Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Petition for Rulemaking and Request for	)	
Emergency Stay of Operation of Dedicated Short-	)	
Range Communications Service in the 5.850-	)	
5.925 GHz Band (5.9 GHz Band)	)	RM-11771

OPPOSITION TO PETITION FOR RULEMAKING AND REQUEST FOR EMERGENCY STAY OF OPERATION

Ari Q. Fitzgerald, Esq.
Wesley B. Platt, Esq.
Hogan Lovells LLP
Columbia Square
555 13th Street, NW
Washington, D.C. 20004

Attorneys for the Alliance of Automobile Manufacturers

James Arden Barnett, Jr., Esq.
Ian D. Volner, Esq.
Stephen R. Freeland, Esq.
Cristina I. Vessels, Esq.
Venable LLP
575 7th Street, NW
Washington, D.C. 20004

Attorneys for the Association of Global Automakers, Inc.

Robert B. Kelly
Koyulyn Miller
Squire Patton Boggs (US) LLP
2550 M Street, NW
Washington, D.C. 20037

Attorneys for The Intelligent Transportation Society of America

August 24, 2016

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Petition for Rulemaking and Request for	)	
Emergency Stay of Operation of Dedicated Short-	)	
Range Communications Service in the 5.850-	)	
5.925 GHz Band (5.9 GHz Band)	)	RM-11771

OPPOSITION TO PETITION FOR RULEMAKING AND REQUEST FOR EMERGENCY STAY OF OPERATION

The Alliance of Automobile Manufacturers (the "Alliance")[1], the Association of Global Automakers ("Global Automakers")[2] and the Intelligent Transportation Society of America ("ITS America")[3] submit this opposition to the petition for rulemaking and request for emergency stay (the "Petition") filed by Public Knowledge and Open Technology Institute at New America

[1] The Alliance is an association of 12 vehicle manufacturers which account for roughly 77percent of all car and light truck sales in the United States. These members are BMW Group, FCA US LLC, Ford Motor Company, General Motors, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche Cars North America, Toyota, Volkswagen Group of America, and Volvo Car USA. *See* http://www.autoalliance.org/members.

[2] Global Automakers represents international motor vehicle manufacturers, original equipment suppliers, and other automotive-related trade associations. Our motor vehicle manufacturer members include American Honda Motor Co., Aston Martin Lagonda of North America, Inc., Ferrari North America, Inc., Hyundai Motor America, Isuzu Motors America, Inc., Kia Motors America, Inc., Maserati North America, Inc., McLaren Automotive Ltd., Nissan North America, Inc., Subaru of America, Inc., Suzuki Motor of America, Inc., and Toyota Motor North America, Inc. *See* http://www.globalautomakers.org/members.

[3] ITS America is an association of public and private organizations that are focused on advanced vehicle technology, smart cities, and new models for mobility. Our members include auto, telecomm, traditional IT and emerging tech, and consumer apps and industrial electronics. We also include public agencies and non-profits, such as road, transit and other transportation infrastructure operators and the research community focused on bringing new technology from the lab to our roads, cars, buses and trucks.

(collectively, the "Petitioners") in the above-captioned proceeding.[4] As explained below, both of the Petitioners' requests are without merit, and the Petition should be denied.

I. INTRODUCTION AND SUMMARY.

The Federal Communications Commission ("FCC" or "Commission") should deny the Petitioners' request to conduct a rulemaking to establish privacy and cybersecurity rules for Dedicated Short Range Communications ("DSRC") in the 5.850-5.925 GHz ("5.9 GHz") band in light of the nature of DSRC service and role of other federal agencies in the sphere.[5] DSRC systems for vehicle to vehicle communications ("V2V") do not collect, transmit, or store any information that is linkable to a particular person or vehicle and thus do not raise consumer privacy issues or implicate the Commission's Customer Proprietary Network Information ("CPNI") or proposed Customer Proprietary Information ("CPI") rules. Furthermore, they already incorporate robust cybersecurity protections. Meanwhile, other federal agencies, such as the National Highway Traffic Safety Administration ("NHTSA") and Federal Trade Commission ("FTC"), already regulate privacy and cybersecurity as they relate to the automobile manufacturers in general.

