that they can be optimized and prioritized. Non-V2V based warning systems are found in more and more vehicles, where they have been integrated to address and minimize distraction. This would not necessarily be the case for aftermarket, non-integrated systems.

Finally, additional concerns, which are discussed in detail elsewhere in this submission, including privacy, security, liability, intellectual property (IP), customer acceptance, certification, governance, and operating rules, apply equally to aftermarket V2V devices. Legal protections in these areas are limited or non-existent, which will likely have a large influence on the viability of the aftermarket V2V device business model. There will be very little utility to installing aftermarket V2V devices for the first decade, given the costs and minimal benefits they will provide to buyers prior to full market penetration.

*23. Are aftermarket V2V devices more likely to be simple Vehicle Awareness Devices (VADs), or are they more likely to be integrated into vehicles as retrofits, more similar to OEM devices? What can the agency do, consistent with its authority, to help ensure that aftermarket devices can be and are installed properly?*

Four types of devices are currently envisioned as V2V On-Board Equipment (OBE) that will communicate via DSRC: 1) Vehicle Awareness Devices, 2) Aftermarket Devices, 3) Retrofit Devices and 4) Integrated Systems. Retrofit Devices and Integrated Systems are generally recognized to be authorized or sanctioned by the automaker for the particular vehicle in which the device or system is installed. The Alliance is aware that aftermarket V2V devices and vehicle awareness devices were deployed in the Model Deployment and further research is ongoing.

The Alliance notes that Aftermarket Devices and Vehicle Awareness Devices have no authorized access to the databus, but may be able to utilize data available via the OBDII port. Access to the databus cannot be allowed to third parties for critical vehicle security and intellectual property protection reasons. However, this means that the V2V OBE performance cannot be guaranteed to meet the potential minimum performance requirements to send basic safety messages. More importantly, the connection of an aftermarket or vehicle awareness device to OBD II port may have adverse effects on integrity and operation of the vehicle databus.

The ANPRM proposes that all new vehicles manufactured after a production phase-in would be required to be equipped with functional V2V communication systems. The typical design solution to such a functional requirement is a fully-integrated approach in order to optimize system performance, design, development, and production costs. Alternatively, retrofit devices may be offered by individual original equipment manufacturers on a case-by-case basis.

*24. Do commenters believe that the agency's technical observations for DSRC devices and safety applications would also apply for vehicles over 10,000 pounds GVWR? If not, why not?*

The Alliance is not in a position to comment on vehicles larger than 10,000 GVWR.

*25. How should NHTSA work to harmonize its actions on V2V with those being taken globally?*

NHTSA should be attentive to opportunities to harmonize all technical requirements that affect vehicle design. The Alliance understands this to be consistent with the approach NHTSA has generally taken with respect to new regulations.

With support from industry, the U.S. DOT is and has been engaged in ongoing harmonization discussions with the EU, Japan, Australia and others that can help inform NHTSA on the issues associated with harmonization, including benefits that allow global economies of scale which allow V2V at a lower cost to consumers. It remains important to recognize that, at this point, the investment of the U.S. DOT and the industry has positioned the US as the leader in crash imminent safety warning applications for V2V. Harmonization should be approached with a goal of avoiding the unnecessary compromising of functionality.

In addition, given frequent cross-border traffic between the US, Canada and Mexico, we believe that it is important that international agreements among NAFTA countries are implemented that address whether/how DSRC devices on vehicles function during and after crossing applicable land boarders. By doing so, this also maximizes the benefits of V2V safety applications as more vehicles in the NAFTA region could seamlessly participate across borders.

**Safety Applications That V2V Could Facilitate**

*26. Do commenters believe that the agency's preliminary findings and conclusions for each of the safety applications discussed in the report are accurate? Why or why not? Please provide any available evidence or research to support your view.*

Generally, Alliance members find the agency's description of possible safety applications to be accurate and reasonable. It is important to note and reaffirm that V2V may have some unique capabilities that may not be possible using current vehicle-based sensing. These features (e.g., LTAP or IMA) may provide unique benefits from V2V technology when compared to other sensing technologies, but when fused together may support new applications or improve some existing applications. Other V2V features may also provide benefit, but because many of them may be achieved using other technologies, identifying the possible incremental benefits and effectiveness of these features is much more complex and difficult to specifically estimate or measure.

*27. The agency would appreciate if commenters, specifically entities currently developing production-intent V2V applications, could provide information regarding V2V applications they anticipate implementing once V2V technology becomes available in the fleet. More specifically, what applications and what safety warning and/or convenience functionality would be available to consumers of their products upon V2V entry to the marketplace?*

The Alliance is not in a position to answer this question for antitrust reasons. Alliance member companies may submit individual responses to this question.

**Public Acceptance**

*28. Do commenters believe that the agency's preliminary assessment of the public acceptance issues associated with V2V is accurate? Why or why not? Please provide any available evidence or research to support your view.*

Alliance members respect their customers' privacy and understand that consumers also want technologies that deliver a clearly-defined benefit, without creating new risks and unintended consequences. We agree with NHTSA's acknowledgement that the agency has limited authority to address the types of privacy and security concerns associated with V2x deployment and uses of the communications network being proposed; however, other parts of the Federal Government have such authority and these government entities should work collaboratively with stakeholders to articulate a framework for privacy and security before further rulemaking proceeds. To support these efforts, NHTSA should expand the scope of privacy concerns it evaluates as the agency proceeds with an NPRM. The Alliance agrees with the need for NHTSA to conduct a Privacy Impact Assessment and we recommend the agency consider conducting further public workshops to thoroughly investigate privacy issues. These should also include an expanded scope that considers all possible uses of the envisioned transportation communications network including all potential internal, external abuses, and other challenges not solely those concerned with safety, mobility and the environment.

Once connected vehicles are deployed, V2X applications are likely to quickly follow, including applications that allow connectivity to infrastructure and various backhaul networks. The onset of a network made possible through V2X applications may increase privacy and security risks for the driving public. To date, the public comments show that the general public has concerns that new threats to privacy and security may result as applications continues to spread into areas of additional use-cases such as mobility, environment, and convenience, in addition to safety applications. The Alliance recommends the privacy impact assessment include analysis of the broader V2X transportation communication network, not just a V2V safety network. This would include public acceptance and privacy concerns relating to uses of the V2X network for commercial ventures, law enforcement and taxation.[6]

---

[6] NHTSA otherwise acknowledges its own expectation that V2V will lead to V2x applications; this is made clear in the Abstract to the report "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," which states in relevant part: "Using this report and other available information, decision-makers will determine how to proceed with additional activities involving vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P) technologies."

Public trust is essential to the success of connected vehicle technologies. These systems are based on a network effect where a broad base of users exchange information to provide benefits to surrounding users. The realization of this technology will only be possible if the public trusts enough to opt-in for core and ancillary services. A failure to gather consumer acceptance and trust will impact the user base of these technologies and, in turn, undermine the potential for providing maximum value added benefits. A lack of public acceptance may even adversely affect sales of new vehicles equipped with this technology.

Automakers, NHTSA, and other government entities must work together to ensure a V2V system that induces consumer trust and public acceptance. Any future system to be deployed must allow for complete and total anonymity for default services that do not provide an opt-out option. These systems must provide secure and trusted protection of all personally identifiable information (PII) associated with the system. Such services that are mandatory must not allow or provide any support to law enforcement for tracking or other types of internal abuse. Similarly, services that provide for opt-in must also clearly communicate what information the user will disclose and the specific purposes and uses of this disclosed information. In order to be successful, these services must be transparent and provide clear benefits that outweigh consumer concerns associated with privacy and security.

*29. Do commenters foresee any issues regarding public or industry acceptance not discussed in the report that the agency should consider in developing its proposal? How do commenters recommend the agency address those issues, if any?*

There are a range of unacknowledged concerns that NHTSA should also consider. Regarding public acceptance[7], most docketed comments to date highlight potential health effects of electromagnetic radiation (EMR), followed closely by comments on privacy concerns. Concerns over the health effects of EMR were not previously anticipated by the agency or industry stakeholders involved in development of this new transportation communications network, but they are a growing public concern and should be thoroughly researched and addressed prior to deployment.

Public commenters raised concerns regarding how this technology may be used, including concerns relating to the current absence of established legal limits on what a new V2X transportation communications network can and cannot be used for, which entity or entities have access, and defining the data to which access is available and for what purposes. These points reflect factors that may influence public acceptance. In addition to general concerns on privacy and security of the data, commenters fear the use of such a new transportation communications network to:

[7] The NHTSA report titled "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," treats the concepts "public acceptance" and "industry acceptance" separately, so the Alliance answer does, too.

- Establish a system capable of tracking individual vehicles;
- Automate law enforcement including traffic citations and off-board vehicle control;
- Leverage of the technology for road use tax collection purposes; or
- Exploit the technology to expand "Big Data" collection.

Regarding industry acceptance, Alliance member companies advocate for thoroughly researched answers to the concerns of our customers in the public acceptance areas, above. In addition to those issues, we also add the following areas that NHTSA should examine:

- New risks posed to vehicle manufacturers related to protection of intellectual property such as increased exposure to patent infringement lawsuits and unintended access to vehicle networks by third parties;
- New privacy risks posed to the public by proposed state legislation attempting to gain access to vehicle data under the guise of consumer protection.
- New liability risks posed by the new transportation communications network for vehicle manufacturers (see Attachment B);
- Need for requirements to ensure interoperability and minimum performance requirements long-term;
- Lack of authorization for regulation of DSRC devices (aftermarket, carry-in, and road-side);
- Lack of authorization for cross-border agreements (NAFTA); and
- The extent to which state and local governments will or should be preempted from passing laws and regulations that result in a patchwork of potentially divergent user and vehicular requirements for the system.

*30. What suggestions do commenters have regarding how the agency should go about educating the public about security and privacy aspects of the V2V technology?*

As detailed in answers to Questions 28 and 29, public trust is essential to the success of vehicle technologies. The Alliance members respect their customers' privacy and also understand that customers want to know how these technologies can deliver benefits to them. Many of the comments that were filed in this proceeding involved privacy. These privacy concerns, if unaddressed, present a challenge to full deployment of connected vehicle technology. We agree with NHTSA that it has limited authority to address privacy. As noted earlier, the Alliance agrees with the need for NHTSA to conduct a Privacy Impact Assessment that comprehends the scope of a V2X transportation communication network, and further recommends that the agency conduct public workshops with the Federal Trade Commission to thoroughly investigate this issue.

