Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	ET Docket No. 21-233
	)	

COMMENTS OF THE ALLIANCE FOR AUTOMOTIVE INNOVATION

Hilary Cain
Senior Vice President, Policy

Sarah Puro
Vice President, Safety and Technology Policy

Tara Hairston
Senior Director, Technology Policy

Alliance for Automotive Innovation
1050 K Street NW, 6th Floor
Washington, DC 20001

Sara M. Baxenberg
Joshua S. Turner
Stephen J. Conley

Wiley Rein LLP
2050 M Street NW
Washington DC

Counsel for Alliance for Automotive Innovation

June 27, 2025

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	ET Docket No. 21-233
	)	

COMMENTS OF THE ALLIANCE FOR AUTOMOTIVE INNOVATION

The Alliance for Automotive Innovation ("Auto Innovators"),[1] which represents the automotive ecosystem in the United States, including automakers, suppliers, semiconductor companies, battery makers, and technology firms, hereby submits these comments in response to the Public Safety and Homeland Security Bureau's ("Bureau") and Office of Engineering and Technology's ("OET") Public Notice in the above-captioned proceeding.[2] The Public Notice

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

[2] *The Public Safety and Homeland Security Bureau and the Office of Engineering and Technology Seek Public Input on Commerce Department Determination Regarding Certain*

seeks comment on whether the Federal Communications Commission ("FCC" or "Commission") should update its Covered List of communications equipment and services that pose a U.S. national security threat ("Covered List") in view of the U.S. Department of Commerce's ("Commerce Department") Bureau of Industry and Security ("BIS") Final Rule on connected vehicle technologies, issued on January 14, 2025 ("BIS Rule").[3] While Auto Innovators appreciates the critical issues at stake in this proceeding, the Public Notice's proposed Covered List update is inconsistent with the BIS Rule, will likely frustrate the Trump Administration's broader policy priorities, and is not required by the Secure and Trusted Communications Networks Act of 2019 ("Secure Networks Act" or "SNA").[4]

I. INTRODUCTION AND SUMMARY

Auto Innovators understands the seriousness of the national security risks posed by foreign adversaries and strongly supports the objectives of the Trump Administration in addressing these risks through the BIS Rule. Indeed, Auto Innovators worked closely with BIS as it developed a framework that helps to preserve national security and to safeguard Americans from these risks while maintaining the flexibility to recognize when the risks can be successfully mitigated. Auto Innovators also appreciates the FCC's commitment to meeting its statutory

Connected Vehicle Technologies, WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233, Public Notice, DA 25-418 (rel. May 23, 2025) ("Public Notice").

[3] *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, Final Rule, 90 Fed. Reg. 5360 (Jan. 16, 2025) ("BIS Rule"); 15 C.F.R. §§ 791.300-791.321.

[4] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) ("SNA" or "Secure Networks Act").

obligations under the Secure Networks Act and acknowledges the integral role that the FCC plays in safeguarding U.S. communications networks from foreign threats.

However, the Bureau's proposed update to the Covered List risks actively harming the policy goals the Trump Administration seeks to achieve as it implements the BIS Rule and exercises the Rule's built-in flexibilities. The Public Notice's proposal to update the Covered List to include the broad product categories identified in the BIS Rule would impose FCC-related restrictions with wide-ranging impacts that would be at variance with carefully defined limitations, critically important implementation timelines, and the general and specific authorizations and advisory opinions that BIS will issue in the future. Considering the Commission's ongoing work to expand the operation of the Covered List to new contexts within FCC regulations, moreover, including these broad product categories could create even bigger departures from the BIS Rule for covered technologies and could complicate the Commission's ability to use or refer to the Covered List in other regulatory contexts.

Updating the Covered List is also legally unnecessary. The FCC is neither obligated nor authorized to add these product categories to the Covered List, because they do not constitute "specific determinations" under the text of the SNA. To avoid confusion and minimize the potential for unintended consequences that could hamper U.S. technology leadership and undermine vehicle safety, the FCC should refrain from making any Covered List update at this time. The agency should instead revisit Covered List revisions only when there is a "specific determination" regarding connected vehicle technologies—*i.e.*, one that enumerates particular entities or products made by particular entities—as required by the SNA.