The Commission should also deny the Petitioners' request for an "emergency stay" of the operation of DSRC services in the 5.9 GHz band. The Petitioners' request is fatally flawed because it was not filed as a separate pleading as required by the Commission's rules and fails to identify a Commission "decision or order" to stay. In addition, the Petitioners fail to meet their burden under the four-factor test applied by the Commission when determining whether to stay the

[4] Public Knowledge and Open Technology Institute at New America, Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.925 GHz Band (5.9 GHz Band) (filed June 28, 2016) ("Petition"); *see also Consumer & Governmental Affairs Bureau Reference Information Center Petition for Rulemaking Filed*, Public Notice, RM-11771 (rel. July 25, 2016).

[5] The Petition indicates that a stay is requested for the "5.850-5.9925" GHz band. Petition at 1. We assume that the Petitioners meant the "5.850-5.925" GHz band.

effectiveness of one of its orders. Irreparable harm would not occur if the Commission were to deny the Petitioners' request for a rulemaking, and the request is unlikely to prevail on the merits. At the same time, other interested parties would be harmed by a stay, and a stay would not be in the public interest.

Congress, the Commission, state highway authorities, and federal agencies with primary jurisdiction over national transportation matters have repeatedly concluded that DSRC is integral to the deployment of Intelligent Transportation Systems ("ITS") and best suited to achieving the public safety and related national transportation goals that underlie this national initiative. The Commission should not deliberately halt or otherwise compromise the significant progress with respect to DSRC made to date, which is described in detail in the comments and reply comments recently filed by these parties and others in response to the Commission's request to refresh the record on 5.9 GHz issues in the pending 5 GHz proceeding.[6]

II. THE COMMISSION SHOULD DENY THE PETITIONERS' REQUEST TO INITIATE A RULEMAKING.

A. DSRC Systems Already Include Robust Privacy and Cybersecurity Protections.

1. DSRC Design and Existing Protections.

Privacy and security are fundamental to the design of DSRC systems, which have multiple layers of safeguards built in to protect those interests. DSRC communications for V2V are designed not to collect or transmit Personally Identifiable Information ("PII"), as the Commission

[6] *See, e.g.*, Comments of the Alliance, Global Automakers, Intelligent Transportation Society of America, and Denso International America, Inc., ET Docket 13-49, at 13-14, 18-25 (July 7, 2016) ("Alliance *et al*. 5.9 GHz Refresh Comments"); Reply Comments of the Alliance, Global Automakers, Intelligent Transportation Society of America, and Denso International America, Inc., ET Docket 13-49 (July 22, 2016) ("Alliance *et al*. 5.9 GHz Refresh Reply Comments").

has proposed to define that term.[7] In fact, DSRC communications do not contain any information that can be linked to an individual or vehicle, as described in greater detail below.[8] Moreover, a Public Key Infrastructure ("PKI") based security system has been carefully designed to protect DSRC security. This system is referred to as a Security Credential Management System ("SCMS"). NHTSA has announced plans to require the use of this system as part of its expected V2V regulation,[9] and General Motors will utilize it for its production V2V system.

The SCMS has incorporated security and privacy by design in the following manner. Along with transmitting Basic Safety Messages ("BSMs"), vehicles attach with their BSMs a certificate from the SCMS and a digital signature of the BSM. This authenticates to a receiving vehicle that the message was sent from a certified device and was unchanged from transmission to reception. Moreover, the certificates are not linked in any way to the Vehicle Identification Number ("VIN") of the transmitting vehicle or any other PII.[10] Additionally, neither the VIN nor any PII is included in the BSM.[11]

In other words, V2V messages sent over DSRC must have certificates as part of a "trust system." In effect, without a valid certificate, messages transmitted over DSRC will not be accepted by others operating in the network. This is true for every device on the DSRC network,

---

[7] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 ¶¶ 60-66 (2016) ("*Broadband Privacy NPRM*").

[8] *See* Section II.C, *infra*.

[9] *See* NHTSA, *Vehicle-to-Vehicle Security Credential Management System*, Request for Information, 79 Fed. Reg. 61927 at 61929 (2014).

[10] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 ¶¶ 60-66 (2016) ("*Broadband Privacy NPRM*").

[11] *See, e.g.*, NHTSA, *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*, DOT HS 812 014, at 145 (2014), *available at* http://bit.ly/1BtNawA ("V2V Readiness Report") (last visited Aug. 24, 2016).

whether the device is from an original equipment manufacturer ("OEM"), an after-market product, or a roadside device.

To ensure privacy and prevent system attacks by SCMS outsiders, the certificates are changed frequently and at random intervals, for example every five minutes. To ensure privacy and prevent attacks by SCMS insiders, operation of key SCMS components are separated if the combined information held by the components would allow the organization to track a vehicle. The design of the SCMS includes safeguards against any one person or operating unit of the SCMS knowing the set of certificates that belong to a single vehicle, even if there is a corrupt insider at the SCMS or an SCMS's database is breached.