**<u>V2V Communications Security</u>**

*32. The current design for the security system for V2V communications, as discussed in Section IX of the report, is based on Public-Key Infrastructure (PKI), which is currently used to secure the passing of data on public networks (such as the internet). V2V envisions a machine-to-machine PKI system. Do commenters believe that using machine-to-machine PKI for V2V is feasible, and that a security system based on PKI provides the level of security needed to support wide-scale V2V deployment? If not, what other security approach would be a better alternative, and why?*

At the outset, the Alliance recommends that this question not be restricted to V2V communications, but also consider V2I and V2X communications, including third-party applications (e.g. data aggregation) and commercial and public non-safety applications, which may inadvertently undermine security and privacy goals.

Based on today's knowledge, the proposed CAMP solution should provide a sufficient level of security and flexibility while covering all V2V-related use cases, wheras the next CAMP research project related to SCMS design is expected to expand the scope to V2X communications. PKI is a well-understood and frequently-used security solution in large-scale deployments today. At this time, there are few alternatives to PKI to support this use case. Those alternatives are 1) Symmetric-key authentication and management and 2) group signatures and group signature infrastructure. Neither is as ideal as PKI.

Symmetric-key management is infeasible for a system of large scale, where devices frequently encounter other devices for the first time, and where traceability is necessary.

Group signatures are more promising than symmetric-key management, but they are not ready for large systems because they are inefficient and have large overhead associated with revocation. Even refined group signatures with improved revocation schemes are not applicable to the V2V use case.[8]

PKIs are used today and are well understood. Due to the shortcomings of symmetric-key management and asymmetric-key management, and the lack of any evidence suggesting problems with the feasibility of a PKI for V2V communication applications, the Alliance contends that PKI is the only reasonable solution.

*33. Do commenters believe that the current security system design (as shown in Figure IX–3 of the research report) is a reasonable and sufficient approach for implementing a secure and trusted operating environment? If so, why? If not, why not, and what improvements are suggested?*

---

[8] Dan Boneh and Hovav Shacham: Group Signatures with Verifier-Local Revocation, in proceedings of the 11'th ACM conference on Computer and Communications Security (CCS), pp. 168-177, 2004

The security system design has been developed to be "private by design." Based on this, the proposed system that is under development is a reasonable approach because it addresses privacy against outsiders and privacy against insiders, including those running active components of the security system. It also assures efficient and privacy-preserving certificate update mechanisms providing a high level of flexibility as well as efficient conditional certificate revocation without loss of backwards privacy.

However, there are some details in the technical report related to the security system that should be clarified, revisited or addressed.

- In several instances in the report, it is unclear whether the USDOT considers the CAMP model or the BAH model. This should be clarified.
- Enrollment Certificate Authority (ECA) and personally identifiable information (PII) - Research Report, Page 190: The report considers the component ECA to be central and assumes that it collects PII. This significantly deviates from the model presented in public by CAMP members in which no PII is required.[9] This conflict should be addressed.
- RSE Coverage Model - Research Report, Page 243: The coverage derived from the NHS roadway model is unrealistic. Based on Figure 2 of the report "Communications Data Delivery System Analysis for Connected Vehicles, Rev. 5, May 29 2013." It is not possible to precisely determine how the NHS model has been derived (the report references Appendix F, but the appendices to this document cannot be found in the ANPRM docket). However, the graph suggests that the coverage for the NHS system has been derived as an average using the interstate highway system and network of secondary roads. This would be an improper method because the NHS model fails to weigh the large differences in volume when it compares secondary roads to interstate roads. These calculations should be revisited.
- Certificate Revocation List Distribution: Based on the RSE Coverage Model, the system currently lacks a sound dissemination model for certificate revocation lists. A potentially viable model could be based on a road-side model with a reassessed number of RSEs. Another option is to study alternative dissemination methods such as epidemic distribution, currently under research by CAMP.[10]

*34. The current security system design includes regular distribution of the Certificate Revocation List (CRL) to identify devices that are not functioning properly, as discussed in Section IX. Do commenters believe the CRL is necessary? If so, why? Is there an alternative approach to using*

[9] Thorsten Hehn and Andre Weimerskirch: The US SCMS Design Overview: A Security Credential Management System for V2X Communications, ITS World Congress 2014, September 2014, Detroit, MI, USA.

[10] Thorsten Hehn and Andre Weimerskirch: The US SCMS Design Overview: A Security Credential Management System for V2X Communications, ITS World Congress 2014, September 2014, Detroit, MI, USA.

*CRLs to take V2V devices ''off-line?'' If so, please describe. If commenters believe that CRLs are necessary, are there alternative methods to CRL distribution beyond what the agency described in the research report? If so, what are they?*

Although there are potential liability concerns associated with revocation, Alliance members support this approach. Certificate revocation lists can be generated by different means[11]:

- Entries can be added manually (e.g., when security researchers publish cryptographic secrets on the internet),
- Entries can be added automatically using misbehavior detection which is primarily designed to efficiently identify misbehaving devices and adequately dissuade hackers from generating spurious messages and to stop the harm if/when they do *See* Attachment B for detailed discussion of liability issues.

*35. Do commenters believe a V2V system would create new potential ''threat vectors'' (i.e., ''ways into'' a vehicle's electronic control unit) that could somehow control a vehicle or manipulate its responses beyond those existing in today's vehicles? If so, please describe the extent to which they might arise in the context of the security approach described in Section IX of the research report.*

Requiring new mechanisms to communicate with vehicles increases the ways in which a potential cyber-attack could occur. While many vehicles currently do or will have Bluetooth capability or embedded cellular modems, a DSRC interface for V2V creates additional, unique security challenges. A primary concern is the potential link between the DSRC, vehicle data busses such as the vehicle communications controller area network (CAN), and on-board safety systems. If malware is introduced via DSRC, the resident vehicle and possibly other vehicles communicating with the resident vehicle could be affected. As more DSRC-equipped vehicles and infrastructure are deployed, the desire by bad actors to exploit these attack vectors may increase. Therefore the risk and concern is potentially magnified but manageable given the in vehicle security measures and PKI structure.

To address this, security for DSRC systems that interface with the on-board communication networks require protection for both over-the-air communications (vehicle-to-vehicle and vehicle-to-backend) as well as in-vehicle protection. The former can likely be addressed by PKI. The latter are more difficult to protect and are not addressed in Section IX of the research report. Rather, they are assumed to be dependent on individual OEM security practices.

*36. Do commenters believe that V2V could introduce the threat of remote code execution, i.e., that, among possible threat vectors, malicious code could be introduced remotely into a vehicle through the DSRC device and could create a threat to affected vehicles? If so, do commenters have or plan to develop information (research or data) on this potential risk in the context of*

[11] Tigran Khatchatrian, Potential Methods for Addressing Misbehavior in Vehicular Communications, , ITS World Congress 2014, September 2014, Detroit, MI, USA.

*V2V, especially the current PKI-based approach to V2V security, as discussed in Section IX in the report?*

The potential link between the DSRC, vehicle data busses such as the vehicle communications CAN, and on-board safety systems could create the risk of malicious code execution. The methods for in-vehicle protection between the DSRC system and vehicle control systems do not appear to be addressed in Section IX and are assumed to be dependent on individual OEM security practices and proprietary knowledge.

Automakers continue to explore this potential risk in the context of V2V as discussed in Section IX of the report in the CAMP partnership. Even though the communication protocol may be robust, concerns remain with the actual device implementation. Protection measures and appropriate implementation discipline will be required.

Such security measures are vehicle platform-dependent, such that the system architecture has a large influence on what security measures are required to address the potential threat vector(s) and security concerns are associated with a particular implementation. Industry best practices are leveraged, but manufacturer's internal designs and architectures are competitive and unique mechanisms to prevent, resist, monitor and recover from attacks will exist.

*37. Do commenters have suggestions on how NHTSA could mitigate these potential threats with standardized security practices and how NHTSA could implement a self-certification or third-party audit or testing program to guard against such threats? What research is needed to accomplish these tasks?*

In the context of V2V, only, security should be considered as two, distinct, interrelated realms. The first is the creation, delivery and management of V2V security certificates. The second is vehicle system and vehicle network cybersecurity.

For V2V certificate security, a PKI system requires that all vehicles/devices be able to transmit, receive, trust and understand certificates to and from other vehicles. Therefore, a single trust root and common protocols are crucial. However, for cybersecurity – the mechanisms to prevent, resist, monitor and recover from attacks against vehicles/devices are competitive. Therefore, vehicle and device makers will develop varied and specific approaches to their own devices.

For certifying, testing or auditing in-vehicle devices, self-certification as per the motor vehicle safty act should remain the norm. However, because devices from different suppliers will likely adopt different approaches and processes to design and validate their security solution, some devices might be more vulnerable than others. The misbehavior detection, device revocation, potential safety concerns, liability, and loss of image that may result from a vulnerable security solution suffice to prevent the need for a rigidly-defined in-vehicle security standard for a warning only system.

*38. The currently contemplated security architecture does not involve encryption of the basic safety message (BSM), as explained in the report. In light of the fact that the system does involve asymmetric encryption of the security certificates that are a prerequisite to acceptance of a vehicle's BSM, does the absence of encryption of the BSM itself create any security threat, e.g., reverse engineering of a V2V system? If so, how might that threat be assessed and addressed?*

The controls currently planned in the design of the SCMS appear adequate based on current knowledge.

As noted in previous answers, the security system is built on PKI, which uses public and private keys (asymmetric cryptography). In PKI, a private key is used for signing and a public key is used to verify the validity of signatures. There is a complex foundation in the V2X system which involves the private key of the root Certificate Authority (CA) in the SCMS. The root CA is used to authenticate intermediate CAs. The intermediate CAs then authenticate pseudonym CAs, which generate pseudonym certificates that are given to certified devices. When a BSM is transmitted, a pseudonym certificate is attached. The BSM is also cryptographically signed with the private key that is associated with the public key (this is included in the pseudonym certificate attached to the message. Upon receipt, the signature is verified and the validity period in the pseudonym certificate attests to the device certified to send BSMs. It also verifies that the signature and the message were not altered from transmission to reception. What is not encrypted includes the status of some specific vehicle systems and general vehicle dynamic information which does not represent a security threat.

There are, however, other potential security threats to the system that should be addressed:

- The private key of the Root CA must be protected. Disclosure of the private key undermines both privacy and security.
- Bad actors can sign any message or certificate in the name of the root CA. This includes standing up new authorities. These authorities can be used to generate and sign enrollment certificates, generate and sign pseudonym certificates, produce certification revocation lists, etc. It needs to be understood that disclosure of the Root CA's private key is a disastrous event for any PKI system. There are rules and procedures following best industry practice, which assist in preventing this type of failure in a multitude of deployed systems.

