TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

April 30, 2024

U.S. Department of Commerce
Bureau of Industry and Security
1401 Constitution Avenue, NW
Washington, D.C. 20230

Re: TechNet Comments on "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles" (Docket No. BIS-2024-0005)

To Whom It May Concern:

TechNet appreciates the opportunity to comment on the Department of Commerce's ("Department") Bureau of Industry and Security's ("BIS") advance notice of proposed rulemaking ("ANPRM") on securing the information and communications technology and services ("ICTS") supply chain for connected vehicles. Connected vehicles (CVs) include virtually all modern internal combustion engine (ICE) vehicles, electric vehicles (EVs), and autonomous vehicles (AVs). We welcome the Administration's whole-of-government approach to respond to evolving national security challenges while noting that any new rules, restrictions, or enforcement actions should seek to minimize disruptions to innovation, supply chains, and regular business activities where feasible.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.4 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

Meeting our national security objectives depends on several factors, including maintaining our economic strength and securing our position as the global leader in technology. The United States automotive industry is a key driver of innovation and economic development. The automotive industry supports a total of 9.7 million American jobs, or about 5% of private-sector employment. Auto manufacturing provides more than $1 trillion to the American economy each year through its collective impact on sales, service, parts development, jobs, and small businesses. Foreign nations are actively working to overtake our lead in automotive development. The Chinese Communist Party has identified strategic and emerging technologies, including electric vehicles and autonomous vehicles, as a key element of economic competitiveness and national defense. In 2022, China surpassed the U.S. in venture capital investments in AVs, with 60% of the global share. U.S. companies, which secured more than half of global investment in the sector in 2021, took in less than 15% in 2023.

Our complex digital world also requires a comprehensive cybersecurity strategy that increases the security and resilience of all networks and protects against cyberattacks through the voluntary coordination of industry and government. A variety of actors, including foreign adversaries, are well-resourced and highly motivated to steal U.S. data and trade secrets and disrupt critical infrastructure using sophisticated cyber weapons. TechNet has long advocated for risk-based and stakeholder-driven policies to protect the U.S. from bad actors, including measures that protect Americans' data, secure America's critical infrastructure and supply chains, and ensure that emerging technologies, like artificial intelligence, leverage security by design principles at their inception. We also support the enactment of comprehensive and preemptive federal data privacy legislation to protect consumers' data, as well as the enactment of a strong federal data breach notification law and measures that protect Americans from identity theft and fraud.

As such, we appreciate that the Administration is contemplating how to further enhance protections for Americans' data vis-a-vis national security and appreciate the opportunity to comment on the BIS's ANPRM focused on connected vehicles. This review comes at an important time as foreign adversaries, notably China, seek to overtake America's lead in automotive innovation. TechNet's concern is focused on original equipment manufacturers (OEMs), tier-1 ICTS system suppliers, and AV deployers that are controlled by, owned by, or subject to the jurisdiction of a foreign adversary. These entities pose a greater concern for CV security than individual component manufacturers. It is imperative that BIS addresses the national security risks that these overseeing entities could pose while minimizing disruption to commercial activity where feasible.

To that end, the TechNet respectfully submits the following recommendations:

Refine Key Definitions

As noted above, the term "connected vehicle" includes a wide range of vehicle types, such as modern ICE vehicles, EVs, and AVs.

As BIS refines its definition of connected vehicles, we recommend BIS consider any preexisting terminology or definitions that federal and state agencies currently employ, including the National Highway Traffic Safety Administration (NHTSA). For example, regarding terminology associated with driving automation systems, including "automated driving systems" (ADS) and "advanced driver assistance systems" (ADAS) features like lane-keeping assistance systems in human-driven vehicles today, BIS could consider definitions from SAE J3016, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," in its regulatory efforts.

Conduct Thorough Analysis of Connected Vehicle Supply Chains

Connected vehicles, which would include virtually all modern internal combustion engine vehicles, electric vehicles, and autonomous vehicles, are defining mobility innovations of this and the next generation. These technologies are revolutionizing how Americans travel and are making our roadways safer and more accessible. The automotive sector is critical to our economic growth, and the importance of U.S. leadership in automotive technology cannot be overstated.