2. Continuing Industry and Government Efforts.

Privacy and security have both played an important role throughout the development and design of the DSRC technology. In addition, the automobile industry, federal government, and other stakeholders continue to devote substantial resources to protecting DSRC systems and users from privacy and security risks. In fact, the automotive industry in particular has taken many steps to ensure that communications over DSRC are safe and secure and that privacy is protected.

For example, for the non-DSRC automobile-based services (such as telematics and infotainment services) that do have the ability to generate PII, the automotive industry has adopted detailed privacy and security principles, including those related to: transparency, respect for content, and data security.[12] These principles apply to the collection, use, and sharing of covered

[12] Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc., *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services* (Nov. 12, 2014), *available at* http://www.autoalliance.org/index.cfm?objectid=CC629950-6A96-11E4-866D000C296BA163 (last visited Aug. 24, 2016).

information available on cars and light trucks sold or leased to consumers in the United States.[13] Participating Global Automakers and Alliance members committed to implementing these principles for new vehicles manufactured no later than Model year 2017.[14] Although, as noted above, DSRC systems for V2V are designed not to generate PII, these efforts relating to systems that have the potential to do so are instructive as to the industry's proactive efforts in this area.

The automotive industry has also developed a cybersecurity guidebook for cyber-physical vehicle systems, which establishes a set of high-level guiding principles for identifying and assessing cybersecurity threats and ensuring that vehicle systems are secure.[15] It is also in the process of developing a common set of security requirements for vehicles, which will identify the criteria that allows hardware platforms to serve as the basis for security enhanced applications in vehicles.[16] In 2015, automobile manufacturers established an Automotive Information Sharing and Analysis Center ("Auto-ISAC") to facilitate the exchange of important cyber threat information and countermeasures in real-time.[17] In addition, the Auto-ISAC has developed an Automotive Cybersecurity Best Practices to further enhance the design of vehicle systems and help protect against potential cybersecurity threats specific to the motor vehicle ecosystem.

---

[13] *Id*. at 1.

[14] *Id*. at 3, 13.

[15] *See* SAE International, Vehicle Cybersecurity Systems Engineering Committee, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, Standard J3061_201601, *available at* http://standards.sae.org/j3061_201601/ (last visited Aug. 24, 2016).

[16] *See* SAE International, Vehicle Electrical System Security Committee, *Requirements for Hardware-Protected Security for Ground Vehicle Applications*, Standard J3101, *available at* http://standards.sae.org/wip/j3101/ (last visited Aug. 24, 2016).

[17] *See* the Alliance, *Cybersecurity: An Industry-Wide Effort to Identifying Emerging Threats and Potential Adversaries, available at* http://www.autoalliance.org/auto-issues/cybersecurity (last visited Aug. 19, 2016).

In addition, the automotive industry continues to partner with the federal government to develop a credentialing system that uses PKI, anonymized certificates, pseudonym certificates, certificate authorities, and a distributed system of Registration Authorities and Linkage Authorities. Working together, we have proposed a final design of the SCMS, including the system architecture, key use cases, system components and operations, and network and hardware requirements.[18] We are currently engaged in SCMS proof-of-concept implementation, and this work is supported by the U.S. Department of Transportation ("USDOT") under a Cooperative Agreement.[19]

Meanwhile, all of the major connected vehicle pilot deployments will have full end-to-end DSRC security implementation based on the standardized SCMS design and the requirements specified in Institute of Electrical and Electronics Engineers ("IEEE") and Society of Automotive Engineers ("SAE") standards. These include the pilot deployments in Ann Arbor, Michigan; Tampa, Florida; New York City; and Wyoming.[20] The upcoming Columbus, Ohio Smart City Challenge pilot deployment will involve 3,000 DSRC vehicles that also will operate using the same SCMS design and implementation.[21]

---

[18] *See, e.g.*, Crash Avoidance Metrics Partnership ("CAMP") Vehicle Safety Communications 3 Consortium, Final Report, *Technical Design of the Security Credential Management System* (2014), *available at* https://www.regulations.gov/document?D=NHTSA-2015-0060-0004 (last visited Aug. 24, 2016).

[19] *See, e.g.*, CAMP Vehicle Safety Communications 5 Consortium, *Security Credential Management System Proof-of-Concept Implementation: EE Requirements and Specifications Supporting SCMS Software Release 1.1* (2016), *available at* http://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf (last visited Aug. 24, 2016).

