

April 30, 2024

Elizabeth L.D. Cannon
Executive Director
Office of Information and Communications Technology and Services
United States Department of Commerce

*Re: Securing the Information and Communications Technology and Services Supply Chain:
Connected Vehicles; BIS-2024-0005*

Introduction

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 Advanced Notice of Proposed Rulemaking (ANPRM) 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.

ITS America’s 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. To that end, ITS America is grateful for the leadership

of the Department of Commerce (“Department”) in considering methods with which to improve the resiliency of transportation connectivity, particularly as it relates to information and communications technology and services (ICTS) with components or software from 15 CFR 7.4 entities.

Secure communication among transportation assets is critical to maintaining safe travel conditions, data privacy, consumer confidence, and national security. ITS America is confident that the Department will be successful in working with the transportation sector and other related stakeholders to identify a secure ICTS supply chain and security measures writ large. We look forward to providing our respective considerations on what aspects of the connected vehicle ecosystem should be the focus of these efforts, as well as ways in which the Department should consider structuring upcoming regulations on this subject to avoid additional disruption to deployment efforts around critical safety technologies.

Please find our comments on these subjects below.

ANRPM Scope and Focus

The transportation industry has benefited from robust collaboration between industry and Federal partners on bolstering cybersecurity practices related to vehicle and infrastructure connectivity. We are encouraged by the Department’s willingness to meet with numerous representatives of the transportation sector on this topic and are confident that transportation stakeholders will continue to be eager contributors to a dialogue about how best to protect the national transportation network against potential harmful activities from foreign adversaries. Further regulatory developments should be considered with on-going input from the ITS industry to ensure effective applicability of any requirements.

While ITS America welcomes the Department’s interest in assessing the respective security challenges remaining within this sector, we strongly recommend that the ANPRM’s regulatory activities be risk-based and flexible to allow adaptability to evolving security risks and be strategically targeted to prioritize mitigation of potential security risks. The present scope of this ANPRM pertains to connected vehicles, which the Department defines as “an automotive vehicle that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device.” As written, the definition encompasses all public and private automotive industry segments without regard to specific public, commercial, or consumer use cases and any potential national security risks associated with them. If the Department were to establish broad rules applying to the entirety of the connected vehicle sector as defined by this ANPRM, meaningful compliance may be prohibitively costly for automakers and their suppliers. Additionally, broad rules may limit innovation and investment in the industry, thereby hampering deployment of critical transportation

safety and efficiency technologies, as well as harm the competitiveness of numerous U.S. companies.

We recommend that the Department be more prescriptive in the definition of connected vehicles and identify the specific sectors (for example on-road, off-road, passenger vehicles, construction trucks, agricultural equipment, etc.) communications, and network types that this ANPRM seeks to address. To help achieve additional clarity related to the scope of upcoming regulatory activities on this topic, the Department should amend the definition within this ANPRM to provide clearer use case-based examples of the aspects of connected vehicles that are of greatest concern, as well as remove or clarify certain ambiguous terminology, such as the terms “related equipment” and “related technologies” in Question 2.

We believe that “connected vehicles” is the wrong term of focus for the purposes outlined in this ANPRM. The Department might be better served in identifying a more specific term of focus to help narrow some of the outstanding questions above, as well as to hone in directly on the top areas of concern for the Department. Specifically, we believe that the Department should prioritize consideration of regulatory activity on vertically integrated vehicles from 15 CFR 7.4 countries, which present the greatest likelihood of vulnerability to intrusion, rather than on areas such as vehicle-to-everything (V2X) communications which already include robust security practices, standards, and guidelines stemming from significant collaboration between regulators and industry. V2X represents a low-risk technology given the ingrained security and privacy protocols and standards associated with V2X communications, as well as the localized nature of the communications, which we will detail later in these comments. Additionally, the scaled deployment of V2X technology is integral to USDOT’s plans to achieve zero fatalities on American roads. As such, we recommend that the Department ensure that the scope of an upcoming rule on this subject avoids a one-size-fits-all approach to transportation connectivity which would threaten the pace and scale of deployment of critical transportation safety and mobility tools. If the ultimate goal of this ANPRM is to insulate the transportation sector from the influence and activity of 15 CFR 7.4 countries, then the Department should work with the U.S. transportation industry (including non-U.S. headquartered companies that sell vehicles in the U.S.) to help facilitate the continued deployment of key transportation technologies, thereby maintaining U.S. leadership in this sector and lessening the influence of global competitors in this area.

