ITS AMERICA

October 28, 2024

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

RE: Docket Number BIS-2024-0005, Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

Dear Ms. Cannon:

As the nation's leading advocate for the technological modernization of our transportation system by focusing on advancing research, development, and deployment of intelligent transportation technology, the Intelligent Transportation Society of America (ITS America) is grateful for the opportunity to comment on the United States Department of Commerce's Notice of Proposed Rulemaking (NPRM) on "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles."

ITS America was founded in 1991 as an advisory council to the United States Department of Transportation (USDOT) on technology innovation and emerging transportation technologies. ITS America is the only organization in the country that represents all sectors – public, private, research and academia, – to advance transportation technology. Our membership includes state and city departments of transportation, transit agencies, metropolitan planning organizations, automotive manufacturers, technology companies, engineering firms, automotive suppliers, and research and academic universities. Our vision is one of a better future transformed by transportation technology and innovation. Safer. Greener. Smarter. For all.

Our work accelerates the deployment of technology that saves lives, promotes sustainability, and advances more efficient and equitable transportation of people and goods. Our members' work focuses on connected and automated vehicle technologies, smart and digital infrastructure, artificial intelligence, sustainable technologies like electric vehicles, and other technologies that support mobility, public transportation, and freight.

Our members are at the forefront of deploying innovative transportation solutions to solve longstanding transportation challenges within the United States. Many of these solutions are underpinned by connectivity in order to seamlessly exchange vital transportation data, alerts, and messages to improve safety, mobility, and sustainability within the transportation sector. These deployments frequently represent partnerships between the public sector and industry to deliver on critical transportation priorities for road users. Given the significant interface between these technologies and the traveling public, it is essential that the connectivity enabling these systems remain secure from hostile cyber

activities. ITS America members and the transportation industry are committed to following robust cybersecurity and privacy best practices and already do so in numerous circumstances, including strong adherence standards from the National Institute of Standards and Technology (NIST), the National Highway Traffic Safety Administration (NHTSA), SAE International, and other organizations.

We are grateful for the work of the Department of Commerce's ("Department") Bureau of Industry and Security ("BIS") on the issue of securing our transportation system, and we support the Department's goals in ensuring our national security and improving the resilience of the information and communications technology and services ("ICTS") and connected vehicle ("CV") supply chain. We share the goals of maintaining safe travel conditions, ensuring data privacy, and protecting our critical infrastructure.

ITS America previously filed comments on the Advanced Notice of Proposed Rulemaking [Docket No. 240227-0060] prior and is pleased to submit comments on this NPRM. We look forward to working together with the Department on how to structure regulations in a way that provides robust national security safeguards while simultaneously considering the nature of current vehicle supply chains, compliance feasibility, economic costs, and our country's transportation safety needs.

Timelines for Implementation

The automotive industry operates on long development timelines, often spanning three-to-seven years for new vehicle models. Designing, testing, and producing a vehicle is a complex, multi-phase process that requires significant time to ensure safety, performance, and regulatory compliance. Once a new platform is designed, changes to critical VCS systems would require additional rounds of design, testing, validation and certification. The NPRM exacerbates these timeline pressures because it forces OEMs to find alternative suppliers that can meet the proposed rule's vague requirements. As written, this NPRM will require most OEMs to identify new suppliers, renegotiate contracts, and potentially redesign software and hardware to meet the same performance specifications while ensuring compliance with the NPRM's overly broad restrictions. Given the specialized nature of automotive components which may perform critical motor vehicle safety functions, finding alternative suppliers that can meet high quality, safety, and regulatory standards takes time, even without the proposed restrictions.

In many cases, supply chains for automotive vehicle connectivity and automated driving systems' software and hardware are deeply integrated and have developed out of other technology designs, some of which have historical design roots in engineering from the PRC. For example, vehicle connectivity system (VCS) software and hardware are an extension of the global mobile technology industry, which derives its design from over thirty years of multiple global engineering inputs, including from the PRC. It would be impossible for most of today's VCS software and hardware suppliers to comply with the proposed NRPM as written because they cannot eradicate legacy software and hardware from historical proprietary Chinese engineering inputs integrated into the foundational technology of today's vehicle connectivity systems.