If the Commission nevertheless moves forward with a Covered List update in an effort to account for the BIS Rule (which it should not), any such update must be carefully crafted to

remain coextensive with the prohibitions implemented by BIS. That must include taking into account any general or specific authorizations and advisory opinions that the agency may issue. To achieve this congruity, the Public Notice's proposal would need to be substantially revised, including through an inter-agency process that ensures that regulations are and remain aligned. Given the complexity of the BIS Rule, incorporating the Rule's covered technologies into the FCC Covered List regime could require a significant expansion of the budget and FCC staff dedicated to administering the Covered List. This particularly true given that BIS intends to continue issuing trade restrictions pursuant to its Information and Communications Technology and Services ("ICTS") authority under Executive Order 13873. Nonetheless, if the FCC seeks to update the Covered List at this time, these steps are crucial to ensure harmonization and reduce duplicative rulemaking proceedings.

II. THE BIS RULE IS A CAREFULLY CRAFTED POLICY THAT APPROPRIATELY ACCOUNTS FOR NATIONAL SECURITY INTERESTS.

The BIS Rule was thoughtfully drafted based on extensive study of the connected vehicle technology industry to address the national security risks the Commerce Department identified. Critically, in consultation with a wide range of stakeholders, it was also carefully crafted to prevent significant unintended consequences. As a result of this deliberative process, the BIS Rule operates by establishing a broad prohibition on certain "connected vehicle"[5] transactions

[5] *See* 15 C.F.R. § 791.301 (defining a "connected vehicle" as "a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways, 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"). Vehicles that are either "operated only on a rail line" or have "a gross vehicle weight rating of more than 4,536 kilograms (10,000 pounds)" are not included within this definition. *Id.*

involving covered software[6] and Vehicle Connectivity System ("VCS")[7] hardware where the covered technologies or vehicles are produced by certain Chinese- and Russian-controlled entities that pose unacceptable national security risks.[8] This broad prohibition is subject to exemptions related to technology production timelines, the opportunity for parties to obtain general and specific authorizations by BIS where risks have been appropriately mitigated, and the ability for entities to request that BIS issue an advisory opinion with respect to a particular transaction. The exemptions and authorizations enable entities to engage in transactions that would otherwise be prohibited under the BIS Rule, where the risks that BIS identified are either less present or appropriately mitigated and therefore do not "pose[] an unacceptable risk to the

[6] The BIS Rule defines "covered software" as "the software-based components, including application, middleware, and system software, in which there is a foreign interest, executed by the primary processing unit or units of an item that directly enables the function of Vehicle Connectivity Systems or Automated Driving Systems at the vehicle level." BIS Rule at 5415; 15 C.F.R. § 791.301. *See also* BIS Rule at 5415; 15 C.F.R. § 791.301. (defining "Automated Driving Systems" 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)."); BIS Rule at 5416; 15 C.F.R. § 791.301 (defining "VCS" as "a hardware or software item installed in or on a completed connected vehicle that directly enables the function of transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz.").

[7] The BIS Rule defines "VCS hardware" as "software-enabled or programmable components if they directly enable the function of and are directly connected to [VCS], or are part of an item that directly enables the function of [VCS], including but not limited to: microcontroller, microcomputers or modules, systems on a chip, networking or telematics units, cellular modem/modules, Wi-Fi microcontrollers or modules, Bluetooth microcontrollers or modules, satellite communication systems, other wireless communication microcontrollers or modules, external antennas, digital signal processors, and field-programmable gate arrays." BIS Rule at 5416; 15 C.F.R. § 791.301.

[8] 15 C.F.R. §§ 791.302, 791.303, 791.304.

national security of the United States or the security and safety of United States persons."[9] And the provision for advisory opinions allows the agency to clarify the scope of the BIS Rule as it applies to individual transactions. Each of these conditions on the BIS Rule's broad prohibition are described in greater detail below.

Exemptions. The BIS Rule's software restrictions and hardware restrictions for completed connected vehicles will take effect starting with model year 2027 vehicles.[10] Restrictions on standalone VCS hardware transactions will take effect in model year 2030 vehicles,[11] or January 1, 2029 for units not associated with a model year.[12] Accordingly, BIS will consider as "exempt" any otherwise-covered transactions that occur prior to these timeframes.

General Authorizations. The BIS Rule contemplates that certain otherwise-prohibited transactions are "low risk use cases" that can be permitted without notification to BIS.[13] The text of the Final Rule itself does not grant any general authorizations, but explains BIS' intention to "issue a set of general authorizations shortly after publication of this rule that align with the general authorizations outlined in the [Notice of Proposed Rulemaking]," including "general authorizations for small businesses; for connected vehicles used infrequently on public roads; for

[9] *Exec. Order No. 13873: Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22689, 22690 (May 15, 2019).

[10] 15 C.F.R. § 791.308(b).

[11] *Id.* § 791.308(a)(2).

[12] *Id.* § 791.308(a)(1).