[20] *See, e.g.*, Alliance *et al*. 5.9 GHz Refresh Comments at 13-14, 18-25.

[21] *See, e.g.*, City of Columbus, Ohio, Smart City Application, at 29 (2016), *available at* http://www.eenews.net/assets/2016/03/31/document_pm_02.pdf (last visited Aug. 24, 2016).

Finally, as discussed in greater detail below, NHTSA has taken an active role in addressing potential privacy and security vulnerabilities for V2V. In addition to its regulatory efforts, for example, NHTSA released a Request for Information ("RFI") in 2014 that seeks information related to the security system that will support V2V operations but will not be established by NHTSA regulation.[22] NHTSA has also funded projects to build a verified message parser for DSRC, anomaly detection, and secure firmware updates.[23]

B. The Petitioners Grossly Exaggerate the Security Risks Posed by DSRC by Mischaracterizing How it Functions.

NHTSA's *V2V Readiness Report* notes that researchers assumed that cybersecurity is an existing vector of risk, and "not a new one created by V2V technologies."[24] While the emergence of V2V technology necessitates unique security standards such as those created and implemented by the IEEE 1609 Working Group, it does not create a new type of risk that did not previously exist.

The Petitioners' claim that "vulnerabilities will only increase" as a result of DSRC technology indicates their fundamental misunderstanding of the difference between overall vehicle cybersecurity and DSRC-specific security. DSRC technology is engineered with stringent security features in accordance with the IEEE 1609 standards; it is designed to intercept and minimize

---

[22] *See* NHTSA, *Vehicle-to-Vehicle Security Credential Management System*, Request for Information, 79 Fed. Reg. 61927 (2014).

[23] *See* UMTRI, *Automotive Cybersecurity Trends in the USA – Vehicle-to-Vehicle Communication*, Vector Cybersecurity Symposium (June 23, 2016), at 17, *available at* https://vector.com/portal/medien/cmc/events/commercial_events/vses16/lectures/vSES16_06_Weimerskirch.pdf (last visited Aug. 24, 2016); *see also generally* SAE & UMTRI, *New NHTSA Cybersecurity Research Projects: Anomaly Detection Systems, Cybersecurity Considerations for Heavy Vehicles, and Cybersecurity of Firmware Updates*, *available at* http://www.nhtsa.gov/DOT/NHTSA/NVS/Public%20Meetings/SAE/2016/SAE%20G_I_Workshop%20-%20UMTRI%20Carter.pdf (last visited Aug. 24, 2016).

[24] *V2V Readiness Report* at 134.

cyber threats before they can enter a vehicle system. Therefore, while DSRC technology cannot (and was never intended to) prevent all cyber threats from accessing vehicle systems through other entry points, the technology itself, and its V2V communication function, do not heighten the risk of cyber-attack.

The Petitioners also assert that the Commission should amend the service rules for DSRC to "reflect the need for cybersecurity protections for wireless networks."[25] However, research conducted through the USDOT shows that DSRC technology "has more security and privacy protections than traditional Wi-Fi."[26] For example, DSRC is the only wireless protocol that mandates the use of PKI to secure the communication channel.[27] In contrast, Wi-Fi uses symmetric cryptography with pre-shared keys, which is significantly less secure.[28]

Similarly, the Petitioners incorrectly assume that DSRC units will "provide an access route for malware to spread directly from car to car." To the contrary, DSRC V2V systems are carefully designed to accept only a single input, the BSM, along with the associated digital signature and security certificate. At the input stage, a parser is incorporated to verify that the message meets all requirements. Messages which do not meet all requirements are immediately discarded, before the message content is passed into the vehicle network. Because of this, it is highly unlikely that a V2V system could generate the apocalyptic scenario imagined by the Petitioners.

---

[25] Petition at 5.

[26] U.S. Department of Transportation, *Connected Vehicles and Our Privacy*, at 1, *available at* http://www.its.dot.gov/factsheets/pdf/Privacy_factsheet.pdf (last visited Aug. 19, 2016) ("*Privacy Factsheet*").

[27] *See supra* Section II.A.1.

[28] *See, e.g.*, Synopsys, *Securing the Internet of Things*, at 13 (2016), *available at* https://hosteddocs.emediausa.com/arc_security_iot_wp.pdf (last visited Aug. 24, 2016); *Privacy Factsheet* at 1.