Considering this history, BIS must amend the proposed rule with clarification that legacy software code developed prior to the effective date of the final rule will not be subject to the prohibitions. Without this certainty, the prohibitions in the proposed rule will cascade through multiple tiers of automotive suppliers, heavily restricting, if not prohibiting, the U.S. auto industry from manufacturing and selling

connected vehicles in the United States.

Assuming new software and hardware suppliers without such legacy ties even can be identified, these new suppliers will need time to ensure their product can meet the rigorous requirements of their OEM customers. Likewise, automotive OEMs must go through rigorous testing and validation processes to ensure that the new components are compatible with their vehicle platforms. These processes are time-consuming, and any failures or defects discovered during testing would require redesigning and additional rounds of validation. For example, the 2027 model year deadline for removing covered software from CVs has already passed. Development of CV technologies for model year 2027 is underway or has already been delivered, and, depending on the complexity of the software, may have been underway for years. A new CV product takes about four to five years to develop from ideation to vehicle launch and sometimes longer. Decisions by manufacturers and suppliers about what technologies and features to pursue and which vendors to select must therefore occur at least four or five years before a particular model year vehicle is set to enter production. Furthermore, VCS and ADS features at the vehicle level are highly complex, involving extensive software integration. Ensuring that software and hardware replacements do not introduce or create vulnerabilities or degrade system performance will require careful validation, especially in safety-critical environments. Lastly, many OEMs operate on a global production scale, so a vehicle designed for one market often shares components with vehicles sold in other markets. Even if a vehicle's VCS or ADS components are intended for a U.S. model, it may require changes to other models globally.

Ensuring compliance across multiple production lines, countries, and regulatory regimes adds layers of complexity that can extend timelines for both hardware and software. The Department's proposed model year 2027 software deadline fails to adequately account for the integration of connected software and ADS technology already underway in many OEM development pipelines. Given that software updates and security patches are continuously deployed in modern vehicles, maintaining compliance without affecting development schedules adds similarly significant complexity relative to the hardware-specific concerns articulated above. To avoid substantial industry disruption, the proposed rule must extend the timeline to ensure the U.S. automotive industry has adequate time to transition from covered software. Specifically, ITS America recommends that the Department provide OEMs and VCS or ADS software suppliers until at least model year 2030 to comply with the NPRM's proposed software prohibitions and until at least model year 2033 or later to comply with the proposed hardware restrictions. As discussed above, the 2027 model year deadline for removing covered software from CVs has already passed. Additionally, ITS America recommends the Department either provide an express exclusion for legacy VCS and ADS software or construct the final rule to apply to applicable covered software designed on or after a future date.

Extending the deadline for software and hardware compliance and clarifying that legacy code is not subject to the prohibition are the critical issues for BIS to address in crafting any final rule. This will ensure industry can advance the Department's national security objectives while minimizing disruption to vehicle supply chains and the U.S. auto industry.

Declarations of Conformity

Given the importance of Declarations of Conformity as a mechanism for OEMs to comply with the requirements outlined in this NPRM, BIS must streamline, improve, and clarify the process associated

with these declarations. The Department should issue specific, detailed guidelines on the types of documentation that must be submitted with the Declaration of Conformity. ITS America recommends that BIS utilize NHTSA's Federal Motor Vehicle Safety Standards self-certification process as a model for how this conformity could be affirmed. Rather than broadly stating that OEMs must prove their vehicles have no prohibited components, the Department should outline specific categories of interest, including what they are looking to receive from supplier declarations and certificates of origin for VCS and ADS components. This should be done in tandem with creating a certification standard or trust mark for VCS hardware components and completed connected vehicles.