[13] BIS Rule at 5401.

display, testing, or research purposes; and for repair, alteration, or competition."[14] And indeed, BIS issued its first two general authorizations on June 10, which include a series of terms and conditions related to "Limited Use Cases" and "Temporary Importation."[15]

Specific Authorizations. In addition to contemplating general authorizations, BIS anticipated that there may be certain transactions involving specific entities that could be authorized consistent with national security objectives. Accordingly, the BIS Rule establishes a specific authorization process "to allow BIS on a case-by-case basis to determine the nature and scope of the undue or unacceptable risk to U.S. national security posed by transactions involving VCS hardware and covered software, including the extent of foreign adversary involvement in the transactions, as well as potential mitigations."[16]

Advisory Opinions. BIS also provided a mechanism by which "VCS hardware importers [or] connected vehicle manufacturers may request an advisory opinion from BIS to determine whether a prospective transaction is subject to a prohibition, or requirement under" the Rule.[17] This codifies a process by which a party may describe a specific transaction to BIS, which will

---

[14] *Id.* at 5402.

[15] *See General Authorizations*, BIS, https://www.bis.gov/oicts/connected-vehicles/general-authorizations (last visited June 18, 2025). The Limited Use Cases General Authorization permits transactions where the completed connected vehicle "will be used on [the] . . . road[] for fewer than 30 calendar days in any twelve-month period" or other specified limited uses, and the Temporary Importation Authorization permits transactions where a connected vehicle incorporating VCS hardware or the VCS hardware itself is being temporarily imported for subsequent export to a non-U.S. market for sale. *ICTS Supply Chain: Connected Vehicles Subpart D: General Authorization No. 1: Limited Use Cases*, BIS, at 2 (June 10, 2025), https://www.bis.gov/media/documents/connected-vehicles-general-authorization-1 ("General Authorization No. 1").

[16] BIS Rule at 5403-04; *see also* 15 C.F.R. § 791.307(g).

[17] 15 C.F.R. § 791.310(a).

then render a determination on whether the transaction is prohibited under the Rule. This important tool will allow companies to seek pre-approval from BIS for their transactions for coverage under the BIS Rule.

These exemption, authorization, and advisory opinion mechanisms are critical components of the BIS Rule's framework and will help provide certainty about the scope of the restrictions, when the restrictions will become effective, and how regulated entities may seek relief. The framework will likewise ensure that BIS has the requisite flexibility to offer relief, as warranted, to allow the U.S. automotive industry to continue to thrive without posing unacceptable risks to U.S. national security. As the BIS Rule becomes effective, BIS will undoubtedly continue to gain experience that will inform its administration of the rule and the types of transactions that are permissible.

III. THE BUREAU'S PROPOSED ADDITION TO THE COVERED LIST WOULD CONFLICT WITH THE BIS RULE'S CAREFULLY CRAFTED FRAMEWORK AND CREATE UNINTENDED CONSEQUENCES FOR COVERED LIST ADMINISTRATION AND COMPLIANCE.

In stark contrast to the careful, considered, and flexible regulatory regime developed by BIS, the Public Notice proposes to simply add the BIS Rule's product categories that underpin the "prohibited transactions" to the FCC Covered List, thereby imposing all existing and future FCC regulatory consequences of Covered List inclusion across this entire class of products. In doing so, the Bureau's proposal leaves out key aspects of the BIS Rule that are intended to make the Rule effective and implementable. Beyond this shortcoming, however, the Public Notice's proposal could create additional unintended consequences because it would be difficult for the FCC to administer, would create significant compliance challenges for regulated entities, and could disrupt the Commission's future Covered List use cases.

A. The Public Notice's Proposal Omits Critical Aspects of the BIS Rule's Framework.

The Public Notice proposes to add the BIS Rule's broad prohibition on covered software and VCS hardware transactions to the Covered List without including—and in many cases, even acknowledging—the exemptions, authorizations, and advisory opinions that are integral to the functionality of the BIS Rule and that form the contours of BIS' national security determination. For example, while the Public Notice notes that "the [BIS Rule] delays some of the transaction restrictions by several years," it nonetheless asserts that "the Commerce Department made a specific determination about unacceptable risks to national security that exist *at present*."[18] Indeed, the Public Notice contemplates updating the Covered List in short order without reference to the multi-year extensions in the BIS Rule.[19] This proposal would mean, for instance, that a model year 2028 vehicle that could lawfully be sold in U.S. markets under the BIS Rule could nonetheless be unavailable to U.S. consumers because the VCS hardware to be included in the vehicle is on the Covered List and therefore would not be able to obtain an equipment authorization.[20]

The Public Notice also makes no reference to the BIS Rule's framework for general and specific authorizations, nor does it acknowledge that this framework will be used to permit hardware or software that would otherwise be prohibited under the BIS Rule but for those

[18] Public Notice at 3 (emphasis added). For the reasons set forth in Section IV, *infra*, the BIS action does not actually constitute a "specific determination" as contemplated by the text of the statute. Any "specific determination" made by BIS must, in any event, be understood to include all of the exemptions, authorizations, and advisory opinions made by the agency.