To that end, and to avoid stifling deployment in this sector, any additional regulations pertaining to OEMs or the transportation industry writ large should be structured in a way which would account for the lengthy production cycle associated with automotive product design and manufacturing, which connectivity technologies are subject to. When considering an application for a temporary authorization, the Department should review whether the automotive manufacturer has demonstrated commitment to and compliance with particular privacy and security best practices, particularly as it relates to any ICTS components that have been supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 countries. To facilitate this, the Department may want to consider developing a trusted partner program by which an

automotive manufacturer could demonstrate such commitment and compliance. Once an automotive manufacturer has been admitted into the trusted partner program, it can self-certify continued compliance with the program requirements. Additionally, ITS America recommends that the Department consider moving towards setting cybersecurity standards for ICTS hardware and software, promote further development of requirements on organizational, processes, technical and methods to ensure cyber security for vehicles and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, and support OEM participation in cross-industry collaboration (Auto-ISAC) to address risks and vulnerabilities in cooperation with national authorities.

V2X Communications

Transportation fatality statistics in the United States are a national tragedy. 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.¹ These numbers do not capture the millions of Americans that are injured on our roads every year, nor the estimated \$800 billion in financial costs that such crashes cost our country annually.² In addition, roadway fatalities disproportionately impact people of color. According to research from the Governors Highway Safety Association, African Americans were killed in traffic crashes at a rate almost 25% higher than Caucasian pedestrians in recent years, and African American pedestrians were killed at a rate twice as high.³ These numbers demonstrate the scale of the problem, but we know that this is not just a number. Each of these fatalities causes a tragic impact on the lives of the family members and friends who knew the victims. The status quo approach to transportation safety measures is insufficient, and innovative technological solutions are required to address this ongoing tragedy.

Transportation connectivity-enabled safety services, including V2X technologies, allow vehicles to communicate with other vehicles, infrastructure, law enforcement, and bicycle and pedestrian road users to avoid crashes and enhance safety. These technologies, which are highly correlated with software and require continuous management throughout their lifecycle, allow vehicles to communicate in milliseconds about critical variables such as GPS location, acceleration, predicted path, and driver controls such as steering input and braking. The National Highway Traffic Safety Administration (NHTSA) has estimated that these technologies have the potential to eliminate or mitigate up to 80% of non-impaired crashes. The National Transportation Safety Board (NTSB) has long recognized the impact these technologies could have if deployed in vehicles at scale, having first identified the potential of V2X to save lives in 1995. NTSB first recommended in

¹ NHTSA, Early Estimate of Motor Vehicle Traffic Fatalities in 2023. Available at: <https://www.nhtsa.gov/press-releases/2022-traffic-deaths-2023-early-estimates>

² Comments of U.S. Department of Transportation, ET Docket No. 19-138, at page 8 (filed Mar. 13, 2020).

³ An Analysis of Traffic Fatalities by Race and Ethnicity, Governors Highway Safety Association. Available at: <https://www.ghsa.org/sites/default/files/2021-06/An%20Analysis%20of%20Traffic%20Fatalities%20by%20Race%20and%20Ethnicity.pdf>

2013 that NHTSA require V2X in new vehicles after identifying additional fatal crashes that could have been prevented by these technologies and have continued to call for the technology's requirement. NTSB has included V2X in their top 10 most-wanted technologies in vehicles.⁴ USDOT recently released a draft National V2X Deployment Plan which outlines its approach to supporting the adoption of these important safety technologies, and we anticipate that the final version of this plan will be released shortly.⁵ These endorsements have demonstrated that the safety benefits associated with connectivity can meaningfully reduce the frequency and severity of fatalities on American roads, allowing the United States to approach Vision Zero.

