DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

49 CFR Part 571

[Docket No. NHTSA-2016-0126]

RIN 2127-AL55

Federal Motor Vehicle Safety Standards; V2V Communications

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT)

ACTION: Notice of Proposed Rulemaking (NPRM).

NOTE: This document has been signed and we are submitting it for publication in the Federal Register. While we have taken steps to ensure the accuracy of this Internet version of the document, it is not the official version. Please refer to the official version in a forthcoming Federal Register publication or on GPO's Web Site. You can access the Federal Register at: www.federalregister.gov.

SUMMARY: This document proposes to establish a new Federal Motor Vehicle Safety Standard (FMVSS), No. 150, to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions. This will create an information environment in which vehicle and device manufacturers can create and implement applications to improve safety, mobility, and the environment. Without a mandate to require and standardize V2V communications, the agency believes that manufacturers will not be able to move forward in an efficient way and that a critical mass of equipped vehicles would take many years to develop, if ever. Implementation of the new standard will enable vehicle manufacturers to develop safety applications that employ V2V communications as an input, two of which are estimated to prevent hundreds of thousands of crashes and prevent over one thousand fatalities annually.

DATES: Comments must be received on or before [INSERT DATE 90 DAYS AFTER PUBLICATION IN THE **FEDERAL REGISTER**.]

ADDRESSES: You may submit comments to the docket number identified in the heading of this document by any of the following methods:

- Online: Go to http://www.regulations.gov and follow the online instructions for submitting comments.
- Mail: Docket Management Facility, M-30, U.S. Department of Transportation, West Building, Ground Floor, Rm. W12-140, 1200 New Jersey Avenue, SE, Washington, DC 20590.
- Hand Delivery or Courier: West Building, Ground Floor, Rm. W12-140, 1200 New Jersey Avenue, SE, between 9 am and 5 pm Eastern Time, Monday through Friday, except Federal Holidays.
- Fax: (202) 493-2251.

Regardless of how you submit your comments, you should mention the docket number of this document. You may call the Docket Management Facility at 202-366-9826.

Instructions: Direct your comments to Docket No. NHTSA-2016-0126. See the **SUPPLEMENTARY INFORMATION** section on "Public Participation" for more information about submitting written comments.

NOTE: This document has been signed and we are submitting it for publication in the Federal Register. While we have taken steps to ensure the accuracy of this Internet version of the document, it is not the official version. Please refer to the official version in a forthcoming Federal Register publication or on GPO's Web Site. You can access the Federal Register at: www.federalregister.gov.

Docket: All documents in the dockets are listed in the http://www.regulations.gov index. Although listed in the index, some information is not publicly available, e.g., confidential business information (CBI) or other information whose disclosure is restricted by statute. Publicly available docket materials are available either electronically in regulations.gov or in hard copy at DOT's Docket Management Facility, 1200 New Jersey Avenue, SE, West Building, Ground Floor, Rm. W12-140, Washington, DC 20590. The Docket Management Facility is open between 9 am and 5 pm Eastern Time, Monday through Friday, except Federal Holidays.

FOR FURTHER INFORMATION CONTACT: For technical issues, Mr. Gregory Powell, Office of Rulemaking, NHTSA, 1200 New Jersey Avenue, SE, Washington, DC 20590. Telephone: (202) 366-5206; Fax: (202) 493-2990; email: gregory.powell@dot.gov. For legal issues, Ms. Rebecca Yoon, Office of the Chief Counsel, NHTSA, 1200 New Jersey Avenue, SE, Washington, DC 20590. Telephone: (202) 366-2992; email: rebecca.yoon@dot.gov.

Contents

I. Executive Summary

The National Highway Traffic Safety Administration (NHTSA) is proposing to issue a new Federal Motor Vehicle Safety Standard (FMVSS) No. 150, to require all new light vehicles to be capable of Vehicle-to-Vehicle ("V2V") communications, such that they will send and receive Basic Safety Messages to and from other vehicles. The proposal contains V2V communication performance requirements predicated on the use of on-board dedicated short-range radio communication (DSRC) devices to transmit Basic Safety Messages (BSM) about a vehicle's speed, heading, brake status, and other vehicle information to surrounding vehicles, and receive the same information from them. When received in a timely manner, this information would help vehicle systems identify potential crash situations with other vehicles and warn their drivers. The proposal also provides a path for vehicles to comply by deploying other technologies that meet certain performance and interoperability requirements, including interoperability with DSRC.

The agency believes that V2V has the potential to revolutionize motor vehicle safety. By providing drivers with timely warnings of impending crash situations, V2V-based safety applications could potentially reduce the number and severity of motor vehicle crashes, thereby reducing the losses and costs to society that would have resulted from these crashes.

More specifically, the agency believes that V2V will be able to address crashes that cannot be prevented by current in-vehicle camera and sensor-based technologies ("vehicle-resident" technologies). This is because V2V would employ omnidirectional radio signals that provide 360 degree coverage along with offering the ability to "see" around corners and "see" through other vehicles. V2V is not restricted by the same line-of-sight limitations as crash avoidance technologies that rely on vehicle-resident sensors. Additionally, V2V communications (BSMs) contain additional information, such as path predictions and driver actions (braking, steering) not available from traditional sensors. This information can be used by receiving vehicles to more reliably predict potential collision events as well as reduce false warnings. This ability to communicate certain information that cannot be acquired by vehicle-resident onboard sensors makes V2V particularly good at preventing impending intersection crashes, such as when a vehicle is attempting to make a left turn from one road to another. V2V also offers an operational range of 300 meters or farther between vehicles, nearly double the detection distance afforded by some current and near-term vehicle-resident systems. These unique characteristics allow V2V-equipped vehicles to perceive and warn drivers of some threats sooner than vehicle-resident sensors can. Furthermore, while the operational status or accuracy of vehicle-resident sensors may be affected by weather, sunlight, shadows, or cleanliness, V2V technology does not share these same system limitations.

As another source of information about the driving environment, moreover, the agency also believes that V2V can be fused with existing radar- and camera-based systems to provide even greater crash avoidance capability than either approach alone. For vehicles equipped with current on-board sensors, the fundamentally different, but complementary, information stream provided by V2V has the potential to significantly enhance the reliability and accuracy of the

sensor-based information available. Instead of relying on each vehicle to sense its surroundings on its own, V2V enables surrounding vehicles to help each other by conveying safety information about themselves to other vehicles. V2V communication can thus detect threat vehicles that are not in the sensors' field of view, and can use V2V information to validate a return signal from a vehicle-based sensor. Further, V2V can provide information on the operational status (e.g., brake pedal status, transmission state, stability control status, vehicle at rest versus moving, etc.) of other V2V-equipped vehicles. Similarly, vehicle-resident systems can augment V2V systems by providing the information necessary to address other crash scenarios not covered by V2V communications, such as lane and road departure. These added capabilities can potentially lead to more timely warnings and a reduction in the number of false warnings, thereby adding confidence to the overall safety system, and increasing consumer satisfaction and acceptance. Although some have contended that vehicle-resident systems could evolve to the point where they have similar ranges to V2V transmissions during the time it will take V2V to penetrate the fleet, the agency believes that these technologies will remain complementary rather than competing even as vehicle-resident systems continue to improve.

In the longer-term, the agency believes that this fusion of V2V and vehicle-resident technologies will advance the further development of vehicle automation systems, including the potential for truly self-driving vehicles. Although most existing automated systems currently rely on data obtained from vehicle-resident technologies, we believe that data acquired from GPS and telecommunications like V2V could significantly augment such systems. Communication-based technology that connects vehicles with each other could not only improve the performance of automated onboard crash warning systems, but also be a developmental stage toward achieving widespread deployment of safe and reliable automated vehicles.[1]

Despite these potential benefits, V2V offers challenges that are not present in vehicle-resident systems. Without government action, these challenges could prevent this promising safety technology from achieving sufficiently widespread use throughout the vehicle fleet to achieve these benefits. Most prominently, vehicles need to communicate a standard set of information to each other, using interoperable communications that all vehicles can understand. The ability of vehicles to both transmit and receive V2V communications from all other vehicles equipped with a V2V communications technology is referred to in this document as "interoperability," and it is vital to V2V's success. Without interoperability, manufacturers attempting to implement V2V will find that their vehicles are not necessarily able to communicate with other manufacturers' vehicles and equipment, defeating the objective of the

[1] Equipping vehicles with V2V could also lead to deployment of connectivity hardware that could potentially be used for other applications, such as connectivity with roadway infrastructure (V2I) and with pedestrians (V2P). These technologies (collectively referred to as "V2X") could increase the vehicle's awareness of its surroundings and enable additional applications. We do not consider these other potential applications here.

mandate and stifling the potential for innovation that the new information environment can create. In addition, there is the issue of achieving critical mass: that V2V can only begin to provide significant safety benefits when a significant fraction of vehicles comprising the fleet can transmit and receive the same information in an interoperable fashion.