[19] *Id*. at 3; *see id*. at 9-10, Appendix A.

[20] *See* 47 C.F.R. § 2.903(a) (prohibiting all equipment on the Covered List from obtaining an equipment authorization).

authorizations. Indeed, as explained above, BIS issued its first two general authorizations for limited use cases and temporary importations on June 10—both of which identify conditions on use or handling of the equipment that must be followed to meet BIS' criteria for the authorizations.[21] The Bureau's approach would mean that if BIS permitted a transaction either by general or specific authorization, thus allowing the import and sale of certain technologies or vehicles, those transactions may not be allowed to occur if a new FCC equipment authorization were required for the underlying hardware because a new authorization cannot be obtained for equipment on the Covered List.[22] And even if the FCC attempted to mitigate this concern by creating a process and hiring sufficient staff to consider requests or act *sua sponte* to exclude from the Covered List entities subject to general or specific authorizations, it is not clear that such action could be taken in a timely fashion—these delays could jeopardize product planning and investment.

The nature of the first general authorizations that BIS has issued underscores this point. Under General Authorization No. 1, BIS will allow otherwise prohibited transactions for limited use cases, including among other things where "the completed connected vehicle that incorporates covered software or VCS hardware *will be used on public roadways for fewer than 30 calendar days in any twelve-month period* starting from its first use on a public roadway[.]"[23] It is not clear how the Commission *could* accommodate this exception; to do so, it would need to

[21] *See General Authorizations*, BIS, https://www.bis.gov/oicts/connected-vehicles/general-authorizations (last visited June 24, 2025).

[22] *See Id*.

[23] General Authorization No. 1 (emphasis added); *see also* 15 C.F.R. §§ 791.300-791.321.

create a Covered List exemption that either only permitted use by a specific entity in a specific application, or that only allowed the equipment to be used less than one month per year.

The same is true of the BIS Rule's advisory opinion process, which the Public Notice likewise does not mention. Accordingly, a covered entity could obtain a determination that a particular transaction was not covered by the BIS Rule through a BIS advisory opinion, but ultimately not be able to deploy the technology in the U.S. because the entity could not obtain the requisite FCC equipment authorization. Accordingly, the Bureau's failure to incorporate the important elements that make the BIS Rule effective would render the proposal in the Public Notice unworkable, causing confusion for regulated entities and deterring investment in U.S. companies.

B. If Adopted, the Public Notice's Proposal Would Create Unintended Consequences That Could Complicate Implementation of and Compliance with the Covered List.

If the Public Notice's proposal were adopted, it could create further unintended consequences beyond its lack of consistency with the terms of the BIS Rule, including with the built-in flexibilities therein. Those consequences include complexities in administering this first-of-its-kind Covered List update as well as potential future FCC restrictions on the covered products, the companies that make them, and those who do business with them, each of which could affect relevant markets and supply chains in ways that BIS did not address or anticipate. These outcomes risk stymying American innovation and technology development, reducing U.S. competition and relevance in the global market, and jeopardizing some onboard safety and technology features in U.S. vehicles.

First, the Public Notice proposes to add entire technology/product categories to the Covered List, which to date has included only specific entities (*e.g.*, Huawei Technologies

Company and ZTE Corporation). This would create administrative challenges for a regime that has, to date, been relatively easy to administer and understand, and which has created an additional powerful tool in the toolbox to protect U.S. national security. Trying to apply the Covered List paradigm to broad categories of activity will inevitably lead to mismatches and confusion. For example, the Public Notice attempts to draw a distinction between Covered List-related regulations that apply to an entity that is "named" on the Covered List versus an entity that is "identified" on the Covered List through certain of that entity's equipment being included.[24] However, the rules referenced in the Public Notice were intended to address an entirely different distinction: the entities literally named on the Covered List, and the subsidiaries and affiliates *of those entities*, who are not included by name on the Covered List but nonetheless fall within its scope by virtue of their relationship to named entities. The Public Notice here suggests that producers of covered software and VCS hardware technology could simply be exempt from the requirements that apply to "named" entities, such as the obligation to submit subsidiary and affiliate information to the Commission.[25] But when it adopted this requirement, the Commission insisted that this obligation was essential to the administration of the simultaneously adopted prohibitions that apply to all "identified" entities:

> In implementing rules and procedures to prohibit authorization of such "covered" equipment produced by particular entities named on the Covered List and their associated entities (e.g., their respective subsidiaries and affiliates), we find that it is critical that the Commission, as well as applicants for equipment authorizations, [telecommunications certification bodies ("TCBs")], and other interested parties, have the requisite, transparent, and readily available information *of the particular entities that in fact are such associated entities of the named entities on the Covered*

[24] Public Notice at 6 (citing 47 C.F.R. §§ 2.903(b), 2.906(d), 2.907(c), 15.103(j), 8.204(c), 8.208(c)(2), 8.220(c)(7)).

[25] *Id*. (citing 47 C.F.R. § 2.903(b)).

> *List*. We find that having this information *on the names of such associated entities* promotes effective implementation of and compliance with the prohibition, by providing the Commission and TCBs in advance of reviewing any equipment authorization applications with a list of all those entities to which the Covered List applies.[26]

The Commission's *post hoc* redefinition of what it means to be "named" and "identified" on the Covered List to fit a novel, descriptive Covered List category is not as simple as the Commission would like it to be, and does not easily fit within the regulatory framework the agency sought to create. Similarly, the Commission claims that its prohibition on Covered List participation in the forthcoming Cyber Trust Mark program can be easily mapped on to the new proposed category; yet when it established the Cyber Trust Mark program (and anticipated the resources that would be necessary to administer it), the Commission only intended to apply the prohibition to entities expressly named on the Covered List for producing covered equipment, their subsidiaries and affiliates, and entities named on other relevant federal agency lists.[27]

Second, the Bureau proposes to make the VCS hardware prohibition turn on the "intended" use for the equipment, asserting that this would create a "narrower class of equipment[]" subject to the prohibition, and thus minimize undue burdens or unintended

[26] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, Report and Order, Order, and Further Notice of Proposed Rulemaking, 37 FCC Rcd 13493, ¶ 185 (Nov. 25, 2022) (emphasis added) (footnote omitted) ("Communications Supply Chain FNPRM").

[27] *Cybersecurity Labeling for Internet of Things*, Report and Order and Further Notice of Proposed Rulemaking, 39 FCC Rcd 2497, ¶ 33 (2024) (adopting proposal "to exclude from the IoT Labeling Program … any IoT device produced by an entity identified on the Covered List (i.e., *an entity named or any of its subsidiaries or affiliates*) as producing 'covered' equipment") (emphasis added) ("IoT NPRM").

consequences.[28] In practice, however, Covered List entities subject to analogous "use"-based restrictions have struggled to demonstrate to the Commission's satisfaction that a given piece of equipment is not being sold for a particular purpose.[29]

The challenges of an "intended use"-based restriction are compounded here, where covered software and VCS hardware regulated under the BIS Rule can still be utilized in vehicles not subject to the Rule. Specifically, the BIS Rule only applies to covered software and VCS hardware to the extent that such technology is "intended to be incorporated into a connected vehicle[.]"[30] The term "connected vehicle" is carefully defined, and – for example – intentionally does not include vehicles that operate solely on rail lines or that weigh over 10,000 pounds, which BIS intends to address in a future rulemaking.[31] Although the proposed update to the FCC Covered List in the Public Notice would incorporate the BIS definition of "connected vehicle" and therefore would account for this distinction, it remains to be seen how the Commission plans to do so in the implementation process. If the agency does not have a defined and reliable procedure for authorizing covered hardware intended for vehicles that fall outside the scope of the BIS Rule, it will restrict the market in ways BIS did not intend.[32]

[28] Public Notice at 5.

[29] *See, e.g.*, Letter from Andrew D. Lipman, Counsel for Dahua Technology USA Inc., to Jessica Rosenworcel, Chairwoman, FCC, ET Docket No. 21-232 (filed June 9, 2023).

[30] BIS Rule at 5375.

[31] *Id.*

[32] *See* 47 C.F.R. § 2.903(a) (prohibiting all equipment on the Covered List from obtaining an equipment authorization).

