The Vehicle Suppliers Association

Comments of

MEMA, The Vehicle Suppliers Association

to the

Bureau of Industry and Security, U.S. Department of Commerce

on the

Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

Notice of Proposed Rulemaking

Docket No. 240227-0060

BIS-2024-0005

October 28, 2024

Introduction

MEMA welcomes the opportunity to respond to the Bureau of Industry and Security's (BIS) Notice of Proposed Rulemaking (NPRM) on "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles."

MEMA, The Vehicle Suppliers Association, is the leading trade association in North America for vehicle suppliers, parts manufacturers, and remanufacturers. It has been the voice of the vehicle supplier industry since 1904. Automotive and commercial vehicle suppliers represent the largest sector of manufacturing jobs in the United States (U.S.), employing over 900,000 people across the country. Direct, indirect, and induced vehicle supplier employment accounts for over 4.8 million U.S. jobs and contributes 2.5 percent to U.S. GDP. MEMA members operate facilities in all 50 states and in more than 300 Congressional districts, with significant concentrations in the Midwest and Southeast.

Suppliers lead the way in new vehicle innovations. Member companies conceive, design, and manufacture the Original Equipment (OE) systems and technologies that make up two-thirds of the value of every new vehicle and supply the automotive aftermarket with the parts that keep millions of vehicles on the road, fueling international commerce and meeting society's transportation needs. Across the entire supply chain, MEMA members are committed to safety and sustainability.

Background and Perspective on Key Issues in the NPRM

MEMA appreciates the opportunity to offer its perspective on the critical issues raised in the NPRM and to present its thoughts as to how this rulemaking may significantly impact the supplier sector. The association, and the industry at large, supports the efforts of BIS to safeguard U.S. citizens, domestic infrastructure and the national interest.

MEMA wishes to acknowledge the notable efforts of the BIS staff in preparing this NPRM and the agency's willingness to consider and reflect upon the points that were raised in response to the February 2024 Advance Notice of Proposed Rulemaking (ANPRM). In its response to the ANPRM, MEMA voiced its concerns that the scope of the rule was too broad and that it would encompass a number of technologies that were not linked to the key areas of perceived risk. Many stakeholders echoed these concerns, arguing that technologies such as Advanced Driver Assistance Systems (ADAS) and Battery Management Systems (BMS) should be removed from the rulemaking. Moreover, MEMA requested that BIS address the proposed definitions in the ANPRM in order to make them more finite and usable for the industry. Finally, MEMA urged BIS to include specific examples which could help to illustrate the requirements for suppliers and other entities within the industry. MEMA expresses its appreciation for the attention given to each of these concerns.

As noted in the association's formal May 2024 comments, MEMA supports the efforts of BIS to ensure U.S. national security and to implement the directives of Executive Order 13873[1]. We believe that BIS has invested considerable time to amend the rule and to attempt to narrow the scope of the components and systems affected. After an extensive review of the NPRM with its members, MEMA wishes to raise several additional concerns and points for BIS' consideration. They are grouped into the following categories:

Definitions: MEMA does not oppose the identification of "Vehicle Connectivity System (VCS) hardware and covered software" as being the focus of the rule. However, there is a need to provide additional clarity in the definitions of the VCS hardware and covered software. The lack of precision in terms may inadvertently lead to the inclusion of technologies which BIS does not intend to be targeting. Further, there are certain portions of the NPRM in which the text does not align with the stated intent of the rule. Finally, MEMA urges explanation or alignment in certain sections as to the intended meaning of the term "persons."

Compliance Timeline: As MEMA shared in its comments to the ANPRM, MEMA requests that BIS provide additional time for the supplier community to analyze the full impacts and plan for alternatives or other avenues to ensure compliance with the new requirements outlined in the NPRM. The timing envisioned in the proposal would pose steep challenges for the industry, particularly as many entities are already deeply ensconced within the negotiations and planning associated with production platforms for Model Year (MY) 2027.

As highlighted in the association's prior submission, companies' supply chains for highly technical modern vehicles require access to a multitude and diversity of sourcing for the necessary materials, subcomponents, and technologies at the required volumes and quality levels in order to remain globally competitive. The due diligence requirement to indirectly vet the full supply chain for covered hardware and software for the purposes of ascertaining potential control by a foreign adversary and ensuring no prohibited transaction exists, as well as the ongoing maintenance of that knowledge, is unprecedented in the automotive industry.