*39. If OEM DSRC devices were kept up-to-date through the current methods of upgrading that existing consumer electronics use today, would the use of this updating process introduce a new attack vector? What are the security ramifications of this vector and what are the possible mitigations of the threat?*

The automotive industry's technical development is consistent with established laws and regulations. It reflects the intrinsic need to ensure the utmost in vehicle safety and customer privacy through security. Security is imperative for safety and system acceptance. In all cases (safety, privacy and security) the industry uses accepted standards and best practices from the automotive and other industries which include acknowledged and verified methods/procedures that can be found in IEEE, SAE, ISO, and other standards organizations. This approach applies to all systems in the vehicle and to all devices used by the vehicle for communicating and interfacing with the external environment.

Any new method of communication introduced to computerized devices in vehicles can be considered as an additional attack vector. Mitigation is critical and can be achieved through many different technical methods. For example, one solution involves integration of an accepted approach, such as Trusted Platform Module (TPM), in order to implement secure boot on the device which could be used in conjunction with several additional layers or methods of security.

Alliance members are engaged in several forums both domestically and internationally to establish best practices in the area of vehicle and wireless security. The Alliance and Global Automakers have joined together to research the creation of a voluntary cybersecurity forum, which would quickly disseminate critical security risk information to its members. This forum would keep the whole industry aware of developments, events and needed data which will assist in mitigating attacks. In the US, the SAE Vehicle Electrical System Security Committee also has been developing a best practices document for vehicular cybersecurity development, as well as researching newly available methods of securing embedded devices via hardware. The industry and government entities should work together to analyze and develop mitigation strategies.

*40. Is there a possibility of cyber-attacks across the entire vehicle fleet and, if so, how should they be analyzed and addressed?*

As referred to in previous responses, the likelihood of fleet-wide attacks decreases since vehicles and devices can be treated as segregated devices which lowers the motivation and increases the challenge to attack an individual vehicle due to security implementation of a particular vehicle and the PKI implementation.

However, if the root CA within the SCMS backend structure is compromised, a cyber-attack across the entire vehicle fleet may be possible and may generate false or missed (due to false revocation) warnings which affect customer satisfaction.

BSMs representing vehicle behavior and activity should be continuously monitored for equipment failure or implausible messages which can be due to technical issues or tampering by hackers. Detection mechanisms reliable enough to properly identify misbehavior should be in place, and robust and efficient reporting mechanisms should be available if an attack occurs. Once a fleet-wide attack is confirmed by the SCMS, DSRC communications between vehicles should be disabled to prevent attack from further propagation.

*41. Are there any other specific security issues that have not been mentioned here, but that should be addressed in the V2V security review? If so, please identify them and discuss how they should be addressed.*

NHTSA assumes that the SCMS need only manage V2V security certificates, meaning there is a relatively low risk of the SCMS being a significant target. There has been no significant testing to validate this assumption. Given that an extremely high level of reliability is needed for this process and it is intended to expand, the system needs extensive verification and validation. The SCMS will have to handle all traffic (noted in question 17) from all vehicles devices and utilize, various backhaul networks set up to handle both security-related communications, V2X and any number of other communications serving a wide variety of purposes. This technical complexity has not yet been addressed at a functional level and will require extensive research in advance of deployment of this technology.

As vehicles begin broadcasting data and communicating between themselves or with infrastructures (for whatever purposes – security or otherwise), some devices will attempt to participate in both pushing to and pulling from this network. If NHTSA deploys this technology without any laws in place to restrict what this new technology can and cannot be used, state and municipal governments will fill likely the gap. Federal law should define and set limits for this technology's allowed uses and limits. If NHTSA does not address this, there may be unbounded security vulnerability.

**Liability**

The Alliance response to the questions and issued raised on liability is in Attachment B.

**Preliminary Cost and Benefits Estimates**

The Alliance response to the questions and issues raised on preliminary cost and benefits estimates is in Attachment C.

**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, DC 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band | ) ) ) ) | ET Docket No. 13-49 |

# COMMENTS OF THE ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC. AND THE ASSOCIATION OF GLOBAL AUTOMAKERS, INC.


Ari Q. Fitzgerald
Edmond Thomas
Mark W. Brennan
Phillip A. Berenbroick
HOGAN LOVELLS US LLP
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5663
ari.fitzgerald@hoganlovells.com

*Counsel to the Alliance of Automobile Manufacturers, Inc. and The Association of Global Automakers, Inc.*

Robert Strassburger
Alliance of Automobile Manufacturers, Inc.
803 7th Street, NW
Suite 300
Washington, DC 20001
(202) 326-5500

Michael Cammisa
Association of Global Automakers, Inc.
1050 K Street, NW, Suite 650
Washington, DC 20001
(202) 650-5555


May 28, 2013

## TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY ..... iv

I. INTRODUCTION ..... 1

II. SUMMARY ..... 3

A. DSRC and Other Connected Vehicle Technologies Will Provide Significant Public Interest Benefits ..... 3

B. DSRC Technologies in the 5.9 GHz Band Are at an Advanced Stage of Development and Are Near Widespread Deployment ..... 4

C. Allowing U-NII Use of the 5.9 GHz Band Could Cause Harmful Interference to and Undermine the Viability of "Safety-of-Life" DSRC Operations ..... 6

D. It is Imperative that the Commission Await the Results of NTIA's 5.9 GHz Band Study and the Finalization of a U.S. Position on Compatibility Before Proceeding with a Proposal for U-NII Use ..... 7

III. DSRC AND OTHER ITS TECHNOLOGIES ARE POISED TO BECOME CENTRAL COMPONENTS OF THE 21ST CENTURY HIGHWAY TRANSPORTATION SYSTEM ..... 9

A. DSRC Services Will Improve Automobile Safety by Reducing Crashes ..... 9

B. DSRC Services Can Provide Significant Traffic Management Benefits, Further Improving Public Safety ..... 12

C. DSRC Services Can Provide Significant Environmental Benefits ..... 14

D. Congress and the Commission Have Long Recognized the Transportation Benefits of Interoperable ITS and DSRC Services ..... 15

IV. DSRC CONNECTED VEHICLE TECHNOLOGY IS AT AN ADVANCED STAGE OF DEVELOPMENT, AND THE COMMISSION SHOULD PROCEED CAUTIOUSLY TO AVOID DISRUPTING ITS DEPLOYMENT ..... 18

V. THE COMMISSION SHOULD NOT ALLOW U-NII USE OF THE 5.9 GHZ BAND UNLESS IT CAN BE OBJECTIVELY DEMONSTRATED THAT SUCH USE WILL NOT INTERFERE WITH DSRC SYSTEMS ..... 22

A. Interference Would Significantly Undermine the Safety Benefits of DSRC Systems and Threaten DSRC Deployment ..... 23

1. Interference to V2V and V2I Services Poses Significant Safety Risks ..... 23

2. Potential Interference to V2V and V2I Services Will Undermine Their Deployment ..... 25

B. U-NII Use of the 5.9 GHz Band Poses a Significant Interference Threat to DSRC Systems and Road Safety ..... 27



\\DC - 023165/000003 - 4675609 v1

1. U-NII Devices in the 5.9 GHz Band Could Cause Harmful Co-Channel Interference ..... 27

2. Adjacent Channel and Adjacent Band Operations by U-NII Devices Could Cause Harmful Interference to DSRC Systems ..... 30

C. The Commission Should Await the Results of NTIA's Study and Other Efforts Regarding the Compatibility of U-NII Use of the 5.9 GHz Band with DSRC and Seek Public Comment on a Proposal for U-NII 5.9 GHz Use Based on Such Efforts ..... 31

D. The Alliance and Global Are Prepared to Work With All Stakeholders to Find a Solution to Interference Issues, if Possible ..... 33

VI. CONCLUSION ..... 34

## EXECUTIVE SUMMARY

Although the Alliance of Automobile Manufacturers ("Alliance") and the Association of Global Automakers ("Global") understand the Commission's desire to unleash additional spectrum for Unlicensed National Information Infrastructure ("U-NII") use, we have grave concerns about allowing such use of the 5850-5925 MHz ("5.9 GHz") Dedicated Short Range Communications Service ("DSRC") band. DSRC holds great promise for improving the safety of United States roadways and substantially enhancing the efficiency of the U.S. highway transportation system. Significant progress has been made toward its widespread deployment. At the cusp of a deployment decision by the National Highway Traffic Safety Administration ("NHTSA"), this potentially life-saving technology will only be effective and viable if it can operate in an interference-free environment.

As discussed more fully below, the Alliance and Global are skeptical that, as proposed by the Commission, U-NII devices will be able to share, or operate in close spectral proximity to, the 5.9 GHz DSRC band without causing severe and persistent, harmful interference to DSRC vehicle-to-vehicle ("V2V") and vehicle-to-infrastructure ("V2I") communications. U-NII use of the 5.9 GHz band could cause harmful co-channel, adjacent channel, and out-of-band interference to DSRC services. This interference would degrade DSRC V2V and V2I communications, make it impossible to confidently develop new latency-sensitive safety and other applications requiring high spectrum availability, and call into question the viability of the U.S. Department of Transportation's and auto industry's shared vision for connected vehicles. The Alliance and Global have initiated dialog with advocates of 5.9 GHz U-NII use to discuss these concerns, with the hope of achieving assurances that through bench and field testing and analysis, and additional

public consultation, the interference issues discussed herein can be resolved. We stand ready to work with the Commission and other stakeholders as this proceeding evolves to address these concerns, but it is important that the Commission continue to preserve the dedicated DSRC spectrum to maximize the potential of this very promising technology.

**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, DC 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band | ) ) ) ) | ET Docket No. 13-49 |

**COMMENTS OF THE**
**ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.**
**AND THE**
**ASSOCIATION OF GLOBAL AUTOMAKERS, INC.**

## I. INTRODUCTION

The Alliance of Automobile Manufacturers, Inc. (the "Alliance")[1] and the Association of Global Automakers, Inc. ("Global"),[2] which together represent the manufacturers of approximately ninety-nine percent of all cars and light trucks sold in the United States,[3] submit these comments in response to the Notice of Proposed Rulemaking ("NPRM") issued by the

[1] The Alliance is an association of twelve of the world's leading car and light truck manufacturers, including BMW Group, Chrysler Group LLC, Ford Motor Company, General Motors Company, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche, Toyota, Volkswagen Group of America, and Volvo Cars. *See* Alliance of Automobile Manufacturers, Members, http://www.autoalliance.org/about-the-alliance/overview.

[2] Global Automakers represents international motor vehicle manufacturers, original equipment suppliers, and other automotive-related trade associations. Our 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. Peugeot Motors of America, Subaru of America, Inc., Suzuki Motor of America, Inc., and Toyota Motor North America, Inc. *See* Global Automakers, Members, http://www.globalautomakers.org/members.