Third, the Public Notice does not attempt to reconcile the difference between the scope of products covered by the SNA and the BIS Rule. Under the SNA, the Covered List is to consist *solely* of "communications equipment or service[s]," which the Act defines as "any equipment or service that is essential to the provision of advanced communications service."[33] The SNA, in turn, states that "advanced communications service" has the meaning given to the term "advanced telecommunications capability" in 47 U.S.C. § 1302,[34] which under that statute "is defined, without regard to any transmission media or technology, as *high-speed, switched, broadband telecommunications capability* that *enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology*."[35]

The BIS Rule, meanwhile, applies to "covered software" and "VCS hardware." "Covered software" is defined as "the software-based components, including application, middleware, and system software, in which there is a foreign interest, executed by the primary processing unit or units of an item that directly enables the function of [VCS] or Automated Driving Systems at the vehicle level."[36] And "VCS hardware" is defined as:

> software-enabled or programmable components if they directly enable the function of and are directly connected to [VCS], or are part of an item that directly enables the function of [VCS], including but not limited to: microcontroller, microcomputers or modules, systems on a chip, networking or telematics units, cellular modem/modules, Wi-Fi microcontrollers or modules, Bluetooth microcontrollers or modules, satellite communication systems, other wireless

[33] 47 U.S.C. § 1608(4).

[34] *Id.* § 1608(1).

[35] *Id.* § 1302(d)(1) (emphasis added).

[36] 15 C.F.R. § 791.301.

> communication microcontrollers or modules, external antennas, digital signal processors, and field-programmable gate arrays.[37]

The categories of hardware and software covered by the BIS Rule are therefore far broader than what the SNA has authorized the Commission to place on the Covered List. The BIS Rule does not require that the hardware or software it covers be "essential to the provision of advanced communications service,"[38] and in fact these technologies often are designed to perform functions that are unrelated to the provision of such services.

Accordingly, it is unclear whether the FCC has the statutory authority under the SNA to place "covered software" and "VCS hardware" on the Covered List as currently defined, and the Public Notice does not attempt to grapple with this issue. And even if these additions were somehow legally permissible, the Public Notice's proposal would likely create confusion for the automotive industry given the clear disparity between these product categories and the scope of the SNA. These challenges would make compliance with the rules proposed by the Bureau and the BIS Rule burdensome and complicated.

Fourth, the FCC continues to expand *how* the Covered List is used, which could create significant unintended consequences that impose prohibitions and limitations far beyond what BIS envisioned. To date, Congress has directed the FCC to use the Covered List in two contexts: (1) establishing a prohibition on using federal Universal Service funding for entities to purchase, rent, lease, or maintain equipment on the Covered List;[39] and (2) establishing a prohibition on

---

[37] *Id.*

[38] 47 U.S.C. § 1608(4).

[39] *Id.* § 1602(a)(1)(A).

reviewing or approving equipment authorization applications pertaining to equipment on the Covered List.[40] However, the Commission has taken unilateral action to use or propose to use the Covered List in numerous other ways, including: (i) banning Covered List entities from serving as labs and other relevant bodies in FCC equipment certification;[41] (ii) banning Covered List entities from participating in the forthcoming Cyber Trust Mark program;[42] (iii) proposing to ban or require accounting of component parts produced by Covered List entities in the equipment authorization process;[43] (iv) proposing to revoke existing equipment authorizations held by Covered List entities;[44] and (v) proposing to amend various licensing regimes to require either disclosing or not using Covered List equipment.[45] Depending on the path the FCC takes with its various Covered List initiatives, even a connected vehicles rule that attempts to be coextensive

[40] 47 U.S.C. § 1601 note (Updates to Equipment Authorization Process of Federal Communications Commission).

[41] *Promoting the Integrity and Security of Telecommunications Certification Bodies, Measurement Facilities, and the Equipment Authorization Program*, ET Docket No. 24-136, Report and Order and Further Notice of Proposed Rulemaking, FCC 25-27 (rel. May 27, 2025).

[42] IoT NPRM ¶ 15.

[43] Communications Supply Chain FNPRM ¶¶ 277-87.

[44] *Id.* ¶ 288.

[45] *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, Notice of Proposed Rulemaking, 39 FCC Rcd 12730, ¶ 85 (2024); *Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, Order and Notice of Proposed Rulemaking, 38 FCC Rcd 4346, ¶ 124 (2023).

with the BIS Rule could become vastly more restrictive over time, falling out of alignment with BIS' determinations.

At a minimum, the Public Notice's proposal to include entire technology and/or product categories on the Covered List (rather than specific, named entities) could complicate the Commission's ability to use the Covered List in other contexts going forward. This is particularly true given that the Commission's action here could serve as a model for how it incorporates future ICTS rules from BIS.[46] Further complicating this, as BIS addresses additional ICTS threats, the Commission could rapidly face pressure to add additional technologies and product categories to the Covered List, swelling the range of those entities "identified" on the Covered List considerably. Accordingly, the FCC should exercise significant caution before taking a step this significant.