[1] https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

Compliance with the NPRM will take time as outlined in greater detail below. Suppliers will likely need to identify and validate new suppliers in order to ensure competency for delivery as well as the ability to meet industry and Tier One suppliers' standards.

A disruption of supply chains would have a significant impact on the industry and potentially bifurcate product development plans; thereby disrupting U.S. innovation contributions to the auto industry.

Compulsory Submission of Business Proprietary Information in the Form of HBOMs and SBOMs: MEMA and its member companies have strongly conveyed their collective opposition to the proposed requirement that Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM) be surrendered to BIS as part of the submission of a Declaration of Conformity (DOC). Based on the text of the NPRM, there would also be a similar requirement for suppliers to provide such proprietary information to the vehicle manufacturers to support the creation of the vehicle manufacturer's own DOC. MEMA contends that HBOMs and SBOMs are highly confidential and business critical information. HBOMs and SBOMs encompass much of the intellectual property and company-specific data which enable the innovation propelled by the supplier industry. This information is a foundational element of U.S. competitiveness.

At this time, it is not industry practice for suppliers to share such in-depth information with their customers as is proposed by the rule. A government requirement to compel the sharing of this information would not only leave suppliers vulnerable to severe competitive and business risks, but also increase risk to the industry and national security at large by the creation of a central repository of this critical information.

Confidentiality Protections: MEMA urges BIS to provide additional details as to how the agency would protect the information provided through (1) a Declaration of Conformity and/or (2) an application for an Authorization. Suppliers wish to receive greater assurance that this data will be held in a manner that does not risk exposure to business competitors or other outside interests through methodologies such as a Freedom of Information Act (FOIA) request.

Moreover, MEMA urges BIS to consider adopting protocols that are already in use by the Department of Commerce[2], which specifically minimize the amount of data to be collected (restraining it to focus solely on the specific data needed to provide the assurance of compliance), and then to delete the data after the requisite assessment is completed. MEMA and its member companies also urge consideration of how each of the distinct VCS hardware importers, suppliers, and connected vehicle manufacturers can retain separation to ensure compliance with antitrust and confidentiality provisions as part of the compliance with the proposed rule.

[2] IT Privacy Policy, Office of Privacy and Open Government, U.S. Department of Commerce – https://www.commerce.gov/opog/it-privacy-policy-office-privacy-and-open-government-us-department-commerce#P38_3503

MEMA Response to Selective Provisions in the NPRM

Definitions:

MEMA appreciates the agency's careful consideration of the comments that many entities provided to the docket in May and for the agency's own investigations into this topic.

The association, however, urges BIS to further refine select segments of the new definitions.

Definition of Software

Several member companies have indicated that the current definition of Automated Driving System could, unintentionally, capture elements of systems which are designated as SAE Level 2 or SAE Level 2 Plus. A review of the complete NPRM yields evidence that BIS does not intend to include SAE Levels 0-2; however, the current definition does not make this clear.

For example, MEMA wishes to highlight Automated Parking Systems which are considered to be a Level 2 technology under SAE J3016[3] because this technology is under the control of the driver. The rule defines ADS 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 accompanying discussion further clarifies that "this definition corresponds to automation Levels 3, 4, and 5 as defined by SAE Internation standard J3016." A system that performs automated parking but does not perform the rest of the "entire dynamic driving task" would not fall within the definition because the system is not performing the entire dynamic driving task. Indeed, SAE J3016 uses automated parking as an example of maneuver-based features in a Level 1 or 2 system in which a driver performs other elements of the dynamic driving task and therefore the system does not meet Level 3. For example, definition 3.7.1 includes as an example of a maneuver-based feature "a Level 2 parking assistance feature [that] automatically performs the lateral and longitudinal vehicle motion control actions necessary to parallel park to a vehicle under the supervision of the driver." An automated parking system where the driver is outside of the vehicle, but still ultimately responsible for supervising the system through the use of an app is still an L2 feature.

Further, there is concern that the definition of software as proposed in the NPRM could still result in an overly broad scope and cascade down into the lower levels of ADAS. For example, companies have inquired if BIS' intent would be to include any type of software that contains or contributes to road object detection even though the actual software does not issue connect requests to the backend. MEMA urges BIS to insert additional clarity into the definition by specifying that underlying ADAS hardware and software that enables SAE Level 2 and SAE Level 2 Plus levels of automation as well as SAE Level 0-2 technologies are excluded from the rule.