The improvement in safety that results from enabling vehicles to communicate with one another depends directly on the fraction of the vehicle fleet that is equipped with the necessary technology, and on its ability to perform reliably. In turn, the effectiveness of any V2V communications technology depends on its ability to reliably transmit and receive recognizable and verifiable standardized information. Because the value to potential buyers of purchasing a vehicle that is equipped with V2V communications technology depends upon how many other vehicle owners have also purchased comparably-equipped models, V2V communications has many of the same characteristics as more familiar network communications technologies.

Viewed another way, an important consequence of any improvement in fleet-wide vehicle safety that results from an individual buyer's decision to purchase a V2V-capable model is the resulting increase in the safety of occupants of other V2V-equipped vehicles. Thus the society-wide benefits of individual vehicle buyers' decisions to purchase V2V-capable models extend well beyond the direct increase in their own safety; in economic parlance, their decisions can confer external benefits on other travelers. Thus a significant "network externality" arises from a new vehicle buyer's decision to purchase a vehicle equipped to connect to the existing V2V communications network.

Conversely, however, the benefits that any individual consumer would receive from voluntary adoption of V2V depend directly on the voluntary adoption of this technology by other consumers. Unless individual buyers believe that a significant number of other buyers will obtain V2V systems, they may conclude that the potential benefits they would receive from this system are unlikely to materialize. As a consequence, they are less likely to invest in V2V communications capabilities that would be would be justified by the resulting improvement in fleet-wide safety. The proposed requirement that all new vehicles be V2V-capable is thus likely to improve transportation safety more rapidly, effectively, and ultimately more extensively than would result from relying on the private decisions of individual vehicle buyers.

Another important consideration in achieving safety benefits from V2V is the long product lifespan of motor vehicles and the resulting slow fleet turnover. This places inherent constraints on the rate at which diffusion of new technologies throughout the entire vehicle fleet can occur. Thus in order to reach the critical mass of participants, a significant portion of the existing vehicle fleet will need replacement and a sustained, coordinated commitment on the part of manufacturers. Due to the inherent characteristics of the automobile market, manufacturers will inevitably face changing economic conditions and perhaps imperfect signals from vehicle buyers and owners, and these signals may not be based on complete information about the effectiveness of V2V technology, or incorporate the necessary foresight to value the potential life-saving benefits of V2V technology during the crucial phase of its diffusion. Without government intervention, the resulting uncertainty could undermine manufacturer plans or weaken manufacturers' incentive to develop V2V technology to its full potential.

We are, therefore, confident that creating the information environment through this mandate would lead to considerable advances in safety, and that those advances might not reach fruition if V2V communications were left to develop on their own.[2]

Overview of the Proposed Rule

The agency believes the market will not achieve sufficient coverage absent a mandate V2V capability for all new light vehicles. A V2V system as currently envisioned would be a combination of many elements. This includes a radio technology for the transmission and reception of messages, the structure and contents of "basic safety messages" (BSMs), the authentication of incoming messages by receivers, and, depending on a vehicle's behavior, the triggering of one or more safety warnings to drivers.

The agency is also proposing to require that vehicles be capable of receiving over-the-air (OTA) security and software updates (and to seek consumer consent for such updates where appropriate). In addition, NHTSA is also proposing that vehicles contain "firewalls" between V2V modules and other vehicle modules connected to the data bus to help isolate V2V modules being used as a potential conduit into other vehicle systems.

The NPRM presents a comprehensive proposal for mandating DSRC-based V2V communications. That proposal includes a pathway for vehicles to comply using non-DSRC technologies that meet certain performance and interoperability standards. A key component of interoperability is a "common language" regardless of the communication technology used. Therefore, the agency's proposal includes a common specification for basic safety message (BSM) content regardless of the potential communication technology. The proposal also provides potential performance-based approaches for two security functions in an effort to obtain reaction and comment from industry and the public. Following is a more comprehensive discussion of the proposal and potential alternatives for different aspects of V2V security:

Communication Technology

- Proposal: NHTSA proposes to mandate DSRC technology – A DSRC unit in a vehicle sends out and receives "basic safety messages" (BSMs). DSRC communications within the 5.850 to 5.925 MHz band are governed by FCC 47 CFR Parts 0, 1, 2 and 95 for onboard equipment and Part 90 for road side units. In reference to the OSI model, the physical and data link layers (layers 1and 2) are addressed primarily by IEEE 802.11p as well as P1609.4; network, transport, and session layers (3,4 and 5) are addressed primarily by P1609.3; security

[2] This analysis for this proposal focuses on the benefits resulting from the implementation of safety applications that are projected to reduce vehicle crashes. The agency did not incorporate any potential benefits from the anticipated expanded use of DSRC for mobility and envirionment benefits. A list of potential mobility and environment applications can be found at http://www.its.dot.gov/pilots/cv_pilot_apps.htm (last accessed: Dec 7, 2016)

communications are addressed by P1609.2; and additional session and prioritization related protocols are addressed by P1609.12. This mandate could also be satisfied using non-DSRC technologies that meet certain performance and interoperability standards.

Message Format and Information

- NHTSA proposes to standardize the content, initialization time, and transmission characteristics of the Basic Safety Message (BSM) regardless of the V2V communication technology potentially used. The agency's proposed content requirements for BSMs are largely consistent with voluntary consensus standards SAE 2735 and SAE 2945 which contains data elements such as speed, heading, trajectory, and other information, although NHTSA purposely does not require some elements to alleviate potential privacy concerns. Standardizing the message will facilitate V2V devices "speaking the same language," to ensure interoperability. Vehicles will not be able to "understand" the basic safety message content hindering the ability to inform drivers of potential crashes.

Message Authentication

- Public Key Infrastructure Proposal: NHTSA proposes V2V devices sign and verify their basic safety messages using a Public Key Infrastructure (PKI) digital signature algorithm in accordance with performance requirements and test procedures for BSM transmission and the signing of BSMs. The agency believes this will establish a level of confidence in the messages exchanged between vehicles and ensure that basic safety message information is being received from devices that have been certified to operate properly, are enrolled in the security network, and are in good working condition. It is also important that safety applications be able to distinguish these from messages originated by "bad actors," or defective devices, as well as from messages that have been modified or changed while in transit.

- Alternative Approach – Performance-based Only: This first alternative for message authentication is less prescriptive and defines a performance-based approach but not a specific architecture or technical requirement for message authentication. This performance only approach simply states that a receiver of a BSM message must be able to validate the contents of a message such that it can reasonably confirm that the message originated from a single valid V2V device, and the message was not altered during transmission. The agency seeks comment on this potential alternative.

- Alternative Approach -- No Message Authentication: This second alternative stays silent on a specific message authentication requirement. BSM messages

would still be validated with a checksum, or other integrity check, and be passed through a misbehavior detection system to attempt to filter malicious or misconfigured messages. Implementers would be free to include message authentication as an optional function. The agency seeks comment on this potential alternative.

Misbehavior Detection and Reporting

- Primary Misbehavior Detection and Reporting Proposal: NHTSA proposes to mandate requirements that would establish procedures for communicating with a Security Credential Management System to report misbehavior; and learn of misbehavior by other participants. This includes detection methods for a device hardware and software to ensure that the device has not been altered or tampered with from intended behavior. This approach enhances the ability of V2V devices to identify and block messages from other misbehaving or malfunctioning V2V devices.

- Misbehavior Detection Alternative Approach: An alternative for misbehavior detection imposes no requirement to report misbehavior or implement device blocking based to an authority. However, implementers would need to identify methods that check a devices' functionality, including hardware and software, e to ensure that the device has not been altered or tampered with from intended behavior. Implementers would be free to include misbehavior detection and reporting and as optional functions. The agency seeks comment on this alternative.

Hardware Security

NHTSA proposes that V2V equipment be "hardened" against intrusion (FIPS-140 Level 3) by entities attempting to steal its security credentials.