[3] *See* Auto Sales, Market Data Center, Wall St. J., May 1, 2013, http://online.wsj.com/mdc/public/page/2_3022-autosales.html#autosalesE.

Federal Communications Commission ("Commission") in the above-captioned proceeding.[4] The NPRM seeks comment on, *inter alia*, making spectrum in the 5.850-5.925 GHz band ("5.9 GHz band") available for Unlicensed National Information Infrastructure ("U-NII") use.[5]

The 5.9 GHz band is allocated for Intelligent Transportation Systems ("ITS"), which utilize Dedicated Short Range Communications Service ("DSRC") systems. DSRC systems, including "safety-of-life"[6] vehicle-to-vehicle ("V2V") and vehicle-to-infrastructure ("V2I") systems, are authorized to operate in the 5.9 GHz band on a primary basis.[7] The Alliance and Global are the main trade associations representing the interests of automobile manufacturers that are developing, testing, and validating 5.9 GHz band DSRC technology.

As discussed below, the Commission should proceed with extreme caution as it considers the substantial technical, policy, economic, and practical challenges to allowing U-NII use of the

---

[4] Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, ET Docket No. 13-49, *Notice of Proposed Rulemaking*, 28 FCC Rcd 1769 (2013) ("*NPRM*").

[5] *Id.* ¶¶ 2, 75.

[6] The Commission has established a priority framework for DSRC communications, explaining that "DSRC communications involving imminent safety-of-life," including, "*e.g.*, vehicle-to-vehicle collision avoidance—must have access priority over all other DSRC communications." Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band), 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, WT Docket No. 01-90, ET Docket No. 98-95, RM-9096, *Report and Order*, 19 FCC Rcd 2458, 2475 ¶ 32 (2004) ("*2003 Licensing and Service Order*"). The International Telecommunication Union Constitution recognizes that "safety-of-life" communications must be given "absolute priority." Int'l Telecomm. Union Constitution Article 40 – Priority of Telecommunications Concerning Safety of Life, *available at* http://www.itu.int/net/about/basic-texts/constitution/chaptervi.aspx. Moreover, Congress created the Federal Communications Commission, in part, "for the purpose of promoting safety of life and property through the use of wire and radio communications." 47 U.S.C. § 151.

[7] *NPRM* ¶ 92 (citing 47 C.F.R. § 2.106 Table of Frequency Allocations—Non-Federal Government footnote NG-160).

5.9 GHz band. Although the Alliance and Global understand the Commission's goal of providing additional spectrum to support wireless broadband services and are fully committed to working with the proponents of U-NII use to evaluate the prospects for coexistence with DSRC, that goal should not be elevated above the goal of facilitating the "safety-of-life" systems for which DSRC technology is intended. The NPRM raises extremely troubling concerns that could undermine the efforts of government and private sector stakeholders to deploy "safety-of-life" DSRC services in the 5.9 GHz band. As explained in more detail below, U-NII use of the 5.9 GHz band could cause harmful co-channel, adjacent channel, and out-of-band interference to DSRC services in numerous ways that would significantly reduce or eliminate the anticipated benefits associated with vehicle-based safety communication systems.

The Commission should not allow U-NII use of the 5.9 GHz band unless a set of rules can be developed and shown, through rigorous bench and field testing, to protect 5.9 GHz "safety-of-life" DSRC systems from harmful interference. Moreover, before any rules allowing 5.9 GHz U-NII use based on such testing are promulgated, the Commission should seek formal public comment on such rules to ensure that they adequately protect DSRC services.

## II. SUMMARY

### A. DSRC and Other Connected Vehicle Technologies Will Provide Significant Public Interest Benefits

DSRC and other connected vehicle technologies are poised to provide significant public safety, traffic management, environmental, and other benefits, and become central components of the nation's twenty-first century highway transportation system. DSRC is a wireless technology that uses the 5.9 GHz band for active vehicle safety systems, which may help prevent or mitigate traffic accidents by providing drivers with greater situational awareness of nearby

vehicles and roadway conditions (through audible/visual warning systems), and may in the future intervene in emergencies (by temporarily taking control of the vehicle braking/steering). It includes both V2V and V2I communications.

V2V is the wireless exchange of data between vehicles, allowing vehicles to sense each other and potential threats and hazards, while also providing feedback to help avoid or mitigate crashes.[8] V2I complements V2V by allowing the exchange of data between vehicles and roadway infrastructure, supplementing the public safety advantages of V2V and providing additional real-time traffic management and road condition information. In this way, mobility-based applications will increase the everyday utility of V2I and V2V systems for the general driving public. Together, these technologies have the potential to provide significant safety benefits to motorists; however, their tremendous promise is threatened by the unintended consequences of the Commission's NPRM and the potentially life threatening impact of U-NII operations in the 5.9 GHz band.

### B. DSRC Technologies in the 5.9 GHz Band Are at an Advanced Stage of Development and Are Near Widespread Deployment

Automakers have invested significant time and resources into DSRC. Technologies that utilize DSRC in the 5.9 GHz band are, in fact, at an advanced stage of development and are nearing readiness for deployment.[9] Message set standards to exchange DSRC information between vehicles manufactured by different automakers have been developed through the

---

[8] U.S. Department of Transportation ("USDOT"), Research and Innovative Technology Administration ("RITA"), Vehicle-to-Vehicle (V2V) Communications for Safety, http://www.its.dot.gov/research/v2v.htm ("RITA: V2V Communications").

[9] Intelligent Transportation Society of America, http://www.itsa.org/advocacy/safety-and-connected-vehicles-.

Society of Automotive Engineers ("SAE") standards-setting process.[10] An IEEE standard, 802.11p, the foundation of which includes the initial Wi-Fi standard, has also been developed for use in DSRC radio devices.[11] In addition, six agencies within the U.S. Department of Transportation ("USDOT") (the National Highway Traffic Safety Administration ("NHTSA"), Research and Innovative Technology Administration ("RITA"), Federal Highway Administration ("FHWA"), Federal Motor Carrier Safety Administration ("FMCSA"), Federal Transit Administration ("FTA"), and the Federal Railroad Administration) are currently conducting a large-scale Connected Vehicle Safety Pilot Program with private industry partners in Ann Arbor, Michigan to validate the effectiveness of DSRC technology and further study how drivers respond to the safety applications enabled in their vehicles.[12] The data collected through this pilot program will serve as the basis for a NHTSA decision expected later this year that could mandate the deployment of connected vehicle technologies in all new vehicles, facilitate voluntary installation of wireless devices in new cars, or spur further research and development.[13]

DSRC-enabled V2V technologies are also being deployed internationally. In Europe, ITS using DSRC will be deployed starting in 2015 on an opt-in basis,[14] and there are similar

---

[10] *See* SAE International, DSRC Implementation Guide (2010), *available at* http://www.sae.org/standardsdev/dsrc/DSRCImplementationGuide.pdf ("SAE DSRC Implementation Guide").

[11] *Id.* at 23.

[12] USDOT, RITA, Connected Vehicle Safety Pilot Program, http://www.its.dot.gov/factsheets/pdf/SafetyPilot_final.pdf.

[13] *Id.*

[14] *See* Press Release, Car 2 Car Communications Consortium, European vehicle manufacturers working hand in hand on development of cooperative Intelligent Transport Systems and Services (C-ITS) (Oct. 10, 2012) *available at* http://www.car-to-

initiatives in Japan, Korea, and China.[15] ABI Research estimates that government mandates and automotive industry initiatives will lead to the widespread adoption of connected vehicle technologies, pushing the penetration rate to 61.8 percent by 2027.[16]

### C. Allowing U-NII Use of the 5.9 GHz Band Could Cause Harmful Interference to and Undermine the Viability of "Safety-of-Life" DSRC Operations

Although the NPRM seeks comment on the potential use of U-NII devices in the 5.9 GHz band, it is unclear whether any such use of the band is compatible with "safety-of-life" DSRC services and, if so, under what conditions.

DSRC services such as V2V and V2I are "safety-of-life" services that cannot tolerate any interruption, delay, or degradation. Even minor interruptions or degradations of V2V or V2I could result in a failure of DSRC safety applications to help a driver avert preventable vehicle collisions. In 2006, the Commission recognized the importance of "safety-of-life" DSRC services and took the unusual step of designating specific DSRC frequencies (channels 172 and 184) strictly for safety-related communications.[17]

U-NII use of the 5.9 GHz band could cause harmful co-channel, adjacent channel, and out-of-band interference to DSRC services. For example, the bandwidth and power limit

---

car.org/index.php?eID=tx_nawsecuredl&u=0&file=fileadmin/downloads/forum08/PressReleases/Press_release_on_MoU.pdf&t=1369177568&hash=e10dbbc1b4f6ba5990d73e5b90ed19fc72b3b436.

[15] ABI Research, V2V Penetration in New Vehicles to Reach 62% by 2027 (2013), http://www.abiresearch.com/press/v2v-penetration-in-new-vehicles-to-reach-62-by-202 ("ABI Research: V2V Adoption").

[16] *Id.*

[17] *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), 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, WT Docket No. 01-90, ET Docket No. 98-95, RM-9096, *Memorandum Opinion and Order*, 21 FCC Rcd 8961, 8963 ¶ 1 (2006) ("*2006 MO&O*").

discrepancies between U-NII and DSRC systems could create substantial detection challenges for U-NII devices. Another likely source of co-channel interference is the certain increase of congestion in the DSRC channels from U-NII devices. These and other interference concerns are discussed in more detail in Section V and the attached Technical Appendix.

Alliance and Global members are currently investing in and developing DSRC services and technologies. If they cannot be absolutely certain that these connected vehicle technologies will be protected against harmful interference from U-NII devices, the potential improvements in road safety enabled by DSRC will never be realized. As discussed below, the full benefits of ITS will only be realized through significant penetration of outfitted vehicles with DSRC equipment. Moreover, automakers will not continue to invest in developing and deploying DSRC systems if DSRC's efficacy is compromised by the operation of U-NII devices in the 5.9 GHz band.