Suppliers across the board have noted that software and hardware are developed by global teams. Concerning the software definition and relevant restrictions, MEMA urges BIS to provide additional guidance on what specific actions and aspects of product development are restricted. MEMA asks BIS to address this concern to a deeper degree. For example, would the restrictions be applicable to

[3] J3016_202104: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International

a single line of code associated with a covered software package or should there be a different arbiter used as an appropriate threshold?

MEMA recommends that the scope of the software definition be refined to include the full software product that enables the function of VCS or ADS at the "vehicle level", but not sub-elements of software. The association further recommends that open source technologies be defined as broadly as possible and with a scope inclusive of state of the art software solutions. The agency should adopt a definition of covered software that excludes the software contained in systems that are subordinate to the ADS. Subordinate systems are defined as those systems that are present in a vehicle regardless of ADS, e.g. powertrain, steering, and braking systems. As stated above, software can often be created by workforce teams made up of individuals from around the world which are involved in the design, development, manufacture, or supply (DDMoS) to create an automotive component or product. Under the proposed rule, some software may be deemed a prohibited transaction by BIS because it originated from a foreign adversary or its DDMoS was partially supported by an individual or entity that is owned by, controlled by, or subject to the direction of a foreign adversary, but not located within the territory of China or Russia. Software can also have significantly long development times.

Covered Software and Prohibited Transactions

MEMA is supportive of the aims and goals BIS has in ensuring that software is safe and secure and protective of national security. In the scenario that a portion of source code or module renders the complete software package a prohibited transaction, industry proposes that BIS establish a set of processes and procedures to create a clear pathway to remedy the classification of "prohibited."

MEMA proposes that such processes and procedures provide clarity on the degree and type of remedy necessary for the software to no longer be deemed a prohibited transaction on import or when a completed connected vehicle is imported.

To this end, the industry recommends that BIS consider integrating accepted international regulatory standards to drive its guidance for industry. For example, BIS could leverage the following proposal:

The ISO/SAE 21434 Road Vehicles-Cybersecurity Engineering Threat Analysis and Risk Assessment (TARA) standard is used to assess the cybersecurity risks in a product. This standard provides a methodology for the software developer to identify critical assets and privacy concerns. This allows for the greatest specificity to address the critical asset(s), i.e. the specific lines of source code or module, at issue, rather than broadly including all software packages.

Further, software modules that do not manage connected vehicle communications or ADS assets would not be considered prohibited transactions. The software modules that do manage critical assets would not be considered prohibited transactions pending a system review by a team not located in or under the influence or control of the PRC or Russia. The process to remedy this situation would include an evaluation of the source code, along with the removal and recoding of any questionable sections, to certify the software product's compliance with the final rule. Such a process could be added as an attestation by the software developer or manufacturer to the Declaration of Conformity. Industry would, therefore, have the ability to utilize code in which development investments were already made and provide a pathway for that code to be certified as compliant. This approach would further recognize the long development cycles and significant

investments associated with new technologies while also ensuring the protection of national security interests.

Definition of VCS Hardware

MEMA submits that the definition of VCS Hardware is too broad, potentially requiring importers to submit HBOMs not only for imported components but also for subcomponents that may not be available or attainable.

MEMA recommends that BIS delete the term "subcomponent" in the VCS hardware definition (and in related portions of the proposed regulation such as 791.305(a)(iii)) as follows; MEMA also recommends that BIS provide additional examples of excluded passive electronics.

VCS hardware includes the following software-enabled or programmable components and subcomponents that support Vehicle Connectivity Systems or are part of items that do so:

- Microcontrollers
- Microcomputers or modules
- Systems on a chip
- Networking or telematics units
- Cellular modules
- Wi-Fi microcontrollers or modules
- Bluetooth microcontrollers or modules
- Satellite navigation systems
- Satellite communication systems
- Other wireless communication microcontrollers or modules
- External antennas
- Digital Signal Processors (DSPs).
- Field-Programmable Gate Arrays (FPGAs)

Alternatively, VCS hardware does not include components that do not aid in its communication function. This includes items like brackets, fasteners, plastics, passive electronics, diodes, FETs, and BJTs.

If BIS cannot remove "and subcomponents" from the definition of VCS hardware, MEMA recommends adopting a version of the "second incorporation principle" from the Export Administration Regulations (EAR) for de minimis calculations.