Effective Date

The agency is proposing that the effective date for manufacturers to begin implementing these new requirements would be two model years after the final rule is adopted, with a three year phase-in period to accommodate vehicle manufacturers' product cycles. Assuming a final rule is issued in 2019, this would mean that the phase-in period would begin in 2021, and all vehicles subject to that final rule would be required to comply in 2023.

Safety Applications

The agency is not proposing to require specific V2V safety applications at this time. We believe the V2V communications we are proposing will create the standardized information environment that will, in turn, allow innovation and market competition to develop improved

safety and other applications. Additionally, at this time, the agency believes that more research is likely needed in order to create regulations for safety applications. In support of this, we are seeking comment on information that could inform a future decision to mandate any specific safety applications.

Authority

Under the Vehicle Safety Act, 49 U.S.C. 30101 et seq., the agency has the legal authority to require new vehicles to be equipped with V2V technology and to use it, as discussed in Section VI below. NHTSA has broad statutory authority to regulate motor vehicles and items of motor vehicle equipment, and to establish FMVSSs to address vehicle safety needs.

Privacy and Security

V2V systems would be required to be designed from the outset to minimize risks to consumer privacy. The NPRM proposes to exclude from V2V transmitting information that directly identifies a specific vehicle or individual regularly associated with a vehicle, such as owner's or driver's name, address, or vehicle identification numbers, as well as data "reasonably linkable"[3] to an individual. Additionally, the proposal contains specific privacy and security requirements with which manufacturers would be required to comply.

The Draft Privacy Impact Assessment that accompanies this proposal contains detailed information on the potential privacy risks posed by the V2V communications system, as well as the controls designed into that system to minimize risks to consumer privacy.

Estimated costs and benefits

In this NPRM, the agency proposes that all light vehicles be equipped with technology that allows for V2V communications, but has decided not to propose to mandate any specific safety applications at this time, instead allowing them to be developed and adopted as determined by the market. This market-based approach to application development and deployment makes estimating the potential costs and benefits of V2V quite difficult, because the

[3] NHTSA intends for the term "reasonably linkable," as used in this NPRM, to have the same meaning as the term "as a practical matter linkable" as used in the definition of "personal data" in Section 4 of the White House Consumer Privacy Bill of Rights: "data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practical matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual." https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (last accessed Dec 7, 2016). The Federal Trade Commission also uses the concept of " linked or reasonably linkable" as a suggested definition of personally identifiable information in its recent comment to the Federal Communications Commission at https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf (last accessed Dec 7, 2016).

V2V communication technology being mandated by the agency would improve safety only indirectly, by facilitating the deployment of previously developed OEM safety application. However, the agency is confident that these technologies will be developed and deployed once V2V communications are mandated and interoperable. Considerable research has already been done on various different potential applications, and the agency believes that functioning systems are likely to become available within a few years if their manufacturers can be confident that V2V will be mandated and interoperable.

In order to provide estimates of the rule's costs and benefits, the agency has considered a scenario where two V2V-enabled safety applications, IMA and LTA, are voluntarily adopted on hypothetical schedules similar to those observed in the actual deployment of other advanced communications technologies. The agency believes that IMA and LTA will reduce the frequency of crashes that cannot be avoided by vehicle-resident systems, and will thus generate significant safety benefits that would not be realized in the absence of universal V2V communications capabilities. In addition, the marginal costs of including the IMA and LTA applications are extremely low once the V2V system is in place, which the agency believes will speed their adoption.

The agency has not quantified any benefits attributable to the wide range of *other* potential uses of V2V, although we believe that such uses are likely to be numerous. Recognizing its experience with other technologies, the agency believes that focusing on two of the many potential uses of V2V technology that are inexpensive to implement provides a reasonable approach to estimating potential benefits of the proposed rule, and is likely to understate the breadth of potential benefits of V2V.

We estimate that the total annual costs to comply with this proposed mandate in the 30th year after it takes effect would range from $2.2 billion to $5.0 billion, corresponding to a cost per new vehicle of roughly $135-$300. This estimate includes costs for equipment installed on vehicles as well as the annualized equivalent value of initial investments necessary to establish the overarching security manager and the communications system, among other things, but, due to uncertainty, does not include opportunity costs associated with spectrum, which will be included in the final cost benefit analysis. The primary source of the wide range between the lower and upper cost estimates is based our assumption that manufacturers could comply with the rule using either one or two DSRC radios.

As discussed above, our benefit calculation examines a case where manufacturers would voluntarily include the IMA and LTA applications on a schedule that reflects adoption rates the agency has observed for other advanced, vehicle-resident safety technologies. Together, these applications could potentially prevent 424,901– 594,569 crashes, and save 955-1,321 lives when fully deployed throughout the light-duty vehicle fleet. Converting these and the accompanying reductions in injuries and property damage to monetary values, we estimate that in 2051 the proposed rule could reduce the costs resulting from motor vehicle crashes by $53 to $71 billion (expressed in today's dollars).

The agency conducted two accompanying analyses to identify meaningful milestones in the future growth of benefits resulting from this proposed rule. These analyses highlight the effect that the passage of time has on the accumulated benefits from this proposed rule. Benefits in the first several calendar years after it takes effect will be quite low, because only a limited number of vehicles on the road will be equipped with V2V, but growth in these benefits will accelerate as time goes on.

First, NHTSA used a "breakeven" analysis to identify the calendar year during which the cumulative economic value of safety benefits from the use of V2V communications first exceeds the cumulative costs to vehicle manufacturers and buyers for providing V2V capability. The breakeven analysis indicated that this important threshold would be reached between 2029 and 2032, depending primarily on the effectiveness of the application technologies.

Next, NHTSA projected future growth in the proposed rule's benefits and costs over successive model years after it would take effect. This analysis identified the first model year for which the safety benefits from requiring vehicles to be equipped with V2V communications over their lifetime in the fleet would outweigh the higher initial costs for manufacturing them. It showed that this would occur in model year 2024 to 2026 if the proposed rule first took effect in model year 2021. This occurs sooner than the breakeven year, because focusing only on costs and benefits over the lifetimes of individual model years avoids including the burden of costs for installing V2V communications on vehicles produced during earlier model years.

Table I-1 Costs* and benefits in year 30 of deployment (2051)

Total annual costs	Per vehicle costs	Crashes prevented and lives saved	Monetary benefits
$2.2 billion-$5.0 billion	$135-$301	Crashes: 424,901-594,569 Lives: 955-1,321	$53 billion-$71 billion

*Note: Does not include spectrum opportunity costs, which will be included in the analysis of the final rule.

In order to account for the inherent uncertainty in the assumptions underlying this cost-benefit analysis, the agency also conducted extensive uncertainty analysis to illustrate the variation in the rule's benefits and costs associated with different assumptions about the future number of accidents that could be prevented, the assumed adoption rates and estimated effectiveness of the two safety applications, and our assumptions about the costs of providing V2V communications capability. Aside from opportunity costs, this analysis showed that the proposed rule would reach its breakeven year between 2030 and 2032 with 90 percent certainty, with even the most conservative scenario showing that the breakeven year would be five to six years later than the previously estimated years (2029-2032). Considering these same sources of uncertainty in the cost-effectiveness and net benefits analyses showed that the proposed rule would become cost-effective and would accrue positive net benefits between MY 2024 and MY 2027 with 90 percent certainty. This indicates that it is very likely to become cost-effectiveness at most one MY later than estimated in the primary analysis, and that even under the most

conservative scenario, this would occur two to three model years later than the initial estimate of 2024-2026.

Regulatory Alternatives

The agency considered two regulatory alternatives to today's proposal. First, the agency considered an "if-equipped" standard, which would entail simply setting a conditional standard stating that "*if* a new vehicle is equipped with devices capable of V2V communications, then it is required to meet the following requirements." However, the agency did not adopt this alternative as the proposal because, as explained above, the agency believes that anything short of a mandate for universal V2V capability on all new vehicles would not lead a sufficient fraction of the vehicle fleet to be equipped with V2V to enable full realization of the technology's potential safety benefits. However, we seek further comment on adopting an "if-equipped" standard as the primary approach to V2V communications technology. We request commenters provide any relevant research and data that supports their position and rationale for this approach to regulation.