At the same time, we also recognize that evolving global threats require express attention from industry and government to protect both consumers and our national security. We

acknowledge that CVs, as well as key ICTS systems within CVs, pose a national security risk if they are controlled by, owned by, or subject to the jurisdiction of a foreign adversary. We believe foreign adversary-controlled OEMs, tier-1 ICTS system suppliers, and/or AV operators pose the most pressing national security risks. These foreign entities oversee the selection of their components and hardware and have far greater authority over their data than a components manufacturer. These overseeing entities should be the focus of BIS's investigation.

We appreciate BIS's engagement with the industry through this ANPRM. Moving forward, we recommend that BIS investigate mitigating measures that continue to promote innovation in the U.S., including sourcing components from a global supply chain when necessary while protecting national security. This process is critical because the safety of hardware and software systems is, in some cases, reliant on these components. TechNet members prioritize safety, which is why our members source high-quality components from around the world.

Global Sourcing

The CV industry needs the highest quality components available on the market — including some manufactured by foreign entities when there is no reasonable alternative produced domestically — to meet performance and safety requirements. Many companies in the CV industry develop and engineer portions of their hardware and software in-house while relying on high-quality vendors and suppliers to supplement to reduce costs, manage production and deployment timelines, and deliver the most cutting-edge and proven technologies. OEMs are required to maintain a global supply chain primarily to obtain the required technologies to achieve safety goals and secondarily to do so in a cost-effective manner.

To ensure the safety and quality of the product, there is a highly rigorous and comprehensive process of assessing and vetting those vendors. One TechNet member describes its process for vetting third-party vendors as a comprehensive review of the vendor's overall security posture and maturity. The company's security team conducts recurring assessments of a vendor's security posture, which may include reviewing third-party certifications, attestation reports, security assessment questionnaires, design documents, and penetration tests conducted by reputable third parties. Similarly, the search process for ICTS integral components includes competitive bidding based on performance requirements. Technical competencies, supply chain optimization, and price determine vendor nominations. This also includes reviewing technical and operational security vulnerabilities. Vendors are vetted for a specific use case and must undergo further assessment if a new use case is proposed to be added for the vendor. After onboarding an ICTS integral component supplier, there is a significant process to transition and integrate the new component. This timeline includes hardware fit and safety analysis, regression testing, re-training models, bug findings, and fixes. This process is critical because, as described above, the safety of software and hardware systems relies on these components.

OEMs, especially in the AV industry, may have sole supplier sources where there aren't the financial or engineering resources and bandwidth to support the parallel path development of multiple components. ICTS components have unique designs based on suppliers, and incorporating multiple sources would mean parallel paths of vehicle integration and development efforts, which is extremely expensive and not practical. OEMs cannot build systems interchangeably using different sensors without making bespoke forks, which could

have cascading effects throughout the system. The process of changing and safely integrating sensors from a new ICTS integral vendor will take at least three to five years minimum. This would severely slow down the progress of CV technology in the U.S. Potential limits on ICTS components would create higher barriers to entry for American-based connected vehicle start-ups and stifle innovation. Any potential BIS rulemaking should, therefore, focus on key connected vehicle ICTS systems — rather than ICTS components — that have an element of foreign adversary control.

High-Quality Hardware

Any potential rule should distinguish between higher-risk transactions or situations involving key connected vehicle ICTS systems with an element of foreign adversary control, and lower-risk ICTS components or hardware. Key ICTS systems would include software, operating systems, battery management systems (BMS), telematics systems, braking systems, ADAS, and ADS. By contrast, one example of lower-risk ICTS hardware that has received prominent but unwarranted policymaker attention recently is LiDAR.