Moreover, although the Petitioners claim that "over the last year, a number of high profile hacking incidents have occurred," there has only been one widely-publicized incident, and that incident was caused by researchers who worked full-time for an entire year to hack their own vehicle.[29] This "incident" was the result of a year-long research project, not a genuine hacking incident and did not involve DSRC.

C. The Commission's CPNI Rules and Proposed CPI Rules Are Inapposite Because DSRC Does Not Collect, Transmit, or Store Information that is Linkable to an Individual or a Vehicle.

Conceding that Section 222 of the Communications Act and the Commissions' CPNI and Pretext Rules do not apply to DSRC,[30] the Petitioners nonetheless insist that the Commission's *Pretexting Order*[31] provides the policy foundation, and presumably the authority, for the FCC to adopt DSRC privacy rules.[32] The Petitioners are wrong.

The justification for the Commission's CPNI rules is based on the nature of the relationship between a common carrier or service provider and its customers. In such relationships, the service provider inevitably comes into possession of information (*e.g.* extent of usage, numbers called, and call durations) about the customer, the unwarranted disclosure of which would be harmful or, at the very least, potentially embarrassing to the customer.[33] Thus, the foundation of the CPNI

[29] Petition at iii, iv.

[30] Petition at viii, 21.

[31] *Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) ("*Pretexting Order*").

[32] *See* Petition at 10-11, 21.

[33] *Pretexting Order* ¶¶ 5, 8 n.16.

rules is to protect PII of a sensitive nature. Indeed, the definition of CPNI is carefully framed in terms of sensitive and PII and specifically excludes aggregate data.[34]

The CPNI rules are inapposite and inapplicable to DSRC because DSRC communications do not capture or transmit CPNI. Further, DSRC does not entail the use of the voice or data public switched telephone network, broadband network, or any other common carrier-like communications network. DSRC also does not involve the collection, storage, or transmission of any information about a consumer's use of or subscription to a "telecommunication service," "telephone exchange service," or "telephone toll service."[35] Instead, DSRC for V2V entails the closed circuit transmission of information related to the "safe and efficient" use of the nation's streets and highways,[36] which the Commission has recognized since allocating spectrum for DSRC.[37]

Indeed, DSRC messages for V2V do not contain **any** information that can be linked to a specific individual or even to a specific DSRC-equipped vehicle. DSRC for V2V does not involve the collection, transmission, or storage of any PII. This means that DSRC does not raise any of the concerns that the Commission has sought to address in its ongoing broadband privacy

[34] *Pretexting Order* ¶¶ 4 n.7, 5, and 6.

[35] *See* 47 U.S.C. § 222(h); 47 C.F.R. § 64.2003.

[36] Intermodal Surface Transportation Efficiency Act of 1991 ("ISTEA"), 105 Stat. 1914, 102 P.L. 240, at § 6052(b); *see also* Alliance *et al*. 5.9 GHz Refresh Reply Comments.

[37] *See Amendment of Parts 2 and 90 of the Commission's Rules to Allocate the 5.850-5.925 GHz Band to the Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Services*, Notice of Proposed Rulemaking, 13 FCC Rcd 14321 ¶ 7 (1998) (observing that DSRC would be used "to increase the safety and efficiency of the Nation's transportation infrastructure").

rulemaking.[38] It also means that, even if the Commission adopts the CPI rules proposed earlier this year, they too would be inapplicable to DSRC.[39]

D. Other Federal Agencies Already Regulate DSRC Privacy and Security.

The Commission should also deny the Petitioners' request to initiate a rulemaking because other federal agencies are already addressing the DSRC privacy and security issues. The Commission has committed to ensuring that its rules do not overlap, duplicate, or conflict with other federal rules.[40] Indeed, the Commission regularly relies on the "expertise and experience" of other federal agencies "to avoid duplicative and overly burdensome regulation."[41] In this case, NHTSA and the FTC already play an active role in protecting DSRC systems from privacy and security risks, and if the Commission were to grant the Petitioners' request, it would risk creating burdensome regulations that would not advance the public interest but would be duplicative of the work done already by other agencies.

1. The National Highway Traffic Safety Administration.

NHTSA has expressed its intent to be the primary regulator of DSRC security. In fact, it has already begun a thorough and rigorous examination of whether there really is a cognizable security threat. For example, NHTSA is "finalizing the [DSRC] architecture and ha[s] research plans to conduct full-scale vulnerability testing and to address any security issues that emerge from

[38] *See, e.g., id*. ¶¶ 1-13.