Second, we considered a regulatory alternative of requiring that V2V-capable vehicles also be equipped with the two safety applications analyzed in this proposed rule – Intersection Movement Assist (IMA) and Left Turn Assist (LTA) – in addition to V2V capability. This alternative would speed the introduction and increase the certainty of safety benefits. However, because performance requirements and test procedures for these safety applications are still nascent, we are not proposing this alternative at this time. However, the agency requests comment on whether sufficient information exists that could assist it in developing FMVSS-quality test procedures and performance standards for these applications.

We seek comment on all aspects of this proposed rule, as well as the Preliminary Regulatory Impact Assessment (PRIA) and Draft Privacy Impact Assessment (PIA) that accompany it. Although a number of specific questions and requests for comment appear in various locations throughout the text, we encourage comments broadly, particularly those that are supported by relevant documentation, information, or analysis. Instructions for submitting comments are located below in the "Public Participation," Section IX.

II. Background

A. The Safety Need

Safety technology has developed rapidly since NHTSA began regulating the auto industry[4] – over the last several decades, vehicles have evolved to protect occupants much better

[4] NHTSA was established by the Highway Safety Act of 1970, as the successor to the National Highway Safety Bureau, to carry out safety programs under the National Traffic and Motor Vehicle Safety Act of 1966 and the

in the event of a crash due to advanced structural techniques propagated by more stringent crashworthiness standards, and some crash avoidance technologies (e.g., electronic stability control) are now required standard equipment. In fact, a recent study of data from our Fatality Analysis Reporting System (FARS) estimates those safety technologies have saved 613,501 lives since 1960.[5] As a result of existing NHTSA standards for crashworthiness and crash avoidance technologies, along with market-driven improvements in safety, motor vehicles are safer now than they have ever been, as evidenced by a significant reduction in highway fatalities and injuries - from 52,627 fatalities in 1970,[6] to 32,675 fatalities in 2015 – a 38 percent reduction.[7]

NHTSA believes the greatest gains in highway safety in coming years will result from broad-scale application of crash avoidance technologies along with continued improvements in vehicle crashworthiness that can reduce fatalities and injuries,.[8] To encourage adoption of such technologies, in February 2015 the agency announced that it would add two types of automatic emergency braking systems—crash imminent braking and dynamic brake support—to the list of recommended advanced safety features in our New Car Assessment Program, known to most Americans as NHTSA's Five Star Safety Ratings. In March, 2016 the agency announced an agreement with vehicle manufacturers to voluntarily make automatic emergency braking (AEB) a standard safety on future vehicles.[9] These technologies, along with technologies required as standard equipment like electronic stability control (ESC), help vehicles react to crash-imminent situations, but do not help drivers react ahead of time to avoid crashes.

This proposed rule would require vehicles to transmit messages about their speed, heading, brake status, and other vehicle information to surrounding vehicles, and to be able to receive the same information from them. V2V range and "field-of-view" capabilities exceed current and near-term radar- and camera-based systems -- in some cases, providing nearly twice the range. That longer range and 360 degree field of "view", currently supported by DSRC, provides a platform enabling vehicles to perceive some threats that sensors, cameras, or radar cannot.

Highway Safety Act of 1966. NHTSA also carries out consumer programs established by the Motor Vehicle Information and Cost Savings Act of 1972.

[5] Kahane, C. J. (2015, January). Lives saved by vehicle safety technologies and associated Federal Motor Vehicle Safety Standards, 1960 to 2012 – Passenger cars and LTVs – With reviews of 26 FMVSS and the effectiveness of their associated safety technologies in reducing fatalities, injuries, and crashes. (Report No. DOT HS 812 069). Washington, DC: National Highway Traffic Safety Administration.

[6] National Highway Traffic Safety Administration, Traffic Safety Facts 2012. Available at http://www-nrd.nhtsa.dot.gov/Pubs/812032.pdf (last accessed Dec. 7, 2016).

[7] National Highway Traffic Safety Administration, Fatality Analysis Report System (FARS) final 2014 data. For more information, see http://www-fars.nhtsa.dot.gov/Main/index.aspx.(last accessed Dec 7, 2016)

[8] For more information, see the agency policy statement on automated vehicles at http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf (last accessed Dec 7, 2016).

[9] See https://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_iihs_commitment_on_aeb_03172016 (last accessed Dec 7, 2016).

By providing drivers with timely warnings of impending crash situations, V2V-based safety applications could potentially reduce the number and severity of motor vehicle crashes, minimizing the losses and costs to society that would have resulted from these crashes. V2V message data can also be fused with existing radar- and camera-based systems to provide even greater crash-risk detection capability (and thus, driver confidence levels) than either approach alone.

1. Overall Crash Population that V2V Could Help Address

The first step in understanding how V2V could help drivers avoid crashes is determining how many crashes could potentially be addressed by V2V-based technologies. We estimate crash harm based on fatalities, injuries (described by MAIS),[10] and what we call "property-damage-only," meaning that no people were hurt, but vehicles sustained damage that will have to be fixed and paid for. Based on 2010-2013[11] General Estimates System (GES) and FARS, the agency estimated that there were 5.5 million police-reported crashes annually in the U.S. during those years. About 33,020 fatalities and 2.7 million MAIS[12] 1-5 injuries were associated with these crashes annually. In addition, about 6.3 million vehicles were damaged in property damage only crashes. These property damage only vehicles were noted as PDOVs.

Overall, these crashes directly cost $195 billion to society in terms of lost productivity, medical costs, legal and court costs, emergency service costs (EMS), insurance administration costs, congestion costs, property damage, and workplace losses. When you add the cost for less-tangible consequences like physical pain or lost quality-of-life, we estimate the total costs for those crashes to be $721 billion.[13]

Because V2V is a communications-based technology, it is relevant to crashes where more than one vehicle is involved: if a single vehicle crashes by itself, like by losing control and leaving the roadway and hitting a tree, V2V would not have been able to help the driver avoid

---

[10] MAIS (Maximum Abbreviated Injury Scale) approach, which represents the maximum injury severity of an occupant at an Abbreviated Injury Scale (AIS) level. AIS is an anatomically based, consensus-derived global severity scoring system that classifies each injury by body region according to its relative importance to fatality on a 6-point ordinal scale (1=minor, 2=moderate, 3=serious, 4=severe, 5=critical, and 6=maximum (untreatable). The AIS was developed by the Association for the Advancement of Automotive Medicine (AAAM). See https://www.aaam.org/abbreviated-injury-scale-ais/ (last accessed Dec 7, 2016) for more information.

[11] 2014 GES and FARS data was not available at the time of NPRM development.

[12] GES and FARS only record the police-reported crash severity scale known as KABCO: K=fatal injury, A= incapacitating injury, B=non-incapacitating injury, C=possible injury, O=no injury. These KABCO injuries then were converted to MAIS scale through a KABCO-MAIS translator. The KABCO-MAIS translator was established using 1982-1986 NASS (old NASS) and 2000-2007 Crashworthiness Data System (CDS). Old NASS and CDS recorded both KABCO and MAIS scales thus enable us to create the KABCO-translator.

[13] Costs are in 2014 dollars and, for clarity, include the economic costs. *See* Blincoe, L. J., Miller, T. R., Zaloshnja, E., & Lawrence, B. A. (2014, May), *The economic and societal impact of motor vehicle crashes, 2010*, (Report No. DOT HS 812 013), Washington, DC: National Highway Traffic Safety Administration (**Revised**, May, 2015), available at: http://www-nrd.nhtsa.dot.gov/pubs/812013.pdf (last accessed Dec 7, 2016).

losing control because there would have been no other vehicle to communicate with. Of the 5.5 million crashes described above, 3.8 million (69 percent of all crashes) were multi-vehicle crashes that V2V-based warning technologies could help address, which would translate to approximately 13,329 fatalities, 2.1 million MAIS1-5 injuries, and 5.2 million PDOVs.

However, some multi-vehicle crashes involve vehicles that would not be covered by this rule, and therefore could not yet be assumed to have V2V capability. As this proposal is currently limited only to light vehicles,[14] the crash population encompasses approximately 3.4 million (62 percent of all crashes) light-vehicle to light-vehicle (LV2LV) crashes, which would translate to 7,325 fatalities, 1.8 million MAIS 1-5 injuries, and 4.7 million PDOVs. The economic and comprehensive costs for these crashes amount to approximately $109 billion and $319 billion, respectively. Figure II-1 helps to illustrate the process for deriving the target population of 3.4 million LV2LV crashes that could be addressed by this proposal. All percentages are percentages of "all police-reported crashes," rather than percentages of the prior line.