To best facilitate compliance without undue burden on industry, BIS should develop voluntary certification processes for VCS hardware suppliers to help streamline the process of compliance at the OEM level. We recognize the Department's decision to forgo a trusted trader program in this NPRM, however we urge the Department to consider a similar certification process for VCS component hardware to ease the burden of selecting suppliers and component parts and reducing uncertainty for Declarations of Conformity. Additionally, many importers and manufacturers in the connected vehicle supply already follow best practices from NHTSA and the Auto-ISAC on securing their software and hardware from cybersecurity threats. The Federal Communications Commission has already begun adopting a "Cyber Trust Mark" program smart devices which helps consumers make decisions on what smart devices to bring into their homes and what devices have passed rigorous cybersecurity and privacy evaluations.[1] Vehicle manufacturers and VCS importers who wish to ensure their vehicles are safe and secure for consumers would strongly benefit from a similar voluntary program. Moreover, this would benefit consumers who purchase and use these vehicles as well. ITS America strongly urges BIS to consider including supply chain certification pathways for the ICTS industry writ large to facilitate compliance with the proposed regulation without significant burden and delay.

While more clarity on the declaration process would be beneficial, ITS America requests that the Department provide additional clarity on a select number of specific areas:

- The Department should provide additional clarity as to how OEMs should interface with tier 3 suppliers and below, which are not mentioned in this NPRM.

- Under the current process proposed in the NPRM, does a connected vehicle manufacturer have to submit declarations for all of the vehicle's covered software and hardware, or just the vehicle itself? The extent to which OEMs must provide compliance documentation for these broader materials suppliers will ultimately have significant impact on the costs that OEMs can anticipate associating with compliance.

- Additionally, the NPRM notes that new Declarations of Conformity would be required for model year vehicles that have already gone through the declaration process but which have undergone "material changes." More clarity as to what constitutes "material change" would be helpful for OEMs their compliance requirements.

- With respect to the process around Declarations of Conformity submissions, is the required 10-

[1] The White House – Biden Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers. 2023

year records retention requirement reasonable, appropriate, and practicable?

- At what point must initial declarations be submitted after the rule takes effect?

Cost Estimates

The Department's estimate of $39,000 for the initial cost for OEMs to comply with the NPRM's requirements appears to underrepresent the potential scope of additional activity required by the new proposed restrictions, compliance activities, and certification requirements. One of the main compliance tasks for OEMs will be conducting extensive due diligence on their supply chains. Given the complexity of global supply chains, this requires identifying and tracking components down to their origins, especially to ensure they are not linked to the PRC or Russia. For large OEMs, the initial audit will certainly be time-consuming and resource-intensive. Additionally, if OEMs are forced to replace suppliers due to the NPRM's restrictions, they may incur additional costs related to renegotiating contracts, redesigning components, and testing new parts. The impact of switching suppliers, especially for critical ICTS components, would likely increase the compliance costs far beyond the NPRM's estimated initial transition costs. Sourcing component parts from new suppliers may lead to greater costs in global markets where there is less competition present. Furthermore, OEMs will likely need to re-engineer or modify certain software and hardware systems to ensure compliance with the NPRM, especially given the complexity of modern connected and autonomous vehicle systems. These initial engineering costs are unlikely to be captured by the $39,000 estimate, particularly for large-scale manufacturers who must make substantial technical changes. Without an accurate and realistic estimate of the costs associated with these requirements, the Department will be unable to firmly predict the costs that these requirements might incur on consumers.

BIS Advisory Opinion and Specific Authorization Concerns

ITS America supports the Department's goal of providing connected vehicle manufacturers and VCS hardware importers with advisory opinions on the nature of their transactions. This is an important step in ensuring that supply chains are secure and support U.S. national security goals, while also helping manufacturers and importers to comply with the rule and avoid unforeseen supply chain and economic disruptions.