Light Detection and Ranging sensors, or LiDAR, are sensing technologies that measure the time it takes for light to return from the objects from which that light reflects. Through infrared light pulses, light photons are projected across a field of view and reflect off the surfaces they encounter. Some of the reflected photons return back to the LiDAR sensor, providing coordinates, which can be used to generate detailed 3D representations of an area. AVs must accurately and reliably perceive objects and vehicles to safely travel on public roads. Accordingly, AV developers equip their vehicles with a combination of high-quality hardware, including ultra-high-definition cameras, imaging radars, and LiDARs. Data from these sensors is processed and fused into a holistic and dynamic picture of the AV's environment. Each of these sensors serves an important function in the AV's ability to safely navigate through the world. LiDAR is commonly used in a range of applications, from our smartphones to precision agriculture; it is an essential technology for AV operation. It is capital-intensive to develop cutting-edge LiDAR, and when coupled with limited demand, the cost-benefit tradeoffs for many LiDAR suppliers are skewed towards manufacturing for ADAS use cases instead of AVs.

The data from LiDAR is fed in real-time to a perception system on board the vehicle. Indeed, LiDAR in many AVs, like cameras and radars, is not a connected device, meaning it is not directly connected to the internet. Many TechNet members report that the internal networks that house these sensors on an AV are physically separate from the internet, and the devices communicate to the AV's computer through a secure gateway using ethernet through commonly accepted best practices and standards. Sensors can also be vetted for evidence of wireless antennas or external chips, and any software and firmware updates intended for the devices can be uploaded by a vendor to an external system, where a developer can retrieve and review them before pushing them to the onboard devices.

AV developers process terabytes of sensor data every time they run a vehicle, so specially designed removable recording systems are often used to record LiDAR and camera data since the data is too large to offload wirelessly. If a third party wanted to try to wirelessly offload this data, an AV developer's wireless networks would not have the capacity to handle this much data (hence why developers manually offload logs on specially designed systems), so a developer would immediately notice if data were attempting to flow out of the company at that volume.

AV developers implement various processes to ensure AV security when updates to sensor systems on board the vehicle are needed. For example, one TechNet member says it does not update self-driving software when the AV is engaged in autonomous driving. The AV must be stationary and in manual mode (i.e., only a vehicle operator could operate the vehicle, not the computer) to receive a software update, which happens at its secure facilities. Most updates currently occur through a physical port; if an AV needs to communicate with the cloud, it is managed through mutual Transportation Layer Security (mTLS) — an industry standard typically used in a Zero Trust cybersecurity framework — to verify the identity of the users and devices requesting or receiving and sharing data. Any future over-the-air software updates would take place in the same secure and controlled settings.

Connectivity

Certain OEMs build their own Telematic Control Unit "TCU," and it must be built to the standards set by the Federal Communications Commission and recognized by the industry. After these devices are manufactured, they must undergo carrier certification and testing protocol from carrier companies before they are able to be used. All connections are made through private network connections with major American-owned network carrier companies.

In the case of connected AVs, many AV developers use remote assistance tools to provide high-level guidance to the vehicle over some form of network connection. However, these tools are distinct from "remote driving" as they do not control the vehicle, which in turn protects against the undue or unacceptable risks contemplated in the ANPRM. Instead, the AV takes the information from the vehicle's sensors and validates it through its onboard computer before taking action. Therefore, it will not take any action that violates its safety decision-making framework.

Data Management

American CV developers work to secure the data collected by the vehicle, how it is managed in-vehicle, how it is managed as it is off-loaded from the vehicle itself, and who has access to the data afterward. We do not have evidence that LiDAR and other sensor equipment suppliers have independent access to their customers' systems. In fact, customers protect their intellectual property from a variety of risks, including independent access. When testing products for security risks, one member says they found no evidence of call-outs to external Internet Protocols (IPs) or other unexpected attempted connections.

For cybersecurity mitigation, most American OEMs follow general best practices when designing their connected vehicle network. These practices block entities from changing the component configuration or firmware without going through the OEM's controlled process update. There are network segmentation (network gateway to segregate internal vehicle networks and external networks) and traffic isolation controls that prevent unauthorized traffic flows between external servers and CV components.