[14] Light vehicles include passenger cars, vans, minivans, sport utility vehicles, crossover utility vehicles and light pickup trucks with a gross vehicle weight rating (GVWR) less than or equal to 10,000 pounds.

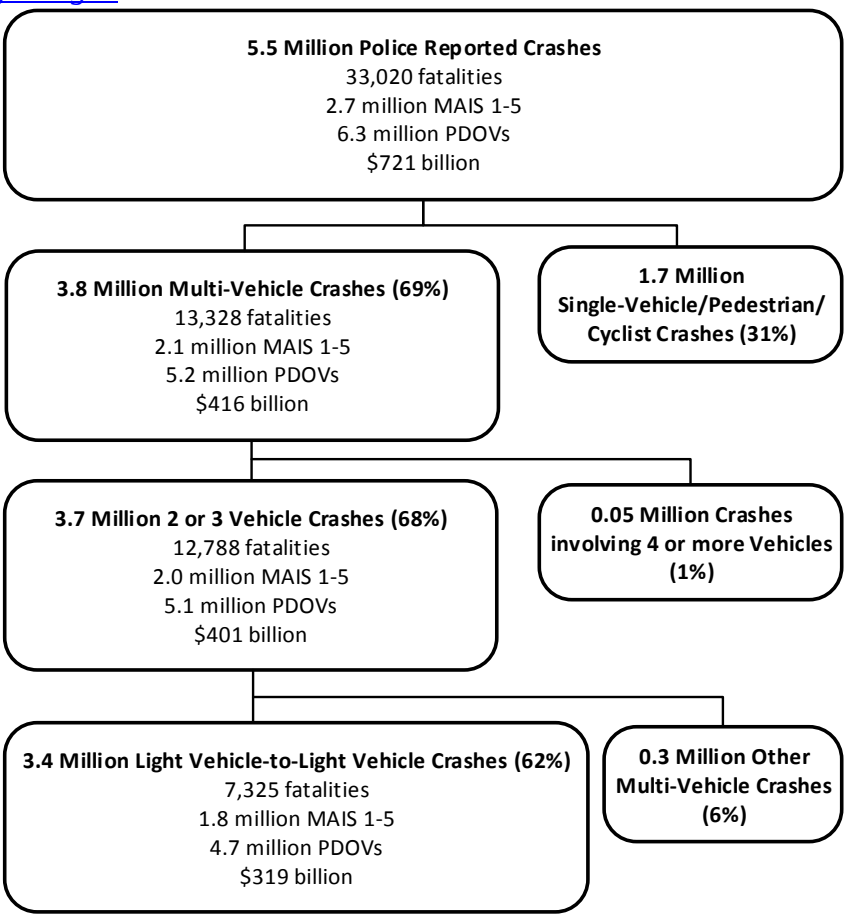

Figure II-1 Crash Population Breakdown for V2V Technology

2. Pre-Crash Scenarios Potentially Addressed by V2V Communications

In a separate analysis that has been updated using an average of 2010 through 2013 General Estimate System data (which does not include FARS data), the agency started with the initial 37 pre-crash scenarios that have been defined based on police-reported crashes from previous analyses for all crashes.[15] Of the 37 scenarios, 17 were deemed potentially addressable

[15] Najm, W.G., R. Ranganathan, G. Srinivasan, J. Smith, S. Toma, E. Swanson, and A. Burgett, "*Description of Light Vehicle Pre-Crash Scenarios for Safety Applications Based on Vehicle-to-Vehicle Communications*." DOT HS 811 731, U.S. Department of Transportation, National Highway Traffic Safety Administration, May 2013. http://www.nhtsa.gov/Research/Crash-Avoidance/Vehicle%E2%80%93to%E2%80%93Vehicle-Communications-for-Safety (last accessed Dec 8, 2016)

by V2V communications. Further statistical analysis focusing on the frequency and severity of those 17 pre-crash scenarios identified the top 10 (priority) pre-crash scenarios that V2V could potentially address. Table II-1 provides a graphical depiction of the flow of the pre-crash scenario breakdown used in the analysis.

Table II-1 37 Pre-Crash Scenario Typology

1	**Vehicle Failure**	**21**	**Vehicle(s) Not Making a Maneuver – Opposite Direction**
2	Control Loss with Prior Vehicle Action	22	Following Vehicle Making a Maneuver
3	Control Loss without Prior Vehicle Action	23	Lead Vehicle Accelerating
4	Running Red Light	24	Lead Vehicle Moving at Lower Constant Speed
5	Running Stop Sign	25	Lead Vehicle Decelerating
6	Road Edge Departure with Prior Vehicle Maneuver	26	Lead Vehicle Stopped
7	Road Edge Departure without Prior Vehicle Maneuver	27	Left Turn Across Path from Opposite Directions at Signalized Junctions
8	Road Edge Departure While Backing Up	28	Vehicle Turning Right at Signalized Junctions
9	Animal Crash with Prior Vehicle Maneuver	29	Left Turn Across Path from Opposite Directions at Non-Signalized Junctions
10	Animal Crash without Prior Vehicle Maneuver	30	Straight Crossing Paths at Non-Signalized Junctions
11	Pedestrian Crash with Prior Vehicle Maneuver	31	Vehicle(s) Turning at Non-Signalized Junctions
12	Pedestrian Crash without Prior Vehicle Maneuver	32	Evasive Action with Prior Vehicle Maneuver
13	Pedalcyclist Crash with Prior Vehicle Maneuver	33	Evasive Action without Prior Vehicle Maneuver
14	Pedalcyclist Crash without Prior Vehicle Maneuver	34	Non-Collision Incident
15	Backing Up into Another Vehicle	35	Object Crash with Prior Vehicle Maneuver
16	Vehicle(s) Turning – Same Direction	36	Object Crash without Prior Vehicle Maneuver
17	Vehicle(s) Parking – Same Direction	37	Other
18	Vehicle(s) Changing Lanes – Same Direction		

see also Najm, W.G., J. Smith, and M. Yanagisawa, "*Pre-Crash Scenario Typology for Crash Avoidance Research.*" DOT HS 810 767, U.S. Department of Transportation, National Highway Traffic Safety Administration, April 2007. Najm, W.G., B. Sen, J.D. Smith, and B.N. Campbell, "*Analysis of Light Vehicle Crashes and Pre-Crash Scenarios Based on the 2000 General Estimates System.*" DOT HS 809 573, U.S. Department of Transportation, National Highway Traffic Safety Administration, November 2002. Available at http://www.nhtsa.gov/Research/Crash-Avoidance/Vehicle%E2%80%93to%E2%80%93Vehicle-Communications-for-Safety (last accessed Dec 8, 2016).

19	Vehicle(s) Drifting – Same Direction		
20	Vehicle(s) Making a Maneuver – Opposite Direction		

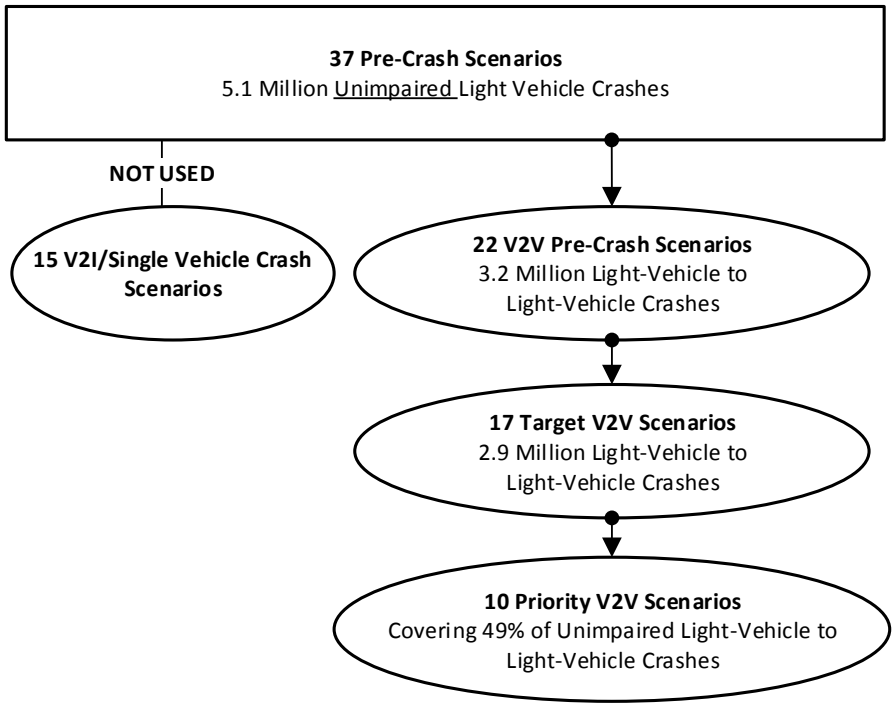

Figure II-2 V2V Pre-Crash Scenario Breakdown[16]

The 10 priority pre-crash scenarios listed in Table II-2 can be addressed by the corresponding V2V-based safety applications.