Connectivity can support numerous additional services which improve transportation efficiency, mobility, and sustainability, including enhanced traffic management, optimized navigation and route planning, remote vehicle management, driver assistance, predictive maintenance, smart parking, over-the-air software updates, and more. Each of these functions represent another reason vehicles with available connectivity represent roughly 50% of new vehicles today, as well as why an estimated 95% of new vehicles will be connected by 2030.⁶ A substantial global ecosystem of original equipment manufacturers (OEMs), tier 1 and tier 2 suppliers, software providers, and other related stakeholders has emerged to facilitate the deployment of these solutions, contributing significantly to the United States economy. While safety benefits remain the foremost motivating factor for connecting the American transportation network, the associated efficiency, sustainability, and economic aspects represent enormous opportunities to improve the transportation experience for the traveling public.

As this industry continues to expand, it is critical that cybersecurity considerations are prioritized throughout the transportation connectivity ecosystem – including in aspects related to the supply chain and operations of associated hardware and software. This prioritization of security and resiliency is reflected in the current standards and practices associated with transportation connectivity, including many of the technologies considered within this ANPRM. Federal partners such as NIST and USDOT have routinely released cybersecurity resources relevant to the topics considered by this ANPRM, including NIST's Cybersecurity Framework 2.0 (CSF 2.0), which includes numerous relevant cybersecurity recommendations for transportation connectivity, including references related to enterprise risk management (ERM) strategies for supply chain risks.

NIST has also released a Privacy Framework and AI Risk Management Framework which both contain relevant recommendations for the transportation industry when connecting vehicles and infrastructure assets. USDOT's Intelligent Transportation Systems Joint Program Office (ITS JPO)

⁴ Remarks by Michael E. Graham, National Transportation Safety Board, US Department of Transportation's Vehicle-To-Everything (V2x) Communications Summit: Preparing for V2x Deployment. Available at: <https://www.nts.gov/Advocacy/Activities/Pages/Graham20220825.aspx>

⁵ Saving Lives with Connectivity: A Plan to Accelerate V2X Deployment, USDOT. Available at: https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment.pdf

⁶ <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/corporate-business-building-to-unlock-value-in-automotive-connectivity>

has created an ITS Cybersecurity Research Program, which includes informative references tailored for the ITS environment, such as “Cybersecurity Framework Profile for Connected Vehicle Environments” and “Intelligent Transportation Systems Penetration Testing.” Additionally, the National Highway Traffic Safety Administration has released a guide titled “Cybersecurity Best Practices for the Safety of Modern Vehicles,” which contains numerous recommendations relevant to the goals of this ANPRM.⁷

The numerous Federal resources provided on this subject have served as valuable reference tools for public and private transportation stakeholders as they continue to protect their connected resources against cyber intrusions. These resources are particularly helpful when used in conjunction with the numerous industry-led standards specifically pertaining to transportation connectivity, often led by groups such as SAE International, the International Organization for Standardization (ISO), and the Institute of Electrical and Electronics Engineers (IEEE). For example, the automotive industry applies ISO 21434 for cybersecurity integrity of software and electronics on-board vehicles and ISO 27001 for cybersecurity management practices for off-board systems that a vehicle might rely on. In addition, there are organizations such as Auto-ISAC whose primary mission is information sharing and analysis against cyber threats. Finally, in regards to data privacy, the automotive industry relies on best practices like those defined in the EU’s General Data Protection Regulation (GDPR) and/or certain U.S. state-level data privacy laws.

As the ANPRM identifies V2X communications as a particular area of focus, we believe it would be productive to look specifically at the security characteristics of these technologies. For cellular-vehicle-to-everything (C-V2X) communications, the 3GPP standard for direct V2X communications, the main security advantage is clear: C-V2X relies on communications that typically take place within a given localized environment, such as a specific intersection or roadway segment. The localized nature of C-V2X communications offers inherent security benefits, such as a reduced attack surface for malicious actors, faster detection and response times to security threats, and greater resilience to disruptions of the larger communication network. The localized-nature of C-V2X communications ensures that there is a limit to the distance and time over which these messages are accessible. Numerous industry standards have been developed to further enhance C-V2X security practices, such as through the message requirements described in SAE J3161/1 (the underlying standard to specify how C-V2X communications are managed) and SAE J3161 (a similar standard describing how vehicle-to-infrastructure communications operate). These SAE standards normatively require use of the IEEE 1609.2 family of standards, which help further define security protocols and encryption methods for protecting data transmitted over C-V2X networks. Additionally, the edge computing aspects of digital infrastructure and connected vehicles, which are important for low latency operations, provide local and redundant security controls. Finally, at this time, C-V2X devices have no control over the functionality of a given

⁷ <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf>

vehicle, and only serve to provide additional information-exchange between drivers, infrastructure, and pedestrians, further limiting the risks associated with C-V2X utilization.