IV. THE SNA DOES NOT REQUIRE AN UPDATE TO THE COVERED LIST BASED ON THE DETERMINATIONS IN THE BIS RULE.

The SNA does not require that the FCC update the Covered List based on the BIS Rule, because the BIS Rule does not involve a "specific determination." As the Public Notice explains, the SNA requires the FCC to update the Covered List based on the determinations made by certain federal entities enumerated in the statute.[47] While the Bureau is correct that the

[46] In February of this year, BIS published an advance notice of proposed rulemaking in the Federal Register that "seeks public input on . . . certain definitions and BIS's assessment of how a class of transactions involving foreign adversary ICTS integral to UAS could present undue or unacceptable risks to U.S. national security and to the security and safety of U.S. persons." *Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems*, Advance Notice of Proposed Rulemaking, 90 Fed. Reg. 271, 273 (Jan. 3, 2025).

[47] *See* Public Notice at 1; 47 U.S.C. § 1601.

Commerce Department made a "determination" pursuant to Executive Order 13873 the Bureau is incorrect that "the Commerce Department made a *specific* determination about unacceptable risks to national security" in promulgating the BIS Rule.[48] It is only a "specific determination" made pursuant to the statute that triggers an obligation to update the Covered List.[49]

"Specific determination" is not defined in the SNA, nor is it used in the governing Executive Order. Applying ordinary tools of statutory construction, however, it is clear that the term does not cover the determination in the BIS Rule. The rule against surplusage counsels that "specific determination" has an independent meaning that is not coextensive with "determination," or else there would be no need to use both words.[50] Put another way, a "determination" that the Secretary makes under the Executive Order—such the determination underlying the BIS Rule—is not necessarily a "specific determination" for purposes of the FCC's Covered List obligation.

Turning to what constitutes a "specific determination," the structure and history of the Covered List counsel in favor of the idea that it means a finding that names an individually identifiable entity. Congress has never authorized the FCC to add whole product categories to the Covered List, and the FCC concedes that it has never attempted to do so; historically, all of the entities added by the SNA itself and by the FCC pursuant to the SNA's direction have been specifically and individually enumerated. Moreover, the Supreme Court's decision in *Loper*

[48] Public Notice at 3 (emphasis added).

[49] 47 U.S.C. § 1601(c).

[50] *See, e.g., Williams v. Taylor*, 529 U.S. 362, 364 (2000) (It is a "cardinal principle of statutory construction that courts must give effect, if possible, to every clause and word of a statute[.]").

Bright Enters. v. Raimondo dictates that Commission decisions must cohere with the best reading of the statute—a determination that is no longer subject to judicial deference.[51] Here, the structure and operation of the Covered List, the applicable canons of construction, and the absurd results that would flow from a contrary conclusion dictate that the best reading of the SNA is that a "specific determination" includes only those determinations that enumerate particular entities or products. In the context of the BIS Rule, such determinations could come through advisory opinions, enforcement actions, or other actions by BIS involving named entities.

Even assuming that "specific determination" could be read to encompass a product category of non-individually-identifiable entities, that "determination" cannot be understood without the context provided in the BIS Rule. And because the BIS has adopted exemptions that prevent the Rule from taking effect for years and contemplates a range of general and specific authorizations and advisory opinions, no final "specific determination" has been made with respect to covered software and VCS hardware generally. It is only once those exemptions expire and BIS has issued those general and specific authorizations and advisory opinions that the FCC could be obligated to update the Covered List based on the presence of a "specific determination." And that eventual "specific determination" that the equipment "poses an unacceptable risk to [U.S.] national security" would apply *only* insofar as the identified risks had not been appropriately addressed, as set forth in a specific or general authorization or an advisory opinion.

[51] 603 U.S. 369, 373 (2024).

V. SHOULD THE FCC DECIDE TO MOVE FORWARD WITH THE PUBLIC NOTICE'S PROPOSAL, IT MUST REFINE THE PROPOSAL TO MINIMIZE POTENTIAL HARMS AND UNINTENDED CONSEQUENCES.