Table II-2 Pre-Crash Scenario/Safety Application Association

Pre-Crash Scenarios	Pre-crash Groups	Associated Safety Application
Lead Vehicle Stopped	Rear-end	Forward Collision Warning
Lead Vehicle Moving	Rear-end	Forward Collision Warning
Lead Vehicle Decelerating	Rear-end	Forward Collision Waring/Emergency Electronic Brake Light
Straight Crossing Path @ Non Signal	Junction Crossing	Intersection Movement Assist
Left-Turn Across Path/Opposite Direction	Left Turn @ crossing	Left Turn Assist

[16] Average of 2010-2013- GES data;* Includes only 2&3 vehicle crashes; **Includes running red-light and running stop sign

Opposite Direction/No Maneuver	Opposite Direction	Do Not Pass Warning
Opposite Direction/Maneuver	Opposite Direction	Do Not Pass Warning
Change Lanes/Same Direction	Lane Change	Blind Spot/Lane Change Warning
Turning/Same Direction	Lane Change	Blind Spot/Lane Change Warning
Drifting/Same Direction	Lane Change	Blind Spot/Lane Change Warning

The six applications listed in Table II-2 were developed and tested in the Connected Vehicle Safety Pilot Model Deployment.[17] These safety warning applications were (1) Forward Collision Warning (FCW), (2) Emergency Brake Light (EEBL), (3) Intersection Move Assist (IMA), (4) Left Turn Assist (LTA), (5) Do Not Pass Warning (DNPW), and (6) Blind Spot/Lane Change Warning (BS/LCW). A description of each safety application and relationship to the pre-crash scenarios is provided below.

(1) Forward Collision Warning (FCW): warns drivers of stopped, slowing, or slower vehicles ahead. FCW addresses rear-end crashes that are separated into three key scenarios based on the movement of lead vehicles: lead-vehicle stopped (LVS), lead-vehicle moving at slower constant speed (LVM), and lead-vehicle decelerating (LVD).

(2) Emergency Electronic Brake Light (EEBL): warns drivers of heavy braking ahead in the traffic queue. EEBL would enable vehicles to broadcast its emergency brake and allow the surrounding vehicles' applications to determine the relevance of the emergency brake event and alert the drivers. EEBL is expected to be particularly useful when the driver's visibility is limited or obstructed.

(3) Intersection Movement Assist (IMA): warns drivers of vehicles approaching from a lateral direction at an intersection. IMA is designed to avoid intersection crossing crashes, the most severe crashes based on the fatality counts. Intersection crashes include intersection, intersection-related, driveway/alley, and driveway access related crashes. IMA crashes are categorized into two major scenarios: turn-into path into same direction or opposite direction and straight crossing paths. IMA could potentially address five of the pre-crash scenarios identified in Table II-2.

[17] The Connected Vehicle Safety Pilot ("Safety Pilot") Program was a scientific research initiative that features a real-world implementation of connected vehicle safety technologies, applications, and systems using everyday drivers. The effort will test performance, evaluate human factors and usability, observe policies and processes, and collect empirical data to present a more accurate, detailed understanding of the potential safety benefits of these technologies. The Safety Pilot program includes two critical test efforts—the Safety Pilot Driver Clinics and the Safety Pilot Model Deployment. See http://www.its.dot.gov/research_archives/safety/cv_safetypilot.htm for more information. (last accessed Dec 7, 2016).

(4) Left Turn Assist (LTA): warns drivers to the presence of oncoming, opposite-direction traffic when attempting a left turn. LTA addresses crashes where one involved vehicle was making a left turn at the intersection and the other vehicle was traveling straight from the opposite direction.

(5) Do Not Pass Warning (DNPW): warns a driver of an oncoming, opposite-direction vehicle when attempting to pass a slower vehicle on an undivided two-lane roadway. DNPW would assist drives to avoid opposite-direction crashes that result from passing maneuvers. These crashes include head-on, forward impact, and angle sideswipe crashes.

(6) Blind Spot/Lane Change Warning (BS/LCW): alerts drivers to the presence of vehicles approaching or in their blind spot in the adjacent lane. BS/LCW addresses crashes where a vehicle made a lane changing/merging maneuver prior to the crashes.

The final table, Table II-3, merges the estimated target crash population for LV2LV crashes detailed in Table II-2 with the separate analysis that provided the breakdown of V2V pre-crash scenarios and relationships to prototype V2V safety applications. The 3.4 million LV2LV are distributed among the pre-crash scenarios that are associated with V2V safety applications and the economic and comprehensive costs. More specifically, Table II-3 provides a breakdown of crashes associated with FCW, IMA, LTA, and LCW scenarios that are used later when discussing potential benefits in Section VII. Crash scenarios associated with DNPW and EEBL are grouped with all remaining crashes under the "other" category due to the fact they are not used when discussing benefits. The agency grouped these two potential applications into the "other" category because of EEBL's advisory nature that cannot be directly attributed to avoiding a specific crash and the agency's current understanding of DNPW indicates it only addresses a limited amount of crashes per a specific situation and where there are three equipped vehicles present, limiting the amount of information available to develop comprehensive effectiveness estimates.

Overall the agency estimates that, together, these four potential safety applications that could be enabled by this proposal could potentially address nearly 89 percent of LV2LV crashes and 85 percent of their associated economic costs.

Table II-3 Crash Scenarios for LV2LV Safety Population

V2V Safety Applications -Crashes	Crash Scenarios	Crashes	MAIS 1-5 Injuries	Fatalities	PDOVs	Economic Costs (Billion)	Comprehensive Costs (Billion)
FCW Rear-End Crashes	Lead Vehicle Stopped	998,664	497,907	242	68,508	$27.4	$65.7
	Lead Vehicle Moving	146,247	80,508	242	12,605	$4.6	$12.9
	Lead Vehicle Decelerating	343,183	173,538	78	25,599	$9.5	$23.1
	Total	1,488,094	751,953	562	106,712	$41.5	$101.6
IMA Intersection	Turn-Into Path, Into	425,145	218,852	472	48,423	$12.6	$34.8

Crossing Crashes	Same Direction or Opposite Direction						
	Straight Cross Path	346,187	251,488	1,399	66,580	$14.4	$49.4
	Total	771,332	470,340	1,871	115,003	$26.9	$84.3
LTA Left-Turning Crashes	Turn Across Path, Initial Opposite Direction	298,542	224,336	613	64,233	$11.7	$37.9
BS/LCW Lane Change/Merge Crashes	Vehicle Changing Lane, Same Direction	475,097	175,044	397	20,816	$11.4	$26.6
Others	Others	378,659	192,152	3,882	4,416,890	$16.7	$66.4
Total	Total	3,411,724	1,813,825	7,325	4,723,654	$108.2	$316.8

Note: due to rounding, the total might not be equal to the sum of each componment

B. Ways to address the Safety Need

The most effective way to reduce or eliminate the property damage, injuries, and fatalities that occur annually from motor vehicle crashes is to lessen the severity of those crashes, or prevent those crashes from ever occurring. In recent years, vehicle manufacturers have begun to offer, or have announced plans to offer, various types of crash avoidance technologies that are designed to do just that. These technologies are designed to address a variety of crashes, including rear end, lane change, and intersection.

1. Radar and camera based systems

Many of the advanced crash avoidance technologies currently available in the marketplace employ on-board sensor technologies such as cameras, RADAR, or LIDAR, to monitor the vehicles' surroundings.[18] These technologies are what we call "vehicle-resident" systems because they are systems installed on one vehicle and, unlike V2V, do not communicate with other vehicles. Cameras, RADAR, and LIDAR that are installed on the vehicle can gather information directly by sensing their surroundings, and vehicle-resident crash avoidance technologies can use that information to warn the driver of impending danger so the driver can take appropriate action to avoid or mitigate a crash. Crash scenarios that can currently be addressed by existing crash avoidance technologies include, but are not limited to, Forward Collision Warning (FCW),[19] Blind Spot Warning (BSW), and Lane Change Warning (LCW).[20]

[18] A LIDAR device detects distant objects and determines their position, velocity, or other characteristics by analysis of pulsed laser light reflected from their surfaces. Lidar operates on the same principles as radar and sonar.
[19] FCW warns the driver of an impending rear-end collision with a vehicle ahead in traffic in the same lane and direction of travel.