Additionally, V2X communications follow robust privacy practices which help safeguard the privacy of user data from misuse and access by external parties. V2X communications utilize digital signatures and certificates for authenticity and integrity of the messages exchanged among end users. Because these messages may contain sensitive information, such as a vehicle's location and speed, privacy is at the core and at every step of the system design as illustrated by three key concepts: pseudonym certificates, privacy from insiders, and privacy from eavesdroppers. To better serve the unique needs of V2X communications, IEEE Std 1609.2 defines a new type of certificate called *pseudonym* certificate that indicates its holder's *permissions* as opposed to the traditional ITU-T X.509 certificate that indicates its holder's *identity*. Neither the pseudonym certificate nor any part of V2X messages, e.g., basic safety message (BSM), personal safety message (PSM), etc. contain any personally identifiable information (PII) that can be used to map a message to its sender. So, the use of pseudonym certificates enables authenticity and integrity of the messages without risking the sender's privacy. To further protect end users' privacy from insiders (i.e. unauthorized access, misuse, or disclosure by individuals who have legitimate access to that information) and in particular from authorities that issue the pseudonym certificates to the end users, the Security Credential Management System (SCMS) implements several unique and novel mechanisms like butterfly keys and linkage values.⁸ These mechanisms ensure that no single component of the SCMS (Certificate Authority, Linkage Authority, Registration Authority, or anyone else) on its own can link a pseudonym certificate to the certificate holder. Finally, V2X messages need to be transmitted at regular intervals, e.g., BSMs are transmitted every tenth of a second. So, even though V2X messages may not contain any PII, there is a risk that an eavesdropper that records all the messages can track a sender by associating the sender with a pseudonym certificate. For this reason, end users are issued multiple random looking pseudonym certificates (so that given any two certificates an eavesdropper can't tell if they belong to one sender or two different senders), and they are prohibited from using a pseudonym certificate for a prolonged period of time.⁹

Supply Chain Concerns

With respect to supply chain concerns relative to components from 15 CFR 7.4 countries, there is no sole source Chinese supplier for C-V2X devices. In fact, the majority of Tier 1 and 2 suppliers in the C-V2X ecosystem are based outside of China. European, Japanese, and Korean suppliers are key players in the supply chain for C-V2X components. Given the diverse nature of the C-V2X supply chain, as well as the aforementioned security and privacy standards currently in place

⁸ see IEEE Std 1609.2.1 and its predecessor, SCMS Proof of Concept that was developed in a collaborative effort by the Crash Avoidance Metrics Partners LLC and USDOT

⁹ see IEEE Std 1609.2.1, SCMS Proof of Concept, and SAE J2945/1.

governing C-V2X utilization, these technologies should not represent a high priority for inclusion within the Department's upcoming regulatory activity regarding transportation connectivity. While ITS America encourages the Department to engage with V2X stakeholders to ensure that the new industry standards governing V2X security and privacy are quickly proliferated and enacted, we would emphasize that any new regulatory activity from the Department pertaining to V2X technologies should be tailored in a way that would not adversely affect USDOT's V2X deployment goals, as not to lessen these technologies' ability to reduce fatalities on American roads.

Cloud Service Providers

Beyond our interest in providing the Department further context on the security, privacy, and supply chain practices of the V2X ecosystem, ITS America is also interested in providing feedback on the relationship between connected vehicle OEMs and cloud service providers (CSPs), particularly in response to question 20 of the ANPRM. ITS America would note that CSPs offer IT infrastructure services, such as virtual server instances and cloud-based storage, compute, and database services. CSPs may also offer infrastructure relating to emerging technologies such as machine learning (ML), artificial intelligence (AI), data lakes, and Internet of Things (IoT). These collective services run in CSP data centers are built to meet high level security requirements (as demonstrated through security assurance certifications such as FedRAMP) to the benefit of all CSP data center customers, including connected vehicle OEMs and Tier-X suppliers, which develop technologies for connected vehicles/products.