The EAR applies to foreign-made items with more than a de minimis amount of U.S.-origin controlled content. Under the "second incorporation principle," U.S. origin subcomponents incorporated into a foreign-made discrete product are not counted in de minimis calculations if that product is later included in another foreign-made item. This principle aims to reduce the burden on purchasers of foreign products, who often cannot determine the U.S. content in those items.

As long as the foreign-made item is considered a "discrete product"—meaning it is purchased at arm's length or sold on its own—the buyer is not required to investigate the U.S. origin of the foreign-made item's components.

MEMA proposes that BIS exclude "discrete" subcomponents from the definition of VCS hardware, as long as these subcomponents are not of Chinese or Russian origin. This proposal strikes a balance

by requiring VCS Hardware Importers to report in their HBOMs subcomponents that are sourced from China or Russia, as well as any subcomponents they have designed themselves, which allows them to access the necessary HBOM information. At the same time, the proposal exempts subcomponents that are commonly sold on their own and purchased at arm's length. This exemption recognizes that VCS Hardware Importers may not be able to obtain HBOM information for these subcomponents from the seller.

MEMA also recommends that the definition be further refined to cover only hardware that is directly connected to the "communication function," but not related to the basic electronics hardware such as processors, capacitors, etc.

MEMA urges BIS to (1) clarify that products that do not connect to the network outside the vehicle (products that connect indirectly/products that communicate only with smartphones via Wi-Fi communication) are not subject to the rule and (2) to specify that component parts which do not contribute to the communication function are excluded from the definition. BIS should further exclude functions with fixed communication partners (such as an OEM's server). BIS should specify that satellite radio (XM, Sirius, etc.) hardware and software are not included in the scope if the rule.

MEMA requests that BIS confirm that the rule is not intended to capture tethered devices (such as diagnostic tools and electric vehicle supply equipment (EVSE) (EV chargers)) which may be connected to the vehicle for a designated period of time in order to assist with vehicle diagnosis and repair or charging.

MEMA requests that BIS further provide affirmative confirmation that the definition excludes low risk items and passive components such as PCBs (bare boards) and parts of microcomputers and other semiconductors that are not directly related to communication functions, such as packages, and assembly (post-process) of semiconductor packages.

In the NPRM, BIS expresses its opinion that the proposed definition of a "vehicle connectivity systems" would exempt most remote keyless entry fobs and immobilizers and certain internal wireless sensors and relays. However, MEMA members have noted that there is communication above 450 MHz which it is presumed that BIS did not intend to cover in this rule (such as ultrawideband (UWB)-enabled key fobs using above 6 GHz spectrum, Bluetooth-enabled key fobs using between 2.4 and 2.48 GHz spectrum, and automotive radar using 77 GHz spectrum). Therefore, MEMA recommends that BIS exclude them from the definition.

Please see below for an alternative proposed definition for VCS Hardware.

Proposed Definition:

VCS hardware includes software-enabled or programmable components that support and are directly connected to the communication function in Vehicle Connectivity Systems, such as:

- Microcontrollers
- Microcomputers or modules
- Systems on a chip
- Networking or telematics units
- Cellular modules
- Wi-Fi microcontrollers or modules
- Bluetooth microcontrollers or modules

- Satellite navigation systems
- Satellite communication systems
- Other wireless communication microcontrollers or modules
- External antennas
- Digital Signal Processors (DSPs).
- Field-Programmable Gate Arrays (FPGAs)

VCS hardware does not include parts that do not contribute to and are not directly connected its communication function, such as brackets, fasteners, plastics, keyless entry fobs and immobilizers and certain internal wireless sensors and relays, satellite radio (XM, Sirius, etc.) hardware and software, tethered devices (such as diagnostic tools and electric vehicle supply equipment (EVSE) (EV chargers)), and passive electronics (PCBs (bare boards) and parts of microcomputers and other semiconductors that are not directly related to communication functions, such as packages, and assembly (post-process) of semiconductor packages). Additionally, VCS hardware excludes discrete subcomponents that are purchased at arm's length or are regularly sold on their own, provided they are not of Chinese or Russian origin.

End Proposed Definition

Legacy Software and Hardware:

MEMA respectfully requests that BIS provide an exemption for legacy code developed before the date that the rule goes into effect. In these instances, the code that is in place may be several years old with code for the most recent application building on years of earlier code. It is difficult to attribute a line of code to a specific individual or entity. The process for developing code is iterative, which increases the challenge to conduct due diligence in legacy cases.