Additionally, some crash-predicting safety applications leveraging these existing sensing technologies are beginning to emerge and NHTSA is aggressively pursuing those technologies that demonstrate safety benefits.

Vehicle-resident systems can be highly effective in mitigating certain crash types, although their performance varies by sensor type, and is limited in certain situations. Perception range varies from 10 meters to 200 meters for LIDAR and 77 GHz radar, respectively, while field-of-view ranges from 18 degrees to 56 degrees for 77 GHz radar and 24 GHz radar,[21] respectively. On-board sensors can also exhibit reduced reliability in certain weather conditions (e.g., snow, fog, and heavy rain), and camera systems, in particular, can exhibit reduced performance when encountering lighting transitions and shadows. Most if not all current sensing technologies are susceptible to performance reductions through foreign objects such as dirt or snow. For camera-based systems, some manufacturers have implemented devices that attempt to keep the camera clear for maximal operation. Both sensor types can be vulnerable to misalignment or damage over time. On-board sensors do, however, perform reliably in "urban canyons" and other situations in which a clear view of the sky is not needed.

2. Communication-based systems

Devices enabling vehicles to communicate with one another or with road-side equipment and/or infrastructure have been prototyped and tested in field operational tests like the Safety Pilot Model Deployment. These devices, when eventually developed for mass production, could be fully integrated into a vehicle when manufactured, or could be standalone aftermarket units not restricted to a single vehicle. These devices offer varying degrees of functionality, but all are designed to communicate safety information to help mitigate crashes.

Safety information that can help mitigate crashes includes data elements like vehicle position, heading, speed, and so forth – data elements that could help a computer-based safety application on a vehicle calculate whether it and another vehicle were in danger of crashing without driver intervention. These pieces of information are collected into what is known as a "Basic Safety Message," or "BSM." In a fully-integrated vehicle communication system, the system is built into the vehicle during production, and consists of a general purpose processor and associated memory, a radio transmitter and transceiver, antennas, interfaces to the vehicle's sensors, and a GPS receiver. It generates the BSM using in-vehicle information obtained from the vehicle's on board sensors. An integrated system can both transmit and receive BSMs, and can process the content of received messages to provide advisories and/or warnings to the driver of the vehicle in which it is installed. Since the vehicle data bus provides a rich data set,

---

[20] BSW and LCW technologies warn the driver during a lane change attempt if the zone into which the driver intends to switch to is, or will soon be, occupied by another vehicle traveling in the same direction. The technology also provides the driver with advisory information that a vehicle in an adjacent lane is positioned in his/her vehicle's "blind spot" zone even when a lane change is not being attempted.

[21] "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application", August 2014, pp. 105

integrated systems have the potential to obtain information that could indicate driver intent, which can help inform safety applications such as Left Turn Assist (LTA),[22] Do Not Pass Warning (DNPW),[23] and BSW/LCW safety applications, all of which can benefit from, or require, information on turn signal status or steering wheel angle.

Aftermarket devices, which are added to a vehicle after its assembly, can vary significantly from both fully-integrated vehicle communication systems, and from one another. The simplest designs may only transmit (and not also receive) a BSM, may only connect to a power source and otherwise operate independently from the systems in the vehicle, and may not run safety applications or provide advisories/warnings to a driver.[24] More sophisticated options may have the ability to both receive and transmit a BSM to nearby vehicles, may connect to the vehicle data bus (similar to fully integrated devices), and may contain safety applications that can provide advisories/warnings to the driver. Depending on the type of aftermarket device, different data elements may or may not be available. This may limit what safety applications can be supported. For example, a device that does not connect to a vehicle data bus may support FCW, but without having access to turn signal information, may not be able to support LTA.

Regardless of whether they are integrated or aftermarket, all communication-based systems are designed to, at a minimum; transmit BSM information such as vehicle position and heading to nearby vehicles. That information may be transmitted using various communication methods – like cellular, Wi-Fi, satellite radio, or dedicated short-range communication (DSRC) – each of which has its own advantages and disadvantages. At this time, DSRC is the only mature communication option that meets the latency requirements to support vehicle communication based crash avoidance, although future V2V standards may also meet the latency requirements.

Cellular networks currently offer fairly widespread coverage throughout the nation and are continuing to expand; however, there are still areas (dead spots) where cellular service is not available. And, although the advancement of long-term evolution (LTE) technology is helping to deliver large amounts of data to cellular users more quickly, transmission rates slow down if a user is moving or is in a high-capacity area with many other LTE users. While many new vehicles today already are equipped with cellular capability, this communication method could

[22] LTA warns the driver of a vehicle, when entering an intersection, not to turn left in front of another vehicle traveling in the opposite direction. LTA applications currently trigger only when the driver activates the turn signal.
[23] DNPW warns the driver of a vehicle during a passing maneuver attempt when a slower-moving vehicle, ahead and in the same lane, cannot be safely passed using a passing zone that is occupied by vehicles travelling in the opposite direction. The application may also provide the driver an advisory warning that the passing zone is occupied when a passing maneuver is not being attempted.
[24] Such a device could still be useful to users, because it would alert other drivers to the presence of their vehicle (i.e., it would help them be "seen better").

possibly introduce security risks, such as cyberattacks or privacy concerns[25], and high costs stemming from cellular data costs and fitting new vehicles with cellular capability.

Wi-Fi technology offers generally higher data rates than the other options, but because of its intrinsic design for stationary terminals, and the need for a vehicle to provide its MAC (media access control) address, and obtain the MAC address of all other vehicles in a Wi-Fi hotspot before it can send communications, transmission rates are significantly reduced if a user is moving. Cost concerns and potential security risks for Wi-Fi are similar to those for cellular communication.[26]

Satellite radio, or Satellite Digital Audio Radio Service (SDARS), uses satellites to provide digital data broadcast service nearly nationwide (across approximately 98% of the U.S. land mass – fundamentally not covering Alaska and Hawaii and covering the southern parts of Canada and northern parts of Mexico. Data download time for satellite communication, however, is slow compared to the other communication options which limits its capability to "back office" type communications versus actual vehicle to vehicle safety communications, and the costs and security risks associated with cellular and Wi-Fi communication also apply to satellite.[27]

DSRC is a two-way short-range wireless technology that provides local, nearly instantaneous network connectivity and message transmission. It has a designated licensed bandwidth to permit secure, reliable communication, and provides very high data transmission rates in high-speed vehicle mobility conditions which are critical characteristics for detecting potential and imminent crash scenarios.[28] Cost concerns and potential security risks are also inherent to DSRC technology.

In this NPRM, the proposal would require V2V communication to use DSRC devices to transmit messages about a vehicle's speed, heading, braking status, etc. to surrounding vehicles, as well as to receive comparable information from surrounding vehicles. As DSRC is based on radio signals, which are omnidirectional (i.e., offer 360 degrees of coverage), V2V offers the ability to "see" around corners and "see" through other vehicles. Consequently, V2V is not restricted by the same line-of-sight limitations as crash avoidance technologies that rely on vehicle-resident sensors. V2V also offers an operational range of 300 meters, or farther, between vehicles, which is nearly double the detection distance afforded by some current and near-term vehicle-resident systems. These unique characteristics allow V2V-equipped vehicles to perceive and warn drivers of some threats sooner than current vehicle-resident sensors can. The proposal

---

[26] BAH CDDS Final Report. See Docket No. NHTSA-2014-0022

[27] "Organizational and Operational Models for the Security Credentials Management System (SCMS); Industry Governance Models, Privacy Analysis, and Cost Updates," dated October 23, 2013, prepared by Booz Allen Hamilton under contract to DOT, non-deliberative portions of which may be viewed in docket: NHTSA-2014-0022

[28] Report and Order FCC-03-0324.

would also allow vehicles to comply using non-DSRC technologies that meet certain performance and interoperability standards.