Cloud services are provisioned and controlled by customers using application programming interface (API) calls or a management console. Customers, including OEMs, can use cloud services in any number of ways to build their own applications or other solutions, and can elect to utilize a combination of services and features to address their specific use cases.

CSP customers maintain full control of their data that they upload to the cloud services, and determine where such data is stored, how it is secured, and who has access to it. Customers can increase their resiliency using cloud services to back up and/or run in parallel in more than one geographic location. Geographically dispersed CSP infrastructure can provide OEMs options beyond the typical on-premises infrastructure on a primary and back up data centers located in relatively close proximity.

Customers, including OEMs, own and manage their data and select the geographic location where their data is stored using API calls or a management console. Customers can back up their data in more than one geographic location. CSPs do not access or use customer data without the customer's agreement or unless necessary to comply with applicable law. In some cases, customers may provide instructions to CSPs that require their services to access or use customer data. For example, if a customer provides instructions for a cloud service to replicate certain

customer data into different data centers, the applicable cloud services will need to access or use that data in order to replicate it as instructed by the customer. A customer may also request a CSP to access their non-production or test data in connection with the CSP advising the customer on cloud architecture best practices.

CSPs take data privacy and security very seriously, which is reflected in, among other things, CSP security assurance programs that use best practices for global privacy and data protection to help customers operate securely within the cloud environment. These compliance programs, supported by certifications or attestations from independent third parties, may include ISO, SOC, CSA (Cloud Security Alliance Controls), TISAX (Automotive Industry Standard), FedRAMP, NIST, etc.

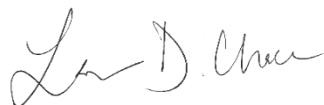
Security is a shared responsibility between CSPs and their customers, with customers controlling the security of what they put on CSP infrastructure. CSPs manage the physical infrastructure of their data centers and the components that enable virtualization. Customers are responsible for configuring the cloud services in a way that protects the confidentiality, integrity, security, and availability of the customer's data. This means connected vehicle OEMs must take active steps to secure their data and applications that are deployed on cloud services. Responsibilities include managing user access, securely configuring the cloud services, encrypting data both in transit and at rest, ensuring network and firewall configurations are robust, and keeping applications updated with the latest security patches. CSPs generally offer customers a variety of services, best practice documents, and training to help customers meet their responsibilities. These offerings, include identity and access management (IAM) features, key management services (allowing customers to create and manage cryptographic keys used to encrypt data, helping to protect data at rest and in transit), intelligent threat detection, and logging and monitoring services. These offerings help connected vehicle OEMs implement robust security measures for their data.

Finally, question 20 asks to “describe what access privileges, controls, and remote capabilities with respect to connected vehicle OEM systems are afforded to the CSP.” It is unclear what is meant by “connected vehicle OEM systems” and the term is not defined or clarified elsewhere in the ANPRM. Additionally, it is unclear what is meant by “control” or “remote capabilities.” Clarification of these terms is necessary for meaningful public review and comment. However, as a general matter and as described above, CSPs do not have access privileges or control of connected vehicle OEM systems or their data running on the CSP's services. CSPs also offer customers services that enable customers to monitor and log access to their accounts hosted on the CSP and customers can encrypt their data, which means the data is rendered useless without the applicable decryption keys (customers are responsible for such keys). CSPs do not have any remote capabilities with respect to connected vehicle OEM systems or devices. It is primarily the responsibility of the OEM, and not the CSP, to control the onboard vehicle systems.

Conclusion

ITS America is grateful for the opportunity to comment on this effort and is eager to work with the Department as it finalizes the scope of a new rule on this subject. We look forward to continuing to support the work of the Department, USDOT, the FCC, and other regulatory partners as we work to develop a regulatory landscape for the next generation of transportation safety solutions that will deliver a secure transportation network that is safer, greener, and smarter for all. If you have any questions, please contact ITS America's Senior Director of Policy and Advocacy, Bobby McCurdy, at bmccurdy@itsa.org.

Sincerely,



Laura Chace
President and CEO
ITS America