[39] *See id*. ¶¶ 14-26. The Commission has proposed to include within the definition of "CPI" both CPNI and PII. *See id*. ¶ 15.

[40] *See, e.g., Final Plan for Retrospective Analysis of Existing Rules*, Public Notice, at 2-3, 11-13, 2012 WL 1851335 (2012).

[41] *Id*. at 11.

that testing."[42] NHTSA also plans to propose and seek comment on various aspects of the DSRC architecture, including the protocols that will ensure security, in its pending rulemaking to require DSRC in all new light vehicles.[43]

In addition, NHTSA has committed to regulating V2V technologies in a way that protects individual privacy.[44] NHTSA considers the Vehicle Infrastructure Integration Consortium's ("VIIC") 2007 Privacy Policies Framework[45] to be a "useful starting point" but plans to modify its approach in the rulemaking to account for advances in technology that have occurred since the framework's release.[46] NHTSA has also pledged to "continue to work with the [USDOT's] Privacy Officer and Office of the General Counsel to assess and reassess any threats to privacy that may be introduced by V2V technology and help identify mitigation measures to minimize any such risks."[47]

Importantly, NHTSA's legal authority to regulate automobile manufacturers in their provision of DSRC is clear. As NHTSA recently acknowledged in an Enforcement Guidance Bulletin concerning "Safety-Related Defects and Emerging Automotive Technologies," its "broad enforcement authority" to investigate, penalize, and potentially mandate recalls involving emerging technologies is no different than its authority with respect to conventional motor vehicle

---

[42] NHTSA, *NHTSA and Vehicle Cybersecurity*, *available at* http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity (last visited Aug. 18, 2016).

[43] *See id*.

[44] *See V2V Readiness Report* at 147.

[45] *See* VIIC, Privacy Policies Framework Version 1.0.2 (2007), *available at* http://bit.ly/2b9zQX6 (last visited Aug. 24, 2016).

[46] *See V2V Readiness Report* at 147-48.

[47] *Id*. at 148.

components.[48] Similarly, manufacturers have the same reporting and notification responsibilities with respect to safety-related defects in these technologies, such as DSRC. By contrast, the FCC's legal and practical authority to impose privacy and cybersecurity obligations on automobile manufacturers in their provision of DSRC is less clear because DSRC does not entail the use of spectrum to operate any conventional telecommunications networks and because, under the Part 95 license-by-rule licensing scheme, automobile manufacturers will generally not be DSRC "licensees" and may not be DSRC equipment manufacturers.[49]

The fact that DSRC is an integral part of the ITS reinforces the conclusion that issues related to privacy and security with respect to DSRC should be left primarily to NHTSA. The USDOT has spent nearly $25 million in researching, designing, and developing increased safety measures and operational protocol for ITS systems.[50] The industry has spent at least that much and considerably more in the development of the certification and related protective measures that it has designed into the system from the inception. After more than a decade and a half of development, and regulatory oversight, USDOT notes that DSRC "is a wireless technology that has more security and privacy protections than traditional Wi-Fi."[51] Accordingly, any action taken by the FCC which lends credence to the unsupported claims made in the Petition would risk usurping and effectively pretermitting the duties that Congress has delegated to the USDOT and, through it, NHTSA.

---

[48] NHTSA, *Request for Public Comment on NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Emerging Automotive Technologies*, 81 Fed. Reg. 18935 (Apr. 1, 2016).

[49] *See* 47 CFR § 95.1503. Under the DSRC service rules, licenses to engage in DSRC communications will be held by individual vehicle operators, and not by the automobile manufacturers themselves. Moreover, DSRC equipment authorizations may be held by the DSRC equipment suppliers.

[50] U.S. Department of Transportation, *Connected Vehicles and Cybersecurity* ("USDOT Cybersecurity Factsheet"), *available at* http://www.its.dot.gov/factsheets/pdf/cv_%20cybersecurity.pdf (last visited Aug. 24, 2016).

[51] USDOT Cybersecurity Factsheet.

2. The Federal Trade Commission.

Automobile manufacturers and equipment suppliers are also subject to oversight by the FTC, which enforces Section 5 of the FTC Act when companies fail to meet privacy and security expectations. As the Commission recognized earlier this year, the FTC has used its authority to prohibit "unfair or deceptive acts or practices in or affecting commerce" to enter into a series of precedent-setting consent orders addressing privacy practices.[52] These orders demonstrate that the FTC is an active enforcer willing to bring actions against companies whenever it believes that the appropriate privacy and security standards have not been met.