MEMA further requests that BIS consider extending select exclusions for legacy hardware that has already been widely produced and installed on vehicles in use in the U.S. For more than ten years, connected vehicles systems have been integrated into vehicles that are currently on the road. As noted above in the section of the comments pertaining to software, it is difficult to backtrack these widely deployed technologies particularly in light of the complexities and intricacies of the automotive supply chain.

Transition Timeline:

MEMA respectfully requests that BIS provide an additional two years of transition for the enforcement of the software stipulations in the regulation and an additional year for the mandates related to hardware.

Suppliers are already deeply engaged in quoting and planning vehicle projects with customers for Model Year (MY 2027). The industry appreciates and understands the desire of the Administration to speed implementation of the rule. However, the very nature of the industry and its due diligence responsibilities relative to the production of safety-critical products makes the proposed timelines prohibitively challenging. Suppliers have noted that dramatic and last-minute changes to the supply chains and the sub-suppliers already selected for such products could pose a safety risk and create a significant challenge and burden for companies. Consequently, we strongly urge BIS to consider providing sufficient additional time for the industry to adjust to these new stipulations and to identify and validate new sub-suppliers.

With respect to software in particular, any time a manufacturer needs to obtain a new source of input (in this case all or some portion of a software code) the new software developer and its corresponding code will need to undergo additional software testing and validation to ensure that it effectively and reliably supports its intended function within the vehicle. While this is important in all cases, it is particularly important for critical safety technologies including those defined as SAE Levels 3-5. These products need to be validated over time before they reach the market to ensure they can safely protect the consumer who purchases them, the drivers using them, as well as pedestrians or other road users.

The design and development of in-vehicle software is also unique compared to many other applications in that each engineer needs to understand how the software that they are in charge of interacts with related components and software in the finished vehicle, and then implement that component feature in line with standards used in the automotive industry and/or those required by federal or state regulators. Even in the event a manufacturer can localize its software development "in-house" in the U.S. or another ally nation, this testing, validation, and certification phase alone can take multiple years.

Moreover, there is a shared interest in working with the agency through the proposed advisory process, but this would necessitate sufficient time for this process to be stood up and made available to the industry.

MEMA has provided an example below to illustrate the minimum five-year timeline that is normally required for a supplier to bid on, acquire, create the requisite supply chain plan for, validate and eventually commence production for a vehicle platform with a customer. In the area of emerging technologies, Tier One or Tier Two suppliers may face an even greater hurdle as the number of sub-suppliers or materials companies that can provide the related item may be small. As noted in MEMA's prior submission, timing represents a particularly critical issue for the mobility sector as sourcing arrangements may last six to seven years on average. Uncertainty and the loss of supply sources could put companies in a position of missing certain windows of business opportunity.

Example for Reference:

Year One – Vehicle manufacturers (OEM) begin the supplier selection process and issue a request for quote (RFQ). Suppliers review and assess the specifications and the design concept definitions provided by the OEM. Suppliers provide a bid with the requisite cost estimate and outline for development and eventual production for the particular vehicle platform.

Year Two – Supplier receives bid and confirmation of the related business from the OEM. Development work commences together with the design validation and testing for the associated initial HW and SW releases.

Year Three – Supplier commences extensive validation process to (1) identify requisite sub-suppliers and confirm sourcing (at the necessary volume and quality levels) and (2) ensure compliance with industry, customer and supplier vendor standards for materials and safety.

Year Four – Supplier finalizes the contracts and sets the timeline for the production lines in its facilities. Supplier commences technology validation testing, certifications and homologation processes as required by other federal agencies responsible for certifying and homologating the device. The supplier acquires various certifications related to the product: in the example of a

telematic unit this would also include carrier authentication and Federal Communication Commission (FCC) certification. In the case of other components, such as multi-media Wi-Fi and Bluetooth-enabled products, FCC certification is still required. This overall validation process traditionally involves several months of coordinated effort as a prototype vehicle (with the technology installed) is driven in multiple jurisdictions, exposed to environmental variables, (severe weather, extreme temperatures etc.), and a range of driving conditions. The associated test data is subsequently compiled and reviewed.

Year Five – Product validation process is completed. Supplier completes all internal mandates and provides final release of the software and/or hardware. Start of Production date is confirmed for ramp up and delivery to the customer.

If there are unforeseen defects, vulnerabilities, or specification changes made during the project test and integration phase (including design, testing, and integration processes) the lead time for a project may need to be adjusted to allow for countermeasures to be implemented by either a vehicle supplier or OEM.