As noted in the NPRM, vehicle and VCS hardware supply chains are often lengthy and complex. Many foreign suppliers sign contracts with U.S.-based manufacturers on model year production cycles, with contractual agreements in place for as long as three to seven years. Changes to hardware and suppliers require long timelines of designing, testing, and due diligence for OEMs. The Department has said in the proposed rule that advisory opinion requests would only be considered for actual transactions, not hypothetical ones. However, given the nature of vehicle supply chains and contracts as outlined above, it is imperative that any advisory opinion from BIS consider hypothetical transactions as well. Vehicle manufacturers and technology importers will face compliance challenges and high costs if they are forced to sign multi-year supplier agreements for prospective transactions without knowing whether their hypothetical transaction with that supplier may constitute a violation of 15 CFR 791. BIS should consider issuing advisory opinions and accompanying analysis of potential suppliers prior to manufacturers signing agreements with those entities. Advisory opinions for hypothetical transactions will help ensure that U.S.-based VCS importers and connected vehicle manufacturers have the certainty

they need to comply with the BIS requirements.

Additionally, it is critical that the advisory opinion process be more explicit and explained in the final rule. There must be uniform guidelines for manufacturers who request advisory opinions on covered transactions. BIS must ensure a standard of fairness and uniformity across the opinion process so that manufacturers are operating on a level playing field and know what to expect from the Department. Uncertainty in these processes brings unnecessary risk and burden to the industry and will result in increased costs to the industry and consumers.

In parallel, BIS should consider implementing a preclearance procedure to ensure auto manufacturers and suppliers have advanced approval for continued use of certain covered software with appropriate risk mitigation. As noted above, software code for automotive use is written on top of legacy code developed for other use cases. Moreover, the software code that supports the function of VCS or ADS has multiple layers, not all of which directly enable or support the communications capabilities of the VCS, but nonetheless support the function of the overall system. This overlap with other non-CV use cases could result in significant disruptions well beyond the automotive industry if companies are required to wait for a specific authorization to use certain code in automotive applications. BIS should therefore establish a process for companies to obtain preclearance for certain covered software items, such as base code that is not specifically designed or developed for automotive applications. Sufficient time must be built into the rules so that preclearance can be granted before any prohibitions are anticipated to affect the market. In addition to allowing preclearance only with respect to certain covered software, BIS could require companies seeking preclearance to meet specified cybersecurity standards and risk mitigation measures specific to ensuring the integrity of the relevant code, including third party vulnerability testing, as applicable. A preclearance process would mitigate the risk of undue harm to industry while still also addressing the supply chain integrity concerns related to connected vehicle software.

Finally, ITS America would encourage BIS to provide a framework and detailed process to effectively guide all involved parties, including suppliers, through the current appeals process described in this NPRM for denied special authorizations. While the NPRM outlines appeal submission timelines and Departmental responsibilities for responding to appeals, additional information should be provided as to what BIS anticipates as valid grounds for an appeal.

Broader Impact on Transportation Safety in the U.S.

While vehicle safety in the U.S. has improved over the last few decades, crashes and fatalities on our roads are still far too high. From 2011 to 2020, 350,000 people died on American roads. NHTSA estimates that there were 40,990 deaths on American roads in 2023 alone. The status quo approaches to transportation safety measures are insufficient, and innovative technological solutions are required to address this ongoing tragedy. Countries around the world have better vehicle safety records than the U.S., so it is imperative that the U.S. does not cede even more ground with an overly broad rule that would put driver and passenger safety at risk and hurt our country's long term economic competitiveness.

Vehicle technologies such as automatic emergency braking (AEB), lane keep assistance, blind spot monitoring, adaptive cruise control, and other ADS and ADAS features have made significant strides in keeping passenger vehicle drivers and passengers safe. Other vehicle features that assist drivers, provide

over-the-air software updates, and predict maintenance needs must continue to remain available so that light-duty passenger vehicles, trucks, and buses operate as safely as possible. These technologies rely on an array of hardware and software to interpret and make appropriate decisions. This also includes technologies that public transportation operators use to keep bus riders and drivers safe, including collision mitigation systems, blind spot monitoring, cameras, radar, and the underlying software that enables their effectiveness.