For the reasons set forth above, the FCC should not update the Covered List now. If the Commission decides to proceed with the Public Notice's proposed update to the Covered List based on the BIS Rule, though, it must ensure that this update: (i) captures the key elements of the BIS Rule, including exemptions, general and specific authorizations, and advisory opinions; and (ii) does not create restrictions on product imports or sales that exceed those imposed by BIS, including as FCC regulations evolve to use the Covered List in different contexts. To achieve these objectives, Auto Innovators proposes the following changes to the Covered List updates proposed in Appendix A of the Public Notice—

> "Automated driving systems and completed connected vehicles designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region, (PRC), or the Russian Federation (Russia)**—but only to the extent such systems and vehicles would be prohibited from import or sale by Department of Commerce regulations as implemented by the Department of Commerce (including, for example, transition periods, specific and general authorizations, and advisory opinions).****"
>
> "Vehicle connectivity systems (VCS) hardware designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia and intended to be included within a completed connected vehicle in the United States; or VCS hardware with integrated covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia**—but only to the extent such hardware would be prohibited from import or sale by Department of Commerce regulations as implemented by the Department of Commerce, (including, for example, transition periods, specific and general authorizations, and advisory opinions).****"
>
> "** This entry on the Covered List relies on the definitions set out in Department of Commerce regulations. *See* 15 C.F.R. § 791.301 (providing definitions of "automated driving system," "completed connected vehicle," "covered software," "vehicle connectivity system," "VCS hardware," and "person owned by, controlled

by, or subject to the jurisdiction or direction of a foreign adversary"). **Systems, hardware, and vehicles that are subject to an exemption, advisory opinion, general authorization, or specific authorization pursuant to Department of Commerce regulations (*see* 15 C.F.R. §§ 791.306-791.308, 791.310) are not included in this entry. This entry covers the identified systems, vehicles, and hardware; entities that design, develop, manufacture, or supply products that fall within this entry are not "named" or "identified" on the Covered List for purposes of FCC regulations.**"

These suggested changes *only* address the discontinuity between the scope of the language proposed and the BIS Rule. They do not address other potential challenges with the Bureau's proposal, including the use of "intended" and any discrepancies between the categories identified and the statutory limitations on the scope of the Covered List, as discussed in Section III, *supra*.

Further, even if the Commission decides to proceed with the update of the Covered List, it need not and should not do so on an expedited basis, as the timing of the Public Notice suggests. Rather, Auto Innovators encourages the Commission to take the time necessary to analyze *all* potential impacts of the Public Notice's proposed inclusion of broad product categories on the Covered List—including those that may not be addressed by Auto Innovators' proposed changes. When BIS developed the BIS Rule, it undertook a multi-year process with careful consideration of stakeholder input. The agency did so because these issues are complex, and the unintended consequences that could flow from the rulemaking could have substantial impacts on the U.S. economy, American technological leadership, national security, and American motorists.

Accordingly, the Commission must ensure that it carefully considers—through an interagency process with BIS and other national security agencies—whether and how the Covered List should be updated, taking into account these factors when doing so. The Commission also must ensure that it has sufficient resources to administer the revised Covered

List. Indeed, once the Covered List is updated for consistency with the BIS Rule, the FCC may need to significantly expand of the budget and FCC staff dedicated to administering the Covered List given the expected changes to the BIS prohibitions to be effectuated through authorizations and advisory opinions.

Taking these steps of interagency coordination and resource management is especially important because, as noted in Section IV above, BIS is already considering adopting additional ICTS regulations similar to the connected vehicle Rule. That includes a potential rule on commercial vehicles, which may involve some or all of the same equipment covered by the connected vehicle rule, but it also includes a variety of potential other rules applying to other sectors and technologies, like drones, routers, and mobile access terminals. As damaging as a hasty decision on the Public Notice could be to the automotive industry and American consumers in this proceeding, the precedent established here may also have long-term impacts on sectors across the U.S. economy.

VI. CONCLUSION

In light of the foregoing, Auto Innovators strongly urges the Commission to refrain from taking any action at this time to update the Covered List based on the BIS Rule. Auto Innovators instead encourages the Commission to work collaboratively with BIS and other national security agencies to identify threats to U.S. national security, and to only update the "Covered List" when "specific determinations" under the SNA have been made. Auto Innovators is pleased to serve as a resource for the Commission as it continues to consider national security issues in the connected vehicle space, and looks forward to future discussions with the agency about this important topic.

Respectfully submitted,

Hilary Cain
Senior Vice President, Policy

Sarah Puro
Vice President, Safety and Technology Policy

Tara Hairston
Senior Director, Technology Policy

Alliance for Automotive Innovation
1050 K Street NW, 6th Floor
Washington, DC 20001

/s/ Sara M. Baxenberg
Sara M. Baxenberg
Joshua S. Turner
Stephen J. Conley

Wiley Rein LLP
2050 M Street NW
Washington DC

Counsel for Alliance for Automotive Innovation

June 27, 2025