Depending on the specific circumstance, such as the aggressive timeline for software phase out proposed in the NPRM, an impacted supplier may be required to find alternative software suppliers. The impacted supplier will likely need to provide requisite training to the alternative software suppliers for the development of VCS software. It is estimated to take 18-24 months for an impacted supplier to 1) hire/contract with and 2) train an alternative software supplier(s), given the growing global demand for in-vehicle software development personnel, and the competitive market for qualified personnel due to the somewhat unique nature of in-vehicle software development.

In addition to the potential challenges of re-sourcing to an alternative software supplier, additional time would be required to integrate any new code into the existing software, including making any necessary modifications to ensure compatibility. In this case, the supplier would need to restart the project test and integration phase as described above to evaluate the amended software in its entirety for factors including safety, customer specification, and regulatory compliance requirements. Modifications to existing software will also require new applications for the required licenses and certifications for the product. In such a scenario, the licensing/certification process could take an additional 18-24 months, in addition to what is outlined in the previous paragraph and excluding any additional time a connected vehicle manufacturer may need to conduct their own evaluation.

Therefore, a minimum of 3-5 years would be required to adequately address the proposed requirements. It is anticipated that there could also be variations in the model timelines outlined above due to factors beyond the suppliers' control.

Based on the timeline articulated above, MEMA strongly urges BIS to provide sufficient flexibility to the industry. MEMA requests that mandatory compliance not be imposed until January 1, 2030 for VCS hardware and until Model Year 2029 for covered software. However, as documented throughout this section, even a modest extension to MY2029 for software compliance may still be a challenge for select manufacturers in some instances.

Declarations of Conformity and Submission of HBOM and SBOM:

As highlighted in the opening section of the document, MEMA and the supplier community are strongly opposed to the compulsory surrender of confidential business information in the form of a mandated attachment of an SBOM and/or HBOM as part of the DOC. It is not industry practice for this information to be shared between suppliers and customers, considering the notable risks that the dissemination of this information poses to corporate intellectual property, and the overall responsibility for safety of the U.S. motoring public who are consumers of the automotive industry.

The issue of SBOM and HBOM-sharing amongst suppliers and vehicle manufacturers is not a new topic. Suppliers and vehicle manufacturers have been engaged in an active dialogue surrounding these concerns for several years, both within the parameters of the

Automotive-ISAC (Information Sharing and Analysis Center)[4] and with government agencies such as the National Institute for Standards and Technology (NIST) and the Department of Homeland Security / Cybersecurity and Infrastructure Security Agency (DHS/CISA). As explained in MEMA's prior submission, the Auto-ISAC was formed in 2015 and currently encompasses more than 70 member companies. This forum, comprised of OEMs and suppliers, "provides a unique global information sharing community to promote vehicle cybersecurity. Auto-ISAC operates as a central hub for sharing, tracking and analyzing intelligence about potential cyber threats, vulnerabilities and incidents related to the connected vehicle." One of the most important tenants of Auto-ISAC is sharing, at times, sensitive information between its member organizations. The Auto-ISAC creates a third, "protected" space where critical information can be communicated across the ecosystem. To date, Auto-ISAC has prepared and released several Best Practices guides for the industry in order to remain abreast of strategic developments.

It is MEMA's understanding that the Auto-ISAC has been working on an informational report on SBOMs. This report outlines best practices for how this information would be shared between different partners within the larger automotive industry. This document reflects several years of work between OEMs and suppliers to identify a viable solution.

MEMA is also concerned that the disclosure of SBOM and HBOM information places industry at a competitive disadvantage as it would reveal trade secret and intellectual property information to the government and to customers, facilitating deep analyses of specific products and a specific company's supply chain. The competitive risks associated with such a disclosure cannot be overemphasized. MEMA views this proposal as one that could yield notable damage to suppliers' proprietary information and technologies and to their respective positions in the market. MEMA has further shared concerns that such actions could undermine a company's investment into research and development activities. Vehicle manufacturers select and make awards to suppliers based on the supplier's unique ability to meet the industry and customer's design specifications while maintaining high standards for design and production. Currently, suppliers provide customers with attestations that are used to ensure compliance with industry and regulatory requirements or to assist customers with other mandates such as those under the U.S.-Mexico-Canada (USMCA) agreement. Suppliers do not provide their vehicle manufacturer customers with a list of suppliers and sub suppliers due to the intellectual property involved. Again, MEMA

[4] Automotive ISAC

emphasizes that this requirement would go counter to standard industry practice and leave suppliers to face several unsustainable risks.