### D. It is Imperative that the Commission Await the Results of NTIA's 5.9 GHz Band Study and the Finalization of a U.S. Position on Compatibility Before Proceeding with a Proposal for U-NII Use

Earlier this year, the National Telecommunications and Information Administration's ("NTIA") 5 GHz Report concluded that more analysis is needed to determine whether the 5.9 GHz band can accommodate U-NII operations without causing harmful interference to "safety-of-life" DSRC operations.[18] NTIA is currently conducting additional analysis to determine the implications for DSRC of U-NII use of the band, which NTIA estimates will

[18] Department of Commerce, Evaluation of the 5350-5470 MHz and 5850-5925 MHz Bands Pursuant to Section 6406(b) of the Middle Class Tax Relief and Job Creation Act of 2012 at 5-13 (2013), *available at* http://www.ntia.doc.gov/files/ntia/publications/ntia_5_ghz_report_01-25-2013.pdf ("NTIA 5 GHz Report").

conclude with final recommendations to the Commission in mid-to-late 2014.[19] Additionally, the U.S. is currently developing a position on possible international uses of the 5.9 GHz band for the International Telecommunications Union's ("ITU") 2015 World Radiocommunication Conference ("WRC-15").[20] Before determining whether to allow U-NII use of the 5.9 GHz band, the Commission should await the results of NTIA's study, as well as bench and field testing of any possible prototype U-NII devices designed for use in the 5.9 GHz band, the completion of work by other domestic and international organizations that are studying potential uses of the 5.9 GHz band, and NHTSA's decision later this year regarding the future deployment of DSRC technologies. If, based on this activity, a concrete view is reached on whether and under what circumstances U-NII devices might be able to operate in the 5.9 GHz band without causing harmful interference to DSRC operations, the Commission should seek formal public comment on such view and any proposed rules for U-NII 5.9 GHz band operations. Because V2V and V2I technologies have the potential to improve traffic safety, such a thorough and rigorous review is essential and will allow all stakeholders to evaluate the Commission's proposal.

The Commission's Part 15 rules require that unlicensed spectrum devices not cause harmful interference to licensed services.[21] U-NII devices have not been shown to avoid interfering with licensed DSRC services, nor has there been any testing to date. Consistent with its legal mandate, the Commission should not allow U-NII operations in the 5.9 GHz band unless it is absolutely certain that such use will comport with its Part 15 rules.

---

[19] *Id.* at 6-4.

[20] *Id.* at 6-3.

[21] 47 C.F.R. § 15.5.

The Alliance and Global are prepared to work with the Commission, NTIA, advocates of 5.9 GHz U-NII use, and other stakeholders on these issues, and we have already begun such a dialog with proponents of U-NII 5.9 GHz use. However, anything short of a deliberate, data-driven testing process for evaluating U-NII/DSRC compatibility will raise serious concerns regarding the viability of DSRC.

## III. DSRC AND OTHER ITS TECHNOLOGIES ARE POISED TO BECOME CENTRAL COMPONENTS OF THE 21ST CENTURY HIGHWAY TRANSPORTATION SYSTEM

From all current indications, DSRC-based connected vehicle technology will be a leading factor in enabling the safe and efficient operation of the highway transportation system for the foreseeable future. With the number of vehicles on U.S. roads continuing to grow but construction of new road capacity likely limited, "smart" vehicles and roadway infrastructure will be necessary to allow the highway system to function in a safe, environmentally sustainable, and efficient manner. USDOT describes the potential for the technology as follows:

> The U.S. Department of Transportation is committed to improving safety and mobility on our nation's roadways. As we look ahead to the next stage of roadway safety in America, connected vehicle technology shows great promise in transforming the way Americans travel. Through wireless technology, connected vehicles ranging from cars to trucks and buses to trains could one day be able to communicate important safety and mobility information to one another that helps save lives, prevent injuries, ease traffic congestion, and improve the environment.[22]

### A. DSRC Services Will Improve Automobile Safety by Reducing Crashes

According to data from NHTSA, in 2011 there were 5,338,000 vehicle crashes, accounting for 32,367 deaths and 2,217,000 persons injured. In 2009, traffic fatalities were the

[22] USDOT Connected Vehicle Technology Fact Sheet, http://www.safercar.gov/ConnectedVehicles/pages/resources.html .

leading cause of death for Americans aged 4 and 11-27.[23] DSRC systems have the potential to make America's roadways safer by helping drivers avoid or mitigate crashes.

As discussed above, DSRC involves both V2V and V2I.[24] According to RITA, V2V has the potential to provide significant road safety benefits. V2V technologies exchange "vehicle-based data regarding position, speed, and location (at a minimum)," which "enables a vehicle to: sense threats and hazards with a 360 degree awareness of the position of other vehicles and the threat or hazard they present; calculate risk; issue driver advisories or warnings; or assist in taking pre-emptive actions to avoid and mitigate crashes."[25] USDOT's plan for DSRC includes, ultimately, making all vehicles (including commercial and public transit vehicles) V2V-enabled and capable of communicating with one another. According to NHTSA, these initial exchanges of data will support future generations of active safety applications and systems, which could "enable active safety systems that can assist drivers in preventing approximately 80% of non-impaired driving accidents."[26]

The benefits of V2V are complemented by connectivity between (1) vehicles and infrastructure, and (2) vehicles and consumer portable electronic devices.[27] V2I involves the "wireless exchange of critical safety and operational data between vehicles and highway

---

[23] USDOT, National Highway Traffic Safety Administration ("NHTSA"), Traffic Safety Facts: 2011 Data (2013), *available at* http://www-nrd.nhtsa.dot.gov/Pubs/811753.pdf.

[24] *NPRM* ¶ 93.

[25] RITA: V2V Communications.

[26] NHTSA, Connected Vehicles, Vehicle-to-Vehicle (V2V) Communications for Safety, http://www.safercar.gov/ConnectedVehicles/pages/v2v.html.

[27] *Id.*

infrastructure."[28] V2I enables transportation infrastructure to become "smart infrastructure" by using the data exchanged between vehicles and infrastructure elements to recognize high-risk situations before they occur and provide alerts and warnings to drivers. According to RITA, the vision for V2I is to deploy enough V2I-enabled infrastructure "to provide the maximum level of safety and mobility benefits for highway safety and operational efficiency nationwide."[29] According to NHTSA, V2I supplements the safety benefits of V2V and can help prevent another 12 percent of vehicle crashes.[30] In addition to its potential safety advantages, V2I can provide improvements in mobility and environmental benefits "by reducing delays and congestion caused by crashes, enabling wireless roadside inspections, or helping commercial vehicle drivers identify safe areas for parking."[31]

A number of additional V2V and V2I applications are being developed in the U.S. and through complementary work in Europe and Japan. These applications (which, like the other V2V and V2I applications mentioned above, require extremely low-latency, high availability communications) include:

- Pre-crash safety communications to reduce injuries when a crash is unavoidable;
- Systems to address violations of traffic control devices (traffic lights and stop signs) and curve-speed-warnings to prevent roadway departures;
- Extensions to road users, such as pedestrians, motorcycle riders, bicyclists, and others through smart phones or other wireless consumer devices;

---

[28] USDOT, RITA, Vehicle-to-Infrastructure (V2I) Communications for Safety, http://www.its.dot.gov/research/v2i.htm ("RITA: V2I Communications").

[29] *Id.*

[30] *Id.*

[31] *Id.*

- Enhancements to currently available systems, such as adaptive cruise control, lane departure prevention, and crash-imminent braking with increased availability, reliability and speed of information; and
- Applications that enable coordination of automated traffic streams.

Because these applications will continue to evolve over time, it is critical that the Commission protect all channels assigned to DSRC against harm or degradation from new U-NII use, and not just the channels currently designated for high-priority safety and public safety use (such as channels 172 and 184).

### B. DSRC Services Can Provide Significant Traffic Management Benefits, Further Improving Public Safety

Traffic congestion wastes time and money and causes unnecessary air pollution. In 2011, urban traffic congestion on U.S. roadways led to 5.5 billion hours of travel delay, increased travel times by almost 20 percent, and squandered more than $121 billion – approximately $818 per average commuter.[32] Traffic congestion also slows the movement of commodities by truck, costing $27 billion in wasted fuel in 2011.[33] Traffic accidents are a principal cause of traffic congestion, triggering about 25 percent of traffic congestion problems – second only to bottlenecks.[34] Bad weather, unexpected road construction, poor traffic signal timing, and special events also contribute significantly to traffic congestion.[35]

---

[32] Texas Transportation Institute, The 2012 Urban Mobility Report at 1, 5 (Dec. 2012), *available at* http://mobility.tamu.edu/ums/report/ ("2012 Urban Mobility Report").

[33] *Id.* at 14.

[34] USDOT, Federal Highway Administration (FHWA), Describing the Congestion Problem, http://www.fhwa.dot.gov/congestion/describing_problem.htm.

[35] *Id.*; *see also* 2012 Urban Mobility Report at 12.

RITA's Applications for the Environment: Real-Time Information Synthesis ("AERIS") program seeks to "generate and acquire environmentally-relevant real-time transportation data, and use these data to create actionable information that support and facilitate 'green' transportation choices by transportation system users and operators."[36] The AERIS program works in conjunction with V2V research efforts to mitigate the negative environmental impacts of surface transportation.[37] RITA is also pursuing Road Weather Connected Vehicle Applications. This program is intended to reduce crash risk due to inclement weather conditions, thereby increasing mobility and reducing road maintenance costs by providing data on real-time road conditions.[38]

Real-time communications between and among vehicles and roadside infrastructure using V2V, V2I, and other DSRC technologies can reduce traffic congestion, shorten travel times, improve traffic flow, and improve traffic signal timing.[39] The most apparent traffic management benefit of DSRC services is derivative – by reducing the number of traffic crashes, as discussed above, DSRC also reduces the incidence of traffic congestion.[40] V2I technologies also transform road infrastructure elements into "smart infrastructure," allowing the exchange of data between infrastructure and vehicles to enable real-time safety warnings, safety message monitoring, and

---

[36] USDOT, RITA, Applications for the Environment: Real-Time Information Synthesis (AERIS), http://www.its.dot.gov/aeris/.

[37] *Id.*

[38] *See* USDOT, RITA, Road Weather Connected Vehicle Applications, http://www.its.dot.gov/connected_vehicle/road_weather.htm.

[39] RITA: V2V Communications; *see also NPRM* ¶ 92.

[40] *See generally* Section III. A, *supra*.

driver information updates related to local traffic disruptions or severe weather.[41] Utilizing the wealth of information communicated between vehicles and infrastructure on existing roadways, DSRC services improve traffic flow and enable more effective traffic management algorithms in traffic signals, easing other common sources of congestion.[42]

### C. DSRC Services Can Provide Significant Environmental Benefits

Traffic congestion also causes massive environmental impacts. According to the Environmental Protection Agency, transportation is the second-largest emitting sector of carbon dioxide ($CO_2$) greenhouse gases, contributing to 32 percent of $CO_2$ emissions in 2010, with the majority of those emissions coming from vehicles operated for personal use.[43] A significant amount of these emissions come from cars and trucks going nowhere. In 2011, cars and trucks idling or inching along in bumper-to-bumper traffic pumped 56 billion pounds of $CO_2$ into the atmosphere, while wasting approximately 2.9 billion gallons of fuel.[44] In addition to greenhouse gas reduction, traffic congestion mitigation strategies have the potential to provide significant reductions in conventional pollutant (e.g., hydrocarbons, carbon monoxide, oxides of nitrogen, diesel particulate, etc.) emissions.[45] To the extent that DSRC services can reduce crashes,

---

[41] RITA: V2I Communications.