The FTC's enforcement powers are substantial. Its consent orders generally require companies to undergo independent, third-party audits of their privacy or security programs every year or every other year for a period of 20 years.[53] This process is "exhaustive and demanding," as the audits typically involve reviews of agreed-upon safeguards, explanations of why those safeguards are appropriate, and explanations of how those safeguards have been implemented.[54] Meanwhile, violations of the FTC's orders can cost a company up to $16,000 per violation or $16,000 per day for a continuing violation, which can add up quickly if a practice affects many consumers.[55]

---

[52] *See Broadband Privacy NPRM* ¶ 8.

[53] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

[54] *See id*. at 606.

[55] *See, e.g.*, FTC, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, *available at* https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited Aug. 19, 2016).

3. Existing FCC Precedent.

In an analogous context, the Commission has refrained from imposing specific, prescriptive rules on equipment manufacturers to protect the integrity of wireless device operations from hacking and malware and ensure that the devices operate as intended.[56] Indeed, the Commission dismissed as unnecessary safeguards that primary, safety-of-life services sought to ensure that unlicensed white space devices could not be tampered with in a manner that compromised their ability to avoid interfering with wireless medical telemetry service ("WMTS") operations.[57] It is difficult to square the Commission's position against imposing such rules on the manufacturers of white space devices with the Petitioners' proposed position of imposing similar rules on automobile manufactures. And, as discussed previously, the basis for imposing security rules on automobile manufacturers in the context of DSRC may not exist if automobile manufacturers hold neither FCC licenses to provide DSRC services nor FCC equipment authorizations to manufacture and sell DSRC equipment.

III. THE COMMISSION SHOULD DENY THE PETITIONERS' REQUEST TO STAY DSRC OPERATIONS IN THE 5.9 GHZ BAND.

The Petitioners ask the Commission to stay all DSRC operations in the 5.9 GHz band. This relief requested by the Petitioners is unprecedented, as it would stop private parties from offering lawful and beneficial services in ways that are consistent with the Commission's rules and

[56] *See, e.g., Amendment of Part 15 of the Commission's Rules for Unlicensed Operations in the Television Bands, Repurposed 600 MHz Band, 600 MHz Guard Band and Duplex Gap, and Channel 37, et al*., Report and Order, 30 FCC Rcd 9551, ¶ ¶ 194, n.490 (rejecting as unnecessary proposals for imposing additional rules on white space device manufacturers that would require that they demonstrate at the time they file their equipment authorization applications system reliability, security and integrity and the steps they have taken to prevent hacking), 196 n.495 (2015) (same).

[57] *Id*.

precedent. It is also difficult to reconcile the Petitioners' request with some of their other statements in the 5 GHz proceeding, which criticized the automotive industry for taking too long to deploy DSRC services.[58] Regardless, the Petitioners' stay request fails for procedural reasons and on the merits, as described below.

A. The Petitioners' Stay Request Suffers from Fatal Procedural Defects.

The Petitioners' request for an "emergency stay" suffers from multiple procedural defects. First, the Petitioners ignore Section 1.44(e) of the Commission's rules, which plainly states that a request for stay must be filed as a separate pleading.[59] "Any such request that is not filed as a separate pleading," the rule explains, "will not be considered by the Commission."[60]

Second, the Petitioners fail to identify which Commission "decision or order" they seek to stay, which makes it difficult to appropriately respond to the request.[61] For example, the Petitioners could be asking the Commission to stay its 1999 decision, which allocated 75 megahertz of spectrum for use by DSRC systems.[62] Or, the Petitioners could be asking the Commission to stay its 2004 decision, which adopted licensing and servicing rules for DSRC in the 5.9 GHz band.[63]

---

[58] *See, e.g.*, Letter from John Gasparini, Policy Fellow, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, ET Docket Nos. 13-49, 15-170 (May 6, 2016) (calling DSRC a product that "never materialized").

[59] *See* 47 C.F.R. § 1.44(e).

[60] *Id*.

[61] *Id*.

[62] *See Amendment of Parts 2 and 90 of the Commission's Rules to Allocate the 5.850-5.925 GHz Band to the Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Services*, Report and Order, 14 FCC Rcd 18221 (1999).

[63] *See Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band) et al.*, Report and Order, 19 FCC Rcd 2458 ¶¶ 46-49 (2004).