Additionally, if left unchanged, BIS's proposed restrictions on vehicle connectivity systems could significantly undermine the U.S. Department of Transportation's (USDOT) efforts to deploy Vehicle-to-Everything (V2X) technology. Nationwide deployment of V2X technology is integral to USDOT's plans to achieve zero fatalities on American roads. V2X technology enables vehicles to communicate with each other, with other road users such as pedestrians, cyclists, individuals with disabilities, and other vulnerable road users, and with roadside infrastructure, through wirelessly exchanged messages. NHTSA estimates that the implementation of two V2X safety applications alone could prevent 439,000 to 615,000 crashes, 13% to 18% of the total reported crashes, and save 987 to 1366 lives annually when fully implemented.

ITS America has been a leading proponent of V2X deployment for decades and released its own vision for a National V2X Deployment Plan in April 2023. Following two years of stakeholder engagement, USDOT released a plan to accelerate the nationwide deployment of V2X titled "Saving Lives with Connectivity." The plan establishes specific short-term, medium-term, and long-term deployment targets for both vehicles and infrastructure. Importantly, ensuring robust cybersecurity and privacy protections is a key pillar of USDOT's plan, and the plan identifies specific actions and milestones to ensure cyber resiliency.

As noted in more detail above, VCS technologies like V2X are built on decades of global engineering from the mobile industry that often includes contributions from PRC engineering teams. Without additional implementation time and exemptions for legacy systems, the proposed restrictions could severely impact industry efforts to deploy V2X technology in U.S. vehicles. ITS America and many of its public sector members are actively engaged in efforts to deploy V2X and help USDOT meet the deployment benchmarks laid out in the national deployment plan. As V2X is an inherently collaborative technology, the success and utility of these infrastructure deployments is predicated on the promise of future vehicle deployments. As currently drafted, the NPRM not only risks unnecessarily delaying V2X deployments in vehicles, but also stranding the substantial ongoing local, state, and federal investments in V2X infrastructure deployment.

Regulations that limit these capabilities would make our roads less safe, less efficient, and less resilient going forward. An overly broad rule from the Department that severely impedes the current supply chain of critical VCS hardware and software would jeopardize the progress that the transportation industry has made to make vehicles and the surrounding road safer for all road users. Light and heavy-duty vehicle manufacturers must continue to have these technologies easily available for their vehicles. Additionally, the U.S. risks falling further behind other countries who already have better safety records and who may have even more vehicles on the road with better safety technology after this rule goes into effect. Any rule that slows the progress made to increasing vehicle safety in the U.S. is counterintuitive to the Department's safety and security aims. As USDOT and the transportation industry at large looks to reach zero deaths on American roadways, the Department of Commerce and BIS must work to ensure that

manufacturers are able to include essential technologies in their vehicles without any impediment going forward so as to not lose progress toward Vision Zero.

Definitions and Additional Questions

ITS America recognizes the effort that the Department has demonstrated on clarifying many of the definitions discussed in the Advanced Notice of Proposed Rule Making related to this rulemaking, and we continue to follow the discussion around the term "connected vehicles" with great interest. Our comments from our previous submission on that term, given that it remains an established term-of-art in the transportation community, remain relevant to this NPRM. For this response, however, we will be discussing terminology outside the scope of our previous comments on this issue.

The NPRM defines "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 the [vehicle connectivity system ("VCS")] or [automated driving system ("ADS")] at the vehicle level." "Firmware" is exempted from this definition. The scope of "covered software" requires several clarifications.