[42] *Id.*; 2012 Urban Mobility Report at 19 (discussing "prominent types of operational treatments," including programs studied by USDOT's Intelligent Transportation Systems Joint Program Office, and the potential benefits of these treatments).

[43] U.S. Environmental Protection Agency, Inventory of U.S. Greenhouse Gas Emissions and Sinks: 1990-2010 at ES-4, ES-8 (Apr. 2012), *available at* http://www.epa.gov/climatechange/Downloads/ghgemissions/US-GHG-Inventory-2012-Main-Text.pdf.

[44] 2012 Urban Mobility Report at 1, 13.

[45] *See* USDOT, FHWA, Air Quality programs, http://www.fhwa.dot.gov/environment/air_quality/.

improve traffic flow, or reduce the time drivers spend in stop-and-go traffic, they will also provide corresponding benefits for the environment.

### D. Congress and the Commission Have Long Recognized the Transportation Benefits of Interoperable ITS and DSRC Services

Over the past twenty years, Congress has authorized billions of dollars for ITS research and development. In addition, years of work by Congress, the Commission, USDOT, and the private sector have laid the groundwork for the coming connected vehicle deployments.

**Congress.** Congress created the ITS program in 1991 with enactment of the Intermodal Surface Transportation Efficiency Act of 1991 ("ISTEA"), which authorized $659 million for Federal research, development, and testing, and implementation of ITS.[46] Congress has continued to fund the ITS program through additional authorizations in 1998 ($1.3 billion through fiscal year 2003)[47] and 2005 ($110 million annually through fiscal year 2009).[48] In addition, in 2012 Congress enacted the Moving Ahead for Progress in the 21st Century Act ("MAP-21"), which authorized an additional $200 million for ITS research and deployment for fiscal years 2012 and 2013 and directed the Secretary of Transportation "to expedite … the development and deployment of intelligent transportation systems," carry out research and development and testing of ITS-enabled vehicles and infrastructure, and submit a report in 2015

[46] *See* Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA), Pub. L. 102-240, § 6059, 105 Stat. 1914 (1991).

[47] *See* Transportation Efficiency Act for the 21st Century (TEA-21), Pub. L. 105-178, 112 Stat. 107 (1998).

[48] *See* Safe Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users, Pub. L. 109-59, 119 Stat. 1144 (2005).

assessing the status of ITS systems and recommending a path for implementing DSRC technologies.[49]

In creating the ITS program, Congress found that "intelligent vehicle highway systems represent the best near-term technology for improving surface transportation for public benefit by providing equipment which can improve highway traffic flow and provide for enhanced safety."[50] In 1998, Congress explained that the investments authorized by ISTEA:

> demonstrated that intelligent transportation systems can mitigate surface transportation problems in a cost effective manner; and continued investment in architecture and standards development, research and systems integration is needed to accelerate the rate at which intelligent transportation systems are incorporated into the national surface transportation network, thereby improving transportation safety and efficiency and reducing costs and negative impacts on communities and the environment.[51]

Moreover, as RITA explains, the ITS program "was designed to facilitate deployment of technology to enhance the efficiency, safety, and convenience of surface transportation, resulting in improved access, saved lives and time, and increased productivity."[52]

**The Commission.** The Commission has also recognized the importance of DSRC for "safety-of-life" and public safety communications. In 2003, the Commission adopted licensing and service rules for DSRC technologies in the 5.9 GHz band to facilitate the development of

---

[49] *See* Moving Ahead for Progress in the 21st Century Act, Pub. L. 112-141, 126 Stat. 405 §§ 53001-53006 (2012).

[50] ISTEA, §6009(a)(6).

[51] TEA-21, § 5202(1)-(2).

[52] USDOT, RITA, Intelligent Transportation Systems Joint Program Office, http://www.its.dot.gov/faqs.htm. *See also 2003 Licensing & Service Order* ¶ 17 (adopting licensing and service rules for DSRC services in the 5.9 GHz band and stating that Congress' goal for the national ITS program was to "increase the safety and efficiency of the nation's surface transportation system").

new and innovative services.[53] The Commission's 2003 Order also adopted a band plan for DSRC services, creating seven, 10 megahertz channels in the band, consisting of one control channel (Channel 178) and six service channels (Channels 172, 174, 176, 180, 182, and 184), and one 5 MHz channel to be held in reserve.[54] In addition, the 2003 Order showed a keen understanding of the importance of DSRC services for "safety-of-life" and public safety communications by establishing a priority framework for those communications in the 5.9 GHz band control channel.[55]

The Commission subsequently amended the 5.9 GHz band plan in 2006 with "safety-of-life" and public safety applications in mind.[56] The 2006 Order designated Channel 172 exclusively for "vehicle-to-vehicle communications for accident avoidance and mitigation, and safety of life and property applications," and designated Channel 184 exclusively for "high-power, longer-distance communications to be used for public safety applications involving safety of life and property, including road intersection collision mitigation."[57] In designating the exclusive-use channels, the Commission explained that "[a]lthough the Commission has long recognized that shared use of spectrum promotes spectrum efficiency, there are cases in which public safety concerns dictate exclusive use of frequencies," and concluded that DSRC constituted such a case because "the delay associated with shared use of a time-critical DSRC

---

[53] *2003 Licensing and Service Order* ¶ 1.

[54] *Id.* ¶¶ 25-29.

[55] *Id.* ¶¶ 30-34.

[56] *See 2006 MO&O*.

[57] *Id.* ¶ 1.

channel could be literally life-threatening in the context of collision avoidance."[58] Such was the situation in 2006, and it remains so today.

**Industry Efforts.** Following the allocation of the 5.9 GHz band for use by DSRC systems, the Intelligent Transportation Society of America ("ITS America"), which at the time was the USDOT-selected Federal Advisory Committee on ITS matters, began holding industry and stakeholder meetings to develop a consensus on interoperability in the deployment of DSRC services.[59] In October 2000, ITS America filed a report with the Commission that addressed licensing and service rules, as well as deployment strategies for DSRC. In May 2002, the American Society for Testing and Materials Subcommittee E17.51 ("ASTM") (which had been working with the FHWA) selected the ASTM-DSRC E2212-013 Standard ("ASTM-DSRC Standard") as the standard for DSRC-based ITS applications in the 5.9 GHz band.[60] Finally, in 2010, the IEEE 802.11p standard was approved and will be "used as the groundwork for DSRC."[61]

## IV. DSRC CONNECTED VEHICLE TECHNOLOGY IS AT AN ADVANCED STAGE OF DEVELOPMENT, AND THE COMMISSION SHOULD PROCEED CAUTIOUSLY TO AVOID DISRUPTING ITS DEPLOYMENT

As discussed above, USDOT, the Commission, and industry stakeholders have laid the foundation for the widespread launch and adoption of DSRC-connected vehicle technologies. Working together, these parties have established standards and protocols for V2V and V2I technologies, established service rules and power levels for their operation, and designated

---

[58] *Id.* ¶ 16.

[59] *2003 Licensing and Service Order* ¶¶ 6, 9.

[60] *Id.* ¶ 9.

[61] SAE DSRC Implementation Guide at 23.

specific channels for their use. This tremendous industry and government effort was necessary to ensure that vehicles and equipment manufactured by different companies will be able to communicate with each other and with DSRC infrastructure, no matter where in the U.S. the need arises.

Federal agencies, vehicle and equipment manufacturers, standards-setting organizations, and other stakeholders are in the midst of numerous research initiatives designed to further develop and implement DSRC.[62] NHTSA, for example, is currently researching DSRC V2V to determine whether to adopt regulations on the future of connected vehicle technology.[63] These regulations could lead to mandated deployment of connected vehicle technologies in new vehicles or voluntary installation of V2V and V2I devices in new cars.[64] NHTSA is expected to reach a decision on this "priority project" in 2013.[65] Other research projects include efforts to globally harmonize connected vehicle technologies,[66] understand and plan for potentially distracting effects of DSRC technologies on drivers,[67] further refine the underlying technology platform,[68] implement certification requirements and mechanisms to protect consumer safety,

---

[62] USDOT, Intelligent Transportation Systems ("ITS"), Connected Vehicle Research, http://www.its.dot.gov/connected_vehicle/connected_vehicle.htm.

[63] *See* NHTSA, Vehicle Safety and Fuel Economy Rulemaking and Research Priority Plan 2011-2013 at 7 (2011), *available at* http://www.regulations.gov/contentStreamer?objectId=0900006480e78ab2&disposition=attachment&contentType=pdf.

[64] ABI Research: V2V Adoption.

[65] *Id.* at 7.

[66] USDOT, ITS, Human Factors Research, http://www.its.dot.gov/connected_vehicle/human_factors.htm.

[67] USDOT, ITS, Harmonization of International Standards and Architecture around the Vehicle Platform, http://www.its.dot.gov/research/harmonization.htm.

[68] USDOT, ITS, Vehicle to Vehicle Communications Systems Engineering, http://www.its.dot.gov/research/systems_engineering.htm.

security, and privacy,[69] and develop "connected vehicle test beds" to provide real-world, operational test beds for DSRC testing and certification activities.[70]

DSRC systems are already being tested in real-world environments. USDOT and the University of Michigan Transportation Research Institute are in the middle of a year-long Safety Pilot Model Deployment ("Safety Pilot") to "test the effectiveness of connected vehicle safety applications for reducing crashes, and show how drivers respond to these technologies while operating a vehicle in a real-world, multi-modal environment."[71] The Safety Pilot began with clinics that tested V2V technologies with hundreds of drivers in controlled environments across the country, and has now entered its second phase, the Safety Pilot Model Deployment.[72] The Safety Pilot Model Deployment utilizes a test site with multi-modal traffic and a high concentration of V2V-equipped vehicles, including a limited set of V2I technologies at intersections with traffic signals.[73] This deployment involves more than 2,800 vehicles, including a mix of cars, trucks, and buses (driven by volunteers from the general public who reflect the general driver population), traveling over 73 lane-miles of freeways and city streets in Northeast Ann Arbor, Michigan.[74] The empirical data collected through the Safety Pilot will "present a more accurate, detailed understanding of the potential safety benefits of these

---

[69] USDOT, ITS, Connected Vehicle Certification, http://www.its.dot.gov/connected_vehicle/connected_vehicle_cert.htm.

