity and guidance will be required by industry to implement the rule. To that end, we recommend that BIS also establish a mechanism through which connected vehicle manufacturers, vehicle connectivity system hardware importers, and other interested parties can seek interpretive guidance from BIS on its implementation and application of the rule, based not only on actual transactions but also on prospective or hypothetical transactions.

- Due Diligence: We appreciate that BIS is not proposing specific due diligence requirements and is instead planning to provide flexibility to connected vehicle manufacturers and vehicle connectivity system hardware importers to develop and implement due diligence efforts that are tailored to their unique operations. We note that, although BIS states in the NPRM that such due diligence efforts "could include using third-party researchers," the proposed regulatory text appears to require the use of such third-party researchers. We agree that the use of third-party researchers should be an option, but not a requirement. To align with BIS's

intent, we propose that the regulatory text related to due diligence in section 791.305 be modified as follows:

> "Documentation of the [VCS hardware importer's] [connected vehicle manufacturer's] due diligence efforts, which may include independent or hired third-party research…"

- Recordkeeping Requirements: The NPRM proposes to require connected vehicle manufacturers and vehicle connectivity system hardware importers to maintain "complete records related to any transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required." The NPRM notes that such records would include "all 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." The NPRM further specifies that such records should be available for at least 10 years after the transaction.

  We understand that the 10-year recordkeeping requirement aligns with recent amendments to the *International Emergency Economic Powers Act* to extend from 5 years to 10 years the statute of limitations for civil and criminal violations. As this expansive recordkeeping obligation for all relevant transactions will likely present significant practical and financial burdens on connected vehicle manufacturers and vehicle connectivity system hardware importers, we urge BIS to narrow the scope of items that must be maintained. For example, BIS could specify that entities maintain:

  > "all primary business records related to the execution of the transaction, such as contracts, import records, bills of sale, essential correspondence, and all other files specified in sections 791.312 and 791.313 to assess compliance with the rule"

- Declarations of Conformity: The NPRM proposes that, in the event of a material change that impacts the content of a Declaration of Conformity, connected vehicle manufacturers and vehicle connectivity system hardware importers would be required to submit an updated Declaration of Conformity within 30 days of such a change.

  We recommend that BIS provide some additional clarification as to what constitutes a material change with respect to the Declaration of Conformity. For example, it is not clear from the NPRM what specific changes to covered software would be considered by BIS to constitute a material change subject to an updated Declaration of Conformity. In addition, the NPRM notes that a vehicle connectivity system hardware importer is only required to submit the make, model, and trim of the completed connected vehicle for which the vehicle connectivity system hardware is intended if the make, model, and trim are known. It is not clear whether a subsequent decision to integrate the vehicle connectivity system hardware into a particular vehicle make, model, and trim would be considered by BIS to be a material change. It would be helpful if BIS could provide a definition and some illustrative examples of material changes to support industry compliance.

To ensure that connected vehicle manufacturers and vehicle connectivity system hardware importers have sufficient time to develop, verify, and submit such updates, we also recommend that the deadline for submission of an updated Declaration of Conformity be 60 days, rather than 30 days.

We further suggest that BIS conform the obligation to submit material changes to Declarations of Conformity with the recordkeeping timelines implemented elsewhere in the NPRM. In other words, connected vehicle manufacturers and Vehicle Connectivity System hardware importers should be under an obligation to update Declarations of Conformity any time there is a material change but only for 10 years after the time the initial Declaration of Conformity is filed.

In addition, BIS should consider clarifying in the NPRM that connected vehicle manufacturers and vehicle connectivity system hardware importers are also permitted to submit amended Declarations of Conformity should a connected vehicle manufacturer or vehicle connectivity system hardware importer discover an error, omission, or other issue with a previously-submitted Declaration of Conformity. BIS could specify that an amended Declaration of Conformity must be submitted by the connected vehicle manufacturer or the vehicle connectivity system hardware importer within 30 days of discovering the error, omission, or other issue.

Finally, the NPRM proposes to require vehicle connectivity system hardware importers to include a "list of third-party external endpoints to which the VCS hardware connects" as part of their Declaration of Conformity. To provide further clarity, BIS should consider providing a plain definition or explanation of what it intends by the term "endpoint."

- Appeals Process: In the NPRM, BIS proposes to create a mechanism by which, among other things, any person whose application for a specific authorization is denied may appeal that decision to the Under Secretary. The NPRM lays out some specifics related to the appeals process, including timelines under which the appeal must be submitted, some direction as to the details that must be provided by the appealing party, and the procedures for an informal hearing. We urge BIS to provide a more detailed framework for the appeals process, including information on how a software supplier can engage or participate if its software is the subject of an appeal by a connected vehicle manufacturer.

- Exports: The NPRM's proposed prohibition on the import of certain vehicle connectivity system hardware is seemingly intended to apply only to vehicle connectivity system hardware that will be integrated into a vehicle for the U.S. market. Similarly, the NPRM's proposed prohibition on the import of connected vehicles containing covered software appears to apply only to vehicles that are intended for the U.S. market. In other words, it is our understanding that the proposed rule would not in any way restrict exports of vehicle connectivity system hardware or connected vehicles from the U.S. to foreign markets. To ensure alignment between BIS and industry on this point, we recommend that the final rule explicitly clarify

that the import of vehicle connectivity hardware for incorporation into connected vehicles for export to a foreign market and the integration of covered software into a connected vehicle assembled in the U.S. for export to another market are not prohibited.

We appreciate your consideration of these recommendations. We welcome the opportunity to engage further with you and provide additional industry perspective and expertise on this consequential and precedential rulemaking.

Sincerely,

Hilary M. Cain
Senior Vice President, Policy