B. None of the Relevant Four Factors Weighs in Favor of a Stay.

The Petitioners' stay request also fails on the merits. When determining whether to stay the effectiveness of one of its orders, the Commission applies the four-factor test established in *Virginia Petroleum Jobbers Ass'n v. FPC*.[64] Under this standard, the party seeking a stay must demonstrate that: (1) it is likely to prevail on the merits; (2) it will suffer irreparable harm if a stay is not granted; (3) other interested parties will not be harmed if a stay is granted; and (4) the public interest favors granting a stay.[65] The relative importance of the four criteria will vary depending on the circumstances of the case, but a showing of irreparable harm is a "critical element" in justifying a request for stay of an FCC order.[66] To warrant injunctive relief, the injury must be "both certain and great; it must be actual and not theoretical."[67] In addition, the petitioner must provide "proof indicating that the harm [it alleges] is certain to occur in the near future."[68]

In this case, not only have the Petitioners failed to meet this burden, but each element weighs in favor of denying the stay request. As explained in Section II, *supra*, the Petitioners' request to initiate a rulemaking should be denied given the nature of DSRC service and role of other federal agencies. DSRC systems for V2V do not collect, transmit, or store any information that is linkable to a particular person or vehicle and thus do not raise consumer privacy issues or

[64] *See, e.g., Connect America Fund; High-Cost Universal Service Support*, Order, 27 FCC Rcd 7158 (WCB 2012) ("*Silver Star Order*") (denying requests to stay an order that established a new methodology for limiting reimbursable capital and operating costs within the high-cost loop support program); *see also Virginia Petroleum Jobbers Ass'n v. FPC*, 259 F.2d 921, 925 (D.C. Cir. 1958); *Washington Metropolitan Transit Comm'n v. Holiday Tours, Inc.*, 559 F.2d 841 (D.C. Cir. 1977).

[65] *See id*.

[66] *See, e.g., Silver Star Order* ¶ 5; *Wisconsin Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1985 (denying stay requests after finding only that the petitioners would not suffer irreparable harm).

[67] *See Silver Star Order* ¶ 7 (quoting *Wisconsin Gas*, 758 F.2d at 674).

[68] *See id*.

implicate the Commission's CPNI or CPI rules. They also already incorporate robust cybersecurity protections. Further, other federal agencies, such as the NHTSA and the FTC, already regulate privacy and cybersecurity as they relate to DSRC and automobile manufacturers in general.

Nor have the Petitioners shown that they or any other party would suffer "irreparable harm" if the Commission does not grant a stay. In fact, the two central documents upon which the Petition is based do not support a finding that harm to the public from the deployment of DSRC or of any modern automotive technology is imminent.[69] Both documents merely posit the theoretical risk of hacking and neither attribute that risk to DSRC. Moreover, neither document addresses, in detail, the security measures that the industry, in cooperation with regulators of jurisdiction, have devised. It is impossible to extrapolate from these documents a justification for the FCC to intrude into these matters.

Finally, a stay would harm many other interested parties and would not be in the public interest because it would delay the great promise that DSRC holds for reducing the number of and damage caused by automobile crashes, providing significant traffic management benefits, and providing significant environmental benefits.[70]

[69] Staff of Senator Edward Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk* (Feb. 2015), *available at* https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf (last visited Aug. 24, 2016). *See also* Federal Bureau of Investigation, *Motor Vehicles Increasingly Vulnerable to Remote Exploits*, Public Service Announcement (Mar. 2016), *available at* https://www.ic3.gov/media/2016/160317.aspx (last visited Aug. 24, 2016).

[70] *See, e.g.*, Alliance *et al.* 5.9 GHz Refresh Comments at 4-9.

IV. CONCLUSION

For the reasons discussed above, both of the Petitioners' requests should be denied.

Respectfully submitted,

/s/ Ari Q. Fitzgerald

Ari Q. Fitzgerald
Wesley Platt
Hogan Lovells US LLP
Columbia Square
555 13th Street, NW
Washington, DC 2004
Tel.: (202) 637-5423

Attorneys for the Alliance

/s/ James Arden Barnett, Jr.

James Arden Barnett, Jr.
Ian D. Volner
Stephen R. Freeland
Cristina I. Vessels
Venable LLP
575 7th Street, NW
Washington, DC 20004
Tel.: (202) 344–4000

Attorneys for Global Automakers

/s/ Robert B. Kelly

Robert B. Kelly
Koyulyn Miller
Squire Patton Boggs (US) LLP
2550 M Street, NW
Washington, D.C. 20037

Attorneys for ITS America