[70] USDOT, ITS, The Connected Vehicle Test Bed, http://www.its.dot.gov/testbed.htm.

[71] University of Michigan Transportation Research Institute, Safety Pilot, http://www.safetypilot.us/.

[72] University of Michigan Transportation Research Institute, Program Overview, http://www.safetypilot.us/program-overview.html ("UMTRI Program Overview").

[73] *Id.*

[74] University of Michigan Transportation Research Institute, How It Works, http://www.safetypilot.us/how-it-works.html.

technologies," as well as their non-safety benefits "relating to mobility and environmental impacts."[75]

Research is also underway to assess how these important DSRC services would be affected by U-NII use of the 5.9 GHz band. NTIA, for example, in conjunction with USDOT, is conducting a quantitative evaluation of the suitability of the 5.9 GHz band for U-NII device operations, and the implications such operations would have for DSRC.[76] Its activity will involve defining the technical characteristics of DSRC systems and U-NII device deployment and technical parameters, conducting simulations under various sharing scenarios, developing initial recommendations related to the suitability of the 5.9 GHz band for U-NII operations, performing laboratory and field measurements, and ultimately finalizing recommendations to the Commission and for international study.[77] As noted above, NTIA is expected to finalize its recommendations to the Commission between July 2014 and December 2014.[78]

The Commission must ensure that all of this promising activity is not undermined or nullified by an ill-informed decision to allow U-NII use of the 5.9 GHz band. Indeed, the fact that the Commission has sought comment on a broad proposal to allow U-NII use of the band has already chilled the discussion of potential investment in DSRC equipment.[79] If previous

---

[75] UMTRI Program Overview. The Safety Pilot assumes that there will be no U-NII device use in the 5.9 GHz band.

[76] NTIA 5 GHz Report at 6-3, 6-4; *see also* David Shepardson, *DOT Urges FCC not to award wireless spectrum without testing*, The Detroit News, May 7, 2013 *available at* http://www.detroitnews.com/article/20130507/AUTO01/305070427/1361/DOT-urges-FCC-not-to-award-wireless-spectrum-without-testing.

[77] *Id.* at 6-4.

[78] *Id.*

[79] *See* Paul Kirby, *Rohde Bemoans Impact of 5 GHz NPRM on Connected-Vehicle Firm*, TR Daily, May 20, 2013 (quoting Greg Rohde on behalf of Savari Networks, a developer of DSRC equipment, that the

experience with new wireless services is any indication, some level of marketplace anxiety will continue until the Commission makes clear its commitment to adequately protect DSRC services.

Such anxiety is not surprising given the experience of other primary users of the 5 GHz band that have been affected by U-NII operations. The NPRM noted that a few years ago NTIA field testing determined that the operation of U-NII devices in the 5.60-5.65 GHz band was causing harmful interference to Terminal Doppler Weather Radar ("TDWR"), which holds primary status in the band.[80] The interference was largely caused by U-NII devices that had been modified to operate outside their authorized spectrum bands.[81] While the interference from U-NII devices was first discovered in 2009, a resolution to the problem has not yet been reached.[82] Without assurance from the Commission that harmful interference to DSRC systems will not occur as a result of expanded U-NII operations, there could be a reduction in research and development and a further chilling of investment in DSRC systems, delaying and possibly foreclosing the widespread deployment of V2V and V2I technologies.

## V. THE COMMISSION SHOULD NOT ALLOW U-NII USE OF THE 5.9 GHZ BAND UNLESS IT CAN BE OBJECTIVELY DEMONSTRATED THAT SUCH USE WILL NOT INTERFERE WITH DSRC SYSTEMS

The Alliance and Global are concerned that DSRC services could be severely compromised by new unrestricted U-NII use of the 5.9 GHz band. The disruption of DSRC

---

Commission's proposal to allow U-NII devices to share the 5.9 GHz band had a "chilling effect" on discussions with potential investors).

[80] *NPRM* ¶ 8.

[81] *Id.* ¶ 9.

[82] *Id.* ¶ 10.

operations in the 5.9 GHz band would cripple the "safety-of-life" and other DSRC applications used for ITS – and threaten DSRC's viability. Prior to any final action in this proceeding, the Commission should demonstrate, through rigorous field and bench testing, that U-NII use of the band will not interfere with DSRC systems, and seek formal public comment on any proposed rules for U-NII 5.9 GHz use developed based on such testing. In that way, all relevant stakeholders will be able to evaluate the potential impact of the Commission's proposal.

### A. Interference Would Significantly Undermine the Safety Benefits of DSRC Systems and Threaten DSRC Deployment

#### 1. Interference to V2V and V2I Services Poses Significant Safety Risks

As the Commission has previously recognized, V2V and V2I applications are "exceptionally time-sensitive and should not be conducted on potentially congested channels."[83] This was precisely the Commission's rationale for designating DSRC channels 172 and 184 exclusively for "safety-of-life" and public safety applications, such as vehicle collision avoidance and mitigation.[84] In fact, "safety-of-life" applications such as V2V and V2I cannot tolerate even infrequent instances of harmful interference. The NPRM observed that applications that use V2V and V2I "need secure, wireless interface dependability in extreme weather conditions, and short time delays; all of which are facilitated by DSRC."[85] Any excessive congestion or interference could lead to increased latency, lost packets of data, or

[83] *2006 MO&O* ¶ 16.

[84] *Id.* ¶¶ 16-17.

[85] *NPRM* ¶ 93.

degraded security functions, significantly decreasing the safety benefits of such applications.[86] If signals are degraded or interrupted, or transmissions are not received, vehicle collisions that could have been prevented may occur.

Recognizing these risks, the Commission took the unusual step of designating specific DSRC frequencies (channels 172 and 184) strictly for safety-related communications.[87] In doing so, the Commission found that "vehicle-to-vehicle collision avoidance and mitigation applications are exceptionally time-sensitive and should not be conducted on potentially congested channels."[88] The Commission reasoned that DSRC public safety applications fall within that class of "cases in which public safety concerns dictate exclusive use of frequencies" because "the delay associated with shared use of a time-critical [DSRC] channel could be literally life-threatening in the context of collision avoidance."[89] Even a delay of milliseconds[90] – while the DSRC system electronically identified and executed the priority event – "could result in an otherwise avoidable vehicular collision."[91] Because DSRC is extremely latency-sensitive,

---

[86] John Maddox, University of Michigan Transportation Research Institute, ITS Spectrum Sharing? – a common sense approach at 9 (Apr. 2013) (included as Attachment 1).

[87] *2006 MO&O* ¶ 16.

[88] *Id.*

[89] *Id.*

[90] A millisecond is one – one thousandth (1/1,000) of a second. 1,000 milliseconds comprise one second. Motor vehicle crashes typically occur over a 100 to 150 millisecond interval. To gain an appreciation of the duration of a typical crash event, consider that light takes approximately 134 milliseconds to travel the circumference of the earth at its equator (a distance of approximately 40,000 kilometers or 25,000 miles) or that the average duration of a single human eye blink is between 100 and 400 milliseconds (see http://bionumbers.hms.harvard.edu/bionumber.aspx?s=y&id=100706&ver=0).

[91] *Id.*

any interference from U-NII devices will degrade DSRC performance and could be catastrophic for drivers.[92]

### 2. Potential Interference to V2V and V2I Services Will Undermine Their Deployment

The real safety benefits of V2V "can only be realized when a sufficiently large part of the installed vehicle base is connected."[93] The Alliance and Global members have worked (and continue to work) closely with federal agencies and other stakeholders to research and develop interoperable DSRC services and technologies, devoting substantial resources to these potentially life-saving applications. In its 2003 Order, the Commission explained that to accomplish the safety and efficiency goals of DSRC-based ITS applications, USDOT envisioned DSRC On Board Units ("OBUs") in every vehicle working with DSRC Road Side Units ("RSUs") embedded within the transportation infrastructure.[94] Because OBUs and RSUs are designed, developed, and manufactured by different automakers and other companies, standards-based interoperability is vital to the viability of DSRC equipment and services. To enable these communications, all DSRC equipment must be capable of communicating on the same frequency and in the same language, include security features that ensure trustworthy communications, and

---

[92] *See* Technical Appendix at 1.3.2 (explaining that U-NII devices operating in the 5.9 GHz band can cause significant interference to the reception of packets carrying safety and other communications. This interference could lead to an unknown and potentially very high rate of inter-packet gaps ("IPG") and packet error rate ("PER"), which would degrade the ability of the vehicle to perform real-time situational awareness and tracking of nearby vehicles and render it unable to provide timely safety warnings of an imminent collision).

[93] *2006 MO&O* ¶ 16.

[94] *2003 Licensing and Service Order* ¶ 14.

manage channel loading to ensure workable message frequencies and power levels.[95] Uncontrolled extraneous signals, such as those from U-NII devices, will therefore be problematic.

If interference to V2V and V2I services or congestion in the 5.9 GHz band minimizes or negates their potential safety benefits, consumers and government regulatory agencies are likely to reject the services. Consumer rejection, in turn, would undermine the development and deployment of these DSRC technologies, making it doubtful that the potentially revolutionary breakthroughs in vehicle and road safety enabled by DSRC will ever be realized. To promote continued investment, interoperability, and widespread consumer adoption, the Commission must ensure that connected vehicle technologies remain viable and not threatened by harmful interference. Without such assurance, the promise of connected vehicle technologies will be unfulfilled.

Finally, significant planning and engineering development has already taken place in reliance on the existing 5.9 GHz band spectral environment. For example, prior to the release of the NPRM, DSRC channel congestion concerns were being addressed based on the assumption that no U-NII devices would be operating in or near the band. Members of the Alliance and Global have invested tens of millions of dollars developing their interoperable DSRC systems in reliance upon the existing spectral environment, and changing that environment so dramatically at this stage would pose severe technical and financial challenges.[96] Moreover, specific changes

---

[95] As the Commission recognized, "[w]ithout an interoperability standard that enables units to communicate with one another regardless of location, equipment used, or the license, the overall effectiveness of the national DSRC operations would be drastically reduced." *Id.* ¶ 14.

[96] *See* Shepardson, *supra* note 76 (noting since 2005 automakers and governments have spent approximately $130 million researching and testing connected vehicle technologies).

to the DSRC service rules aimed at facilitating compatibility with U-NII use of the 5.9 GHz band would require the Commission to commence a separate rulemaking proceeding, which would create significant uncertainty regarding DSRC's operating environment and, ultimately, its time-to-market.