First, as drafted, the NPRM defines "covered software" to include any software with a "foreign interest." The NPRM defines "foreign interest" as "any interest in property of any nature whatsoever, whether direct or indirect, by a non-U.S. person." This definition (particularly given the NPRM's reference to the Office of Foreign Asset Control's use of the same term) may be misinterpreted as being so broad as to sweep in virtually any software code a non-U.S. person has ever accessed or developed, and any code worked on in a covered country, even if the engineers are employed by a wholly- owned subsidiary of a U.S. company, the software is wholly owned by the U.S. parent company, and the U.S. parent company conducts rigorous cybersecurity and vulnerability testing outside of the covered country. ITS America believes that the NPRM and the underlying executive order, which are limited in scope to restricting technologies that pose an "undue" or "unacceptable" risk to national security, should not be read so broadly as to encompass code subject to these safeguards. In particular, the NPRM does not set forth any standards to determine whether a particular code stack has a "foreign interest," even if it includes historical code worked on by engineers long before the effective date of the proposed rule. The definition of "foreign interest" must be amended to apply only to cases where a foreign person retains a legal ownership or control interest in the software code and should exclude wholly owned subsidiaries of U.S. companies and employees of such subsidiaries. BIS should similarly amend the definition of VCS hardware to include "foreign interest" to clearly define the scope of covered hardware. Additionally, ITS America requests clarification as to BIS's understanding of "primary processing unit" and "at the vehicle level" as it relates to the NPRM's definition of covered software, as well as if the definition of "support" within this NPRM's context of covered software is consistent with the definition of support in part 744 of the Export Administration Regulations.

ITS America would also encourage the Department to further develop the NPRM's definition of firmware, which the NPRM currently characterizes as software specifically programmed for a hardware device with a primary purpose of controlling, configuring, and communicating with that hardware device. To avoid ambiguity, the Department could incorporate technical specifications into this definition of firmware, such as the types of processors it operates on (such as real-time operating systems and/or embedded systems), and the specific hardware components it controls. This would help

automakers and suppliers identify which components need to be scrutinized and ensure the definition is not overly broad. Additionally, firmware that can be remotely or manually updated, particularly over-the-air (OTA) updates, could present greater security risks than static, non-updatable firmware. BIS could clarify that "firmware" in the NPRM refers specifically to updatable firmware, which could be vulnerable to cyberattacks, data exfiltration, or unauthorized modifications. This would address one of the NPRM's main national security concerns - foreign adversaries exploiting the ability to modify firmware after vehicles have been deployed.

Additionally, ITS America applauds BIS for specifically excluding open-sourced software from the definition of covered software by default. We would recommend, however, that the definition of "open-source software" align with other ways in which open-sourced software is defined in law, specifically by the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which defines the term as "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."

ITS America encourages the Department to offer additional clarity as to the meaning of "integrated or attached" hardware or software – particularly, our members would benefit from confirmation as to whether software or hardware attached by a Bluetooth device or USB would be subject to the NPRM's proposed restrictions, or if the rule is rather envisioned to only include integrated technologies. Where do after-market safety technologies fit into these prohibitions? Similarly, what is the OEM's responsibility for providing consumers with the ability to attach insurance-related vehicle tracking devices?

Similarly, the NPRM twice refers to "operational design domains" to describe a vehicle's automated functions, but the term has yet to be defined in this document. Additional context to the Department's intentions with and understanding of that term would be a helpful tool for navigating the ADS provisions of this upcoming rule.

Finally, the NPRM states "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." However, the definition of VCS hardware includes global satellite navigation systems (GNSS). As GNSS receivers do not transmit information and simply receive information which is not directly used to control the vehicle we believe they should be excluded from the rule. This would make the treatment of GNSS consistent with the treatment of lidar in the NPRM: "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."

--

ITS America remains grateful for the Department's continued commitment to ensuring that transportation connectivity remains both effective and secure, and we are grateful for this opportunity to provide our feedback on this NPRM. We look forward to working together with the Department on how to structure regulations in a way that provides robust national security protections while simultaneously considering utilizing these capabilities to significantly improve safety and mobility on American roads. If you have any questions about our above response, please contact ITS America's Senior Director of

Policy and Advocacy, Bobby McCurdy, at bmccurdy@itsa.org.

Sincerely,

Laura Chace
President and CEO
Intelligent Transportation Society of America