Congruently, requiring connected vehicle manufacturers to provide a DOC including HBOMs and SBOMs should not serve as a proxy for obtaining the HBOMs and SBOMs from VCS hardware and software suppliers. For this scenario, MEMA strongly recommends that the attestation (please see below) from the supplier serve as the vehicle for ascertaining compliance from the supplier toward the connected vehicle manufacturer. Such a process would support national security while concurrently protecting the innovation, investments, and supply chain of the automotive industry.

Instead, MEMA respectfully requests that suppliers be permitted to provide a signed attestation by a representative with approval authority from a VCS hardware importer or connected vehicle manufacturer which confirms the company and the specific product's compliance with the specifics of the regulation. The entity in question would also provide a high-level "summary" of the relevant HBOM or SBOM which includes a few key elements of information, such as:

- Company Name of Entity Providing the Declaration of Conformity
- Product Name
- Customer
- Signed Attestation: No knowledge of foreign adversary relationship

Suppliers would subsequently maintain records as necessary to document compliance with the BIS Final Rule. Further, the supplier would provide additional data on a specific HBOM or SBOM to BIS upon request or in the case of a situation such as a compliance audit. MEMA recommends that the government then delete the SBOM and HBOM data once the audit or investigation is resolved. This protocol would mirror the methodology used by the European Union in the case of the General Data Protection Regulation (GDPR)[5] as well as the data procedures that are utilized as best practices by the Federal Trade Commission (FTC) and the Department of Commerce itself[6].

MEMA further highlights the concern that the concentration of this high volume of HBOM and SBOM information in a database could pose a heightened risk to industry, and to vehicle and driver safety if a leak or a cyber-attack were to occur in the future. The release of this information could provide a perfect roadmap for other entities to fraudulently copy select technologies and products or for a malignant entity to create an effective plan of attack as they would gain knowledge as to which specific OEMs have certain products and/or software on select vehicle platforms. If this database were ever compromised, it could also provide a potential roadmap for nefarious actors of where they might focus their attention to compromise vehicles on the road.

MEMA also wishes to address an additional point concerning the submission of the DOC. In the NPRM, BIS proposes to require the submission of the DOC on an annual basis or "whenever there is a material change." MEMA urges BIS to recast the stated proposal as this could impose an enormous burden on suppliers and their customers. Changes to covered software and hardware may occur on a frequent basis and may not be of a sufficiently critical nature to trigger a new report to the

[5] Art. 5 GDPR - Principles relating to processing of personal data - GDPR.eu

[6] IT Privacy Policy, Office of Privacy and Open Government, U.S. Department of Commerce – https://www.commerce.gov/opog/it-privacy-policy-office-privacy-and-open-government-us-department-commerce#P38_3503

government. MEMA urges BIS to amend the rule so as to confirm that (1) the DOC is due only on an annual basis from a VCS hardware importer and a connected vehicle manufacturer and (2) that a supplemental report is only required if a material change has now rendered the entity to be out of compliance with the regulation.

Over the Air Updates

MEMA also requests additional clarity as to how BIS would view an Over the Air Update (OTA) to a piece of covered hardware or software. OTAs are increasingly common in the mobility sector and often provide a critical fix to address a cybersecurity risk or other issue on the vehicle. MEMA would emphasize that an OTA should not be deemed a material change unless it causes the final software or hardware to fall out of compliance with the regulation.

Software for connected vehicle applications is being updated on a constant basis, and it is unclear how BIS would address the timing for reporting on required over-the-air update transactions designed to address safety concerns including patches to address cybersecurity risks or threats and energy management issues. MEMA strongly recommends BIS allow the importation and deployments of Firmware Over the Air (FOTA) or Software Over the Air (SOTA) updates as soon as the Declaration of Conformity has been submitted to BIS. MEMA requests that BIS clarify the process for reporting and approval and the timelines for different cases including:

1. Pre-production
2. Running change in production
3. Recall in the field
4. OTA update in the field to address a safety concern

While not exhaustive in all possible cases, BIS should at minimum address these four that are common types. Each of these may have different timing expectations. Under worst-case scenarios, such as recall in the field, it may not be safe to use a vehicle until the update is successfully introduced. For the safety critical or security critical updates, excessive delays waiting for review and approval could have a negative impact on customers and potentially other businesses who depend on a robust transportation support network.