### B. U-NII Use of the 5.9 GHz Band Poses a Significant Interference Threat to DSRC Systems and Road Safety

U-NII use of the 5.9 GHz band could cause harmful co-channel, adjacent channel, and out-of-band interference to DSRC services. As Deputy Transportation Secretary John Porcari has explained, it is unknown whether the Commission's spectrum sharing proposal "will meet DOT's safety requirements and support existing technical standards."[97] Several key interference possibilities are discussed briefly below, and in more detail in the attached Technical Appendix ("TA"). Since applications will continue to evolve over time, it is critical that the Commission protect all channels assigned to DSRC against degradation from new U-NII use. To do otherwise would limit future innovations in the band.

#### 1. U-NII Devices in the 5.9 GHz Band Could Cause Harmful Co-Channel Interference

**Detection Issues Due to Channel Size Disparities.** One potential cause of co-channel interference is the bandwidth discrepancy between U-NII and DSRC technologies. This discrepancy could create lower layer sensing conflicts between the two operations.[98] As IEEE 802.11 Wi-Fi devices, U-NII devices operate based on 20 MHz wide (or wider) channels, while DSRC is licensed and designed for use over 10 MHz channels. Because current Wi-Fi devices

---

[97] *Id.*

[98] *See* Technical Appendix at 1.4.1.

have not been designed to detect 10 MHz channel widths, they would need to be modified (to be capable of verifying that two or more DSRC channels are clear simultaneously) in order to detect DSRC packets and avoid interfering with the DSRC transmissions. Such a redesign would require significant testing both in the laboratory and field to verify its efficacy.

Even if U-NII transmitters were able to achieve the difficult task of simultaneously monitoring two or more DSRC channels, the nomadic nature of vehicle traffic raises questions whether U-NII devices could avoid interfering with DSRC systems. DSRC V2V systems are constantly in motion and do not continuously transmit, which creates significant detection challenges for U-NII devices.[99] Moreover, the absence of DSRC transmissions at any given time or place has little bearing on the probability that DSRC transmissions will occur in the future. When a quiet DSRC device initiates a transmission, a U-NII device must not only detect it in mid-operation, but must instantaneously vacate the channel. This requires the U-NII device to continually monitor the channel on which it is transmitting, which is difficult.

If U-NII devices cannot detect DSRC signals, they will transmit at the same time as DSRC safety messages, causing harmful interference and disrupting, delaying, or degrading the delivery of the DSRC packets with consequential safety implications.[100] In such instances, significant sequences of DSRC packets supporting crash-avoidance safety applications could become unreadable, rendering DSRC "safety-of-life" systems ineffective when called upon.[101]

---

[99] NTIA 5 GHz Report at 5-11.

[100] *See* Technical Appendix at 1.5.2 (it is possible that a DSRC channel could be detected by a U-NII device as "clear" at a time when DSRC vehicles are just coming into range. The subsequent U-NII transmission could then unknowingly disrupt DSRC transmissions).

[101] *See id.* at 1.4.3.

**Power Limit Disparities and Sensing Concerns.** Another potential cause of co-channel interference to DSRC systems from U-NII devices is the disparity in power levels between U-NII devices and DSRC applications. Existing U-NII 5 GHz signal detection technology was not developed to detect DSRC signals, but was instead designed to detect high-power radar signals. It is unclear whether existing U-NII signal detection technology can be viably modified to detect transient-low power DSRC signals.[102]

Currently, V2V safety applications operate at a power range of 18-20 dBm EIRP.[103] The NPRM proposed to allow U-NII devices to operate in the 5.9 GHz band at significantly higher power levels, with a "maximum output power limit [that] is the lesser of 1 Watt and 17 dBm + 10 Log (B) where B is 26 dB emission bandwidth."[104]

The prospect of asymmetrical sensing is a major concern. Because U-NII devices are likely to operate at considerably higher power levels than are DSRC applications, the U-NII devices may be unable to "hear" DSRC operations when higher-powered U-NII devices are also present. As a result, U-NII packets may be sent at the same time that DSRC units attempt to send critical safety communications, causing the DSRC packets to be unreadable by DSRC receiving devices.[105]

**Channel Congestion.** Another likely source of co-channel interference is the certain increase of congestion in the DSRC channels from U-NII devices. Channel congestion on DSRC V2V safety channels is expected to be common in major metropolitan areas, where significant

---

[102] NTIA 5 GHz Report at 5-10, 5-12.

[103] Technical Appendix at 1.4.3.

[104] *NPRM* ¶ 97.

[105] Technical Appendix at 1.4.3.

numbers of deployed U-NII devices are expected. Even if the U-NII devices were running at very low power or operating at significant distance from the vehicles using DSRC, the aggregation of many such U-NII devices would raise the noise floor within the DSRC band, potentially causing harmful interference.[106] Moreover, the Commission will have no control over unlicensed users of the 5.9 GHz band (or even a mechanism for reliably tracking those users), which could result in instances of user misbehavior and disregard for the Commission's rules, causing further harmful interference.

While the NPRM proposes allowing U-NII devices to operate both indoors and outdoors in the 5.9 GHz band,[107] congestion in the band would remain a concern even if the Commission restricted U-NII devices to indoor use. If the Commission adopted an indoor only restriction for 5.9 GHz U-NII devices, it would not be able to exercise the necessary oversight to ensure that the rule was followed. A U-NII device user could simply walk outdoors, making any such restriction superfluous. Further, it is not apparent how radio frequency-permeable openings (*e.g.*, windows) in buildings could be prevented from allowing significant leakage from U-NII devices to the outdoor environment where the transmissions could disrupt DSRC operations.

### 2. Adjacent Channel and Adjacent Band Operations by U-NII Devices Could Cause Harmful Interference to DSRC Systems

Because U-NII devices operating in or adjacent to the 5.9 GHz band would transmit at significantly higher maximum power levels than DSRC systems, U-NII operations in or near the 5.9 GHz band have the potential to cause harmful interference to sensitive DSRC safety applications.

---

[106] *See id.* at 1.4.4, 1.5.6.

[107] *NPRM* ¶ 97.

**Adjacent Channel Interference.** As detailed above, the Commission specified Channels 172 and 184 for V2V for vehicle collision avoidance and mitigation and public safety applications. These channels were set aside for specific uses in order to separate "safety-of-life" services from other, higher-powered DSRC operations. The Commission's proposal to permit U-NII devices to operate in the 5.9 GHz band would allow the unlicensed devices to operate at a maximum power level that is significantly higher than the power levels being used for DSRC safety services. This high-powered U-NII use could cause harmful interference to sensitive V2V safety applications, even when U-NII devices are transmitting on an adjacent channel.[108]

**Out-of-Band Interference.** Finally, even if U-NII devices are not permitted to operate in the 5.9 GHz band, placing U-NII operations in spectrum bands that are immediately or closely adjacent to channels used for V2V safety applications would still have the potential to cause harmful interference. The maximum power levels and antenna gain requirements that the Commission has proposed for U-NII operations[109] increase the likelihood that such operations in adjacent or proximate bands will cause harmful interference to DSRC safety applications.[110]

### C. The Commission Should Await the Results of NTIA's Study and Other Efforts Regarding the Compatibility of U-NII Use of the 5.9 GHz Band with DSRC and Seek Public Comment on a Proposal for U-NII 5.9 GHz Use Based on Such Efforts

As discussed above, NTIA's January 2013 report on U-NII use of the 5.9 GHz band raised numerous concerns regarding whether U-NII use of the band could be compatible with

---

[108] *See* Technical Appendix at 1.6.1, 1.7-1.7.5.

[109] *See NPRM* ¶ 97 (proposing antenna gain requirement of 6 dBi for non-point to-point systems and 23 dBi for point-to-point systems).

[110] *See* Technical Appendix at 1.6.2.

DSRC use.[111] NTIA identified a number of risk elements to DSRC services associated with U-NII use, arising primarily from the fact that existing U-NII regulations, devices, and technologies were not developed with DSRC in mind.[112] NTIA is in the process of conducting further studies on the suitability of the 5.9 GHz band for U-NII use and plans to submit recommendations to the Commission between July and December 2014.[113] And USDOT officials have said that "thorough, independent, and accurate testing … must be completed before the final decision on sharing the spectrum is made."[114]

In addition to NTIA's domestic work, the United States is further investigating compatibility between U-NII devices and DSRC operations as it develops its position on possible uses of the 5.9 GHz band internationally for the ITU's WRC-15 and other fora.[115] This international work is being performed under the State Department's International Telecommunication Advisory Committee ("ITAC"), which is studying U-NII and incumbent system characteristics to address the risks identified by NTIA's 5 GHz Report and determine whether and under what conditions spectrum sharing might be possible.[116] These studies must be finalized by the end of 2014, coinciding with the finalization of NTIA's study, in preparation for WRC-15. Additionally, other nations are likely to proffer their own studies on uses of the 5.9 GHz band before and at WRC-15.[117]

---

[111] NTIA 5 GHz Report at 5-12.

[112] *Id.* at 5-10, 5-11, and 5-12.

[113] *Id.* at 6-4.

[114] Shepardson, *supra* note 76 (quoting Deputy Transportation Secretary John Porcari).

[115] NTIA 5 GHz Report at 6-3.

[116] *Id.*

[117] *Id.*

The Commission should await the results of the NTIA analysis and the conclusion of ITAC's study of interference risks in the 5.9 GHz band, and leverage international work on this issue as well, to develop a fully informed proposal regarding potential U-NII use of the 5.9 GHz band. Once a proposed course of action has been developed, and consistent with the Administrative Procedure Act ("Act"), the Commission should seek formal public comment on such proposal, including any U-NII rules or restrictions that might be envisioned. The Commission should not take premature action now regarding shared use of 5.9 GHz spectrum, as doing so would involve incomplete, inconclusive data regarding the grave risks posed by 5.9 GHz U-NII use to life-saving DSRC technologies.

### D. The Alliance and Global Are Prepared to Work With All Stakeholders to Find a Solution to Interference Issues, if Possible

The Alliance and Global have started to engage with advocates of U-NII use of the 5.9 GHz band in an attempt to resolve these very important interference issues. While the Alliance and Global recognize the importance of the Commission's goals to free up additional spectrum for Wi-Fi use and welcome the opportunity to ascertain whether DSRC systems for ITS can coexist with U-NII devices in the band, we are skeptical that the Commission's current plan would effectively protect 5.9 GHz DSRC operations and have indicated as such to U-NII stakeholders. It is the Alliance and Global's view that DSRC, as a licensed service in the 5.9 GHz band and an enabler of "safety-of-life" V2V or V2I systems, should receive significant protection from any U-NII operations in the 5.9 GHz band. As noted previously, current U-NII devices use higher transmit powers and larger channel bandwidths than DSRC. This poses a considerable risk of causing harmful interference to 5.9 GHz DSRC systems.