<u>Leverage Existing Cybersecurity Standards</u>

As described above, securing a CV requires diligence throughout its development and operation. Because the technology is cutting-edge, proprietary, and highly valuable, CV developers are diligent in how they approach cybersecurity. Cybersecurity risks are

constantly evolving, so continuous improvement in handling them is critical. We recommend that BIS highlight existing cybersecurity standards and best practices and work with other federal agencies and industry on strengthening existing cybersecurity standards, including NHTSA and Automotive ISAC. For example, TechNet members follow public sector guidance from NIST's Cybersecurity Framework and NHTSA's Cybersecurity Best Practices for the Modern Vehicle. If a new threat emerges, BIS should work with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") to share this information with federal partners, including NHTSA, to update these standards to address these new concerns.

As AV developers scale and mature their businesses, they are working towards compliance with the International Organization for Standardization ("ISO") standards ISO 21434 and ISO 27001, which are worldwide standards that define requirements for cybersecurity engineering in road vehicles, and information security, cybersecurity, and privacy protection requirements for information security management systems. Many TechNet member companies serve on SAE International standards-setting committees, including the Automated Vehicle Safety Consortium, which publishes best practices that SAE says will inform and lead to industry-wide standards for ADS. Additionally, many AV developers have created and published Voluntary Safety Self-Assessments (VSSAs) — assessments that NHTSA encourages entities engaged in AV testing and deployment to publish to demonstrate to the public their approach to safety — which include discussion on how they incorporate vehicle cybersecurity considerations into their AVs.

Coordinate with Related Agencies

We believe the U.S. Department of Transportation and NHTSA are well-positioned to advise BIS on any safety impacts of potential prohibitions or restrictions.

Further, the U.S. Government should work with States to promote consistent regulatory frameworks that facilitate the safe testing and deployment of AVs, which in turn encourages continued investment in and operation of AVs and associated technologies in America. Congress and the Administration could create incentives to promote and facilitate research and investment in the development and manufacturing of ICTS products and services integral to CVs in the U.S. TechNet has also long-supported the establishment of a uniform, national framework that promotes the safe testing, deployment, and operation of AVs. By clarifying federal and state roles, granting exemptions where applicable, and expedited rulemaking, the federal government can accelerate AV innovation in the U.S.

Additionally, policymakers should invest in workforce programs to develop and train the workers needed for CV and ICTS-related jobs and industries. For example, the *CHIPS and Science Act of 2022* established the Regional Technology and Innovation Hubs Program to support regions with the potential for rapid growth in key emerging technologies. The "Headwaters Hub," a public-private consortium based in Montana, is dedicated to advancing technologies in photonics-based sensing and autonomous systems. The Hub is now seeking program funding from the Department of Commerce's Economic Development Agency to support technology maturation and development, increase entrepreneurial opportunities, and establish new education and workforce programs in the region. TechNet is also urging Congress to provide $4 billion in funding for fiscal year 2025 to expand tech hub development nationwide.

Conclusion

Geopolitical shifts and concerns over national security, data governance, digital sovereignty, and economic dependencies are increasingly evolving, and we appreciate the Administration's whole-of-government approach to addressing these challenges.

As with any hardware or software components integrated into a CV — whether manufactured in the U.S. or abroad — ensuring the security and integrity of the product is paramount to U.S. OEMs, suppliers, and AV developers. We want to reiterate that we appreciate BIS undertaking this review and believe the greatest national security risks are posed by adversary foreign-controlled OEMs, tier-1 ICTS system providers, and AV developers. Limiting U.S.-based CV developers' access to the best and most performant ICTS components, especially without a thorough evaluation and accurate assignment of risk, would negatively affect the development and deployment of CVs in America and weaken our global competitiveness.

In a complex world that relies increasingly on emerging technologies, it has never been more important to ensure the U.S. addresses emerging threats while maintaining our ability to innovate and compete. We appreciate your attention to our views on this matter and look forward to serving as a resource.

Sincerely,

Executive Vice President