Recognition of Investments and Production in Ally Countries:

MEMA has interpreted the specifications surrounding the DOC as requiring the filing of the documentation by the hardware importer or the connected vehicle manufacturer unless 100% of the covered hardware or software is created within the United States. The association urges BIS to consider providing a broader exclusion that would provide an exemption if 100% of the covered hardware or software is designed, developed, manufactured, or supplied by entities within the U.S. or its key ally nations. Such a list would include countries such as Brazil, Canada, India, Mexico, Japan, Malaysia, South Korea, Switzerland, Thailand, Vietnam, nations within the European Union, and NATO nations. This approach would align with the Administration's focus on strengthening relationships with key nations that have long-held connections with the U.S. and on friend-shoring as a means to reduce critical dependencies on foreign nations of concern.

MEMA urges BIS to consider the tremendous administrative burdens that the proposed requirements would impose on suppliers. Under the proposal, companies would need to investigate

their entire supply chain to ensure compliance. This includes verifying the involvement of third-party suppliers and conducting thorough screening of contractors. Given the broad definition of, and disclosure requirements for a "foreign interest," companies may need to implement additional supply chain controls to mitigate the risk of unknowingly violating the rule and would need to disclose significant information about their supply chains even if there is absolutely no involvement from the PRC or Russia.

Confidentiality Protections:

MEMA urges BIS to consider utilizing federal government accepted frameworks to protect against the release of confidential information. MEMA has referenced the existing processes used by other federal government agencies that have been successful in enabling the protection for the sharing of highly sensitive, Confidential Business Information (CBI) while still supporting regulatory goals and a competitive marketplace. Industry strongly recommends that BIS align and exchange information with the Department of Homeland Security (DHS), Customs Border Protection (CBP), the Environmental Protection Agency (EPA), and other relevant agencies on best practices concerning information sharing, data protection, and preventing duplicative burdens across government and industry.

These protocols have generally been utilized by industry, have proven their protective capabilities, and allow compliance with the various regulatory agencies in the U.S.

Additional Issues of Concern:

MEMA welcomed the examples and real-world scenarios included in the NPRM. The industry is grateful for the guidance articulated through these examples and for BIS' recognition of the multiple and complex scenarios that a company may encounter.

Concerning Example 19, MEMA appreciates BIS' clarification that it does not intend that an employee's nationality would form the *sole* basis for a determination, but there is a lack of clarity about what is "controlled by" or other aspects of an employee's private relationships that may be part of the determination. For persons working on hardware or software-citizenship will not be the "sole" measurement, but that implies that it is *one* of the measurements.

Excerpt from the NPRM:

"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."

Inconsistencies in the Use of the Term "Persons" Throughout the NPRM

As an example of inconsistent use of the term "Persons" found throughout the NPRM, MEMA would like to highlight the following:

Definition of Connected Vehicle Manufacturer: Means "a U.S. person (1) manufacturing or assembling completed connected vehicles in the United States . . ." This suggests "person" includes corporate entities.

But the definition of "Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" includes "(3) 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" and "(4) Any corporation, partnership, association, or other organization with a principal place of business in headquartered in, or otherwise organized under the laws of a foreign adversary. . . ."

This suggests a difference between the use of the term "person" (subpart 3) and legal entity (subpart 4).

So, the proposal seems to be inconsistent in whether "person" means both natural persons and companies, or only natural persons.

This becomes important when looking at things like the definition of "foreign interest" - "any interest in property of any nature whatsoever whether direct or indirect, by a non-U.S. person." Presumably person here includes companies, but is not clear given how "person" is used elsewhere in the proposed rule. This ambiguity should be resolved.

Conclusion

MEMA appreciates the opportunity to share its concerns and feedback on this rulemaking with BIS. As articulated above, MEMA and the supplier community support the intent of the rulemaking and BIS' efforts to ensure U.S. national security. However, we urge the Administration to carefully consider aspects of the rule which could erode U.S. competitiveness and place suppliers in a position of great risk relative to their intellectual property and business confidential information.

MEMA reiterates its sincere interest in continuing to work with the agency as this proceeding moves forward and we are grateful for BIS' recognition of the points and thoughts articulated by the industry in the docket.

If you have any questions concerning this document, please do not hesitate to contact Ana Meuwissen at ameuwissen@mema.org or Bill Frymoyer at bfrymoyer@mema.org.