V2V is subject to the current limitations of GPS technology. This includes accuracy levels that are perceived to be only sufficient for warning applications vs. control applications such as automatic braking. The GPS dependency also poses challenges where sky visibility is limited (e.g., under bridges, in tunnels, in areas of heavy foliage, and in highly dense urban areas). Some of these issues, however, can be resolved through techniques such as "dead-reckoning."[29] V2V also requires that a significant number of vehicles be equipped with V2V technology to realize the effectiveness of the system, and similarly, whereas vehicle-resident sensors can "see" stop signs and traffic lights (and use that information to slow or stop the vehicle), the infrastructure also would need to be able to send messages to V2V-equipped vehicles if V2V was to have similar capability.

3. Fusion of vehicle-resident and communication-based systems

Both vehicle-resident and communication-based safety systems have certain strengths and limitations, and as such, NHTSA and many commenters to the ANPRM, like the Automotive Safety Council, Hyundai Motor Group, IIHS, Motor & Equipment Manufacturers Association, and Volvo Cars, believe that combining ("fusing") communication-based systems with vehicle-resident crash avoidance systems to exploit the functionality of both system types presents a significant opportunity. Given the proposed V2V system, we are confident that the technology could be easily combined with other vehicle-resident crash avoidance systems to enhance the functionality of both types of systems. Together, the two systems can provide even greater benefits than either system alone.

For vehicles equipped with current on-board sensors, V2V can offer a fundamentally different, but complementary, source of information that can significantly enhance the reliability and accuracy of the information available. Instead of relying on each vehicle to sense its surroundings on its own, V2V enables surrounding vehicles to help each other by reporting safety information to each other. V2V communication can also detect threat vehicles that are not in the sensors' field of view, and can validate a return from a vehicle-based sensor. This added capability can potentially lead to improved warning timing and a reduction in the number of false warnings, thereby adding confidence to the overall safety system, and increasing consumer satisfaction and acceptance. Similarly, vehicle-resident systems can augment V2V systems by providing the information necessary to address other crash scenarios not covered by V2V communications, such as lane and road departure. These systems can work collectively to advance motor vehicle safety, as was further evidenced in the comments submitted by the Automotive Safety Council and IIHS.

---

[29] The process of calculating one's position, especially at sea, by estimating the direction and distance traveled rather than by using landmarks, astronomical observations, or electronic navigation methods.

The Automotive Safety Council commented that, in addition to the safety advantages from increased sensing range and the environment use cases, V2V also offers advantages with respect to operation status (e.g., brake pedal status, transmission state, stability control status, vehicle at rest versus moving, etc.) IIHS suggested that whereas current FCW systems are designed to operate off the deceleration of the vehicle directly ahead, V2V could permit communication with all vehicles ahead in the lane of travel, thus warning all vehicles, not just those equipped with FCW, of the eminent need to slow down or stop.

IIHS contended, however, that onboard sensing systems may evolve during the time it will take V2V to penetrate the fleet, potentially to the point where they have similar ranges to V2V transmissions, such that it may be difficult to quantify how much V2V will reduce collision frequency and severity beyond the capabilities of sensor-based systems. Along similar lines, the Automotive Safety Council countered some of its earlier comments by stating that "it is possible that DSRC technology may be obsolete before the safety goals of V2V systems are realized" such that it may be a better approach to pursue the installation of well-tested, standalone technologies that are currently available.

The agency appreciates the commenters' views on the co-existence of the technologies with varying capability and expressing support for the agency's approach in this proposal. We do disagree, however, with the comments indicating that V2V should not be pursued because onboard sensing systems exist in the marketplace. The agency views these technologies as complementary and not competing. Providing a data rich information environment should, most likely, enable more capability to enhance vehicle safety.

The agency requests comments its views concerning the potential of fusing connected and vehicle-resident technologies. In particular, the agency requests comment on what specific applications could use both technologies to enhance safety. The agency also seeks comment on whether an if-equipped option for V2V would be preferable, given the development of vehicle-resident technologies.

4. Automated systems

Automated systems perform at least some aspects of a safety-critical control function (e.g., steering, throttle, or braking) automatically – without direct input by a human driver. Examples of automated systems include Crash Imminent Braking (CIB) and Dynamic Brake Support (DBS). These systems are designed, respectively, to automatically apply the vehicle's brakes if the human driver does not respond at all to warnings that are provided, or to supplement the human driver's braking effort if the driver's response is determined (by the system) to be insufficient, in order to mitigate the severity of a rear-end crash, or to avoid it altogether.

Although many automated systems currently rely on data obtained from on-board sensors and cameras to judge safety-critical situations and respond with an appropriate level of control, data acquired from GPS and telecommunications like V2V could significantly augment such systems, since, as mentioned previously, vehicle communication-based systems, like V2V, are capable of providing warnings in several scenarios where vehicle-based sensors and cameras

cannot (e.g., vehicles approaching each other at intersections).[30] Honda Motor Col, Ltd commented that "…the ability of vehicles to directly communicate with one another will greatly assist in the ability to safety and effectively deploy" higher-level driver assistance and automated technologies in Honda vehicles. Along similar lines, Meritor WABCO and the Automotive Safety Council both mentioned that V2V safety applications with warning capability will enhance current active safety systems, but should not be considered a replacement for them.

Systems Research Associates, Inc. stated that "it is irrefutable that V2V, V2I, and V2P communications will be absolutely critical to the successful development of self-driving vehicles that can avoid collisions, navigate responsibly, and achieve a transport objective efficiently and in a timely manner." Similarly, IEEE USA commented that V2V can provide the trusted map data and situation awareness messages necessary for innovative safety functions, and support the flow of traffic with self-driving cars.

Other commenters, including Robert Bosch LLC and Motor & Equipment Manufacturers Association expressed that V2V data should serve as a supplemental input in developing automated vehicles, but cautioned the agency that vehicles should not have an external, V2V exclusive infrastructure and communication medium dependency. This approach may unnecessarily limit the adoption or implementation of automated systems. Furthermore, the Automotive Safety Council commented that "V2V should be considered as one of the supporting sensor sets for automated vehicle applications, where it can augment the information available to the vehicle about the surrounding environment" by increasing the range and/or reliability of data from sensors, but it is "…not sufficient alone as a sensor to support automated vehicles nor a technology that will inhibit the development of automated applications. In order to ensure robust decisions for autonomous functions, sensing redundancy at the vehicle level may still be required to meet functional safety requirements, and/or for functions where the V2V technology is not capable of providing the necessary data or inputs to the vehicle."

Competitive Enterprise Institute expressed concerns that a V2V mandate may harm vehicle automation efforts. The company cited Google and Bosch's ability to develop vehicle automation systems that use onboard sensors and computers to map vehicle surroundings in real-time and make direction decisions without widespread vehicle-to-vehicle connectivity as reason to suggest that V2V is unnecessary for full-scale automation. The company also commented that if automated systems were required to interact with V2V under a new Standard, this would generate "large and as yet uncontemplated cybersecurity, crash, and products liability risks." Similarly, the Automotive Safety Council commented that the security system described in the V2V Readiness report "does not provide sufficient protection against all abuse of the V2V system" in the event that active safety applications which leverage the V2V infrastructure, are considered in the future. The group suggested that because "the data fed into the DSRC device from the vehicle sensors is not cryptographically protected," an attacker "could simply feed a

DSRC device bad data, which is subsequently cryptographically signed using the proposed PKI system and transmitted to nearby vehicles." The Automotive Safety Council suggested that this could allow an attacker to "cause a vehicle to rapidly swerve off the road to avoid a collision with a car that does not exist in reality but was interpreted to exist" because the vehicle received false, but cryptographically signed and thus trusted, data from a nearby malicious vehicle.

QUALCOMM Incorporated maintained an opposing position to Competitive Enterprise Institute and the Automotive Safety Council. The company commented that, "while it is possible to implement a certain level of vehicle automation…without V2V, V2V can enhance the overall reliability and coverage of autonomous vehicle technology." Consequently, the company contended that there is no conflict between the deployment of DSRC and automated vehicles, and further suggested that the two technological advances should be pursued simultaneously so that the additional safety benefits offered by DSRC can penetrate the fleet and be realized in both autonomous and non-autonomous vehicles. Overall, this approach is aligned with the agency's view that V2V is complementary, and not competing, with automated vehicle deployment.

The agency requests comment on the interplay between V2V and autonomous technologies.

C. V2V Research Up Until this Point

1. General Discussion

The U.S. Department of Transportation, along with other research partners in State DOTs, academia, and industry, has been evaluating how to incorporate communication technology into transportation infrastructure since the mid-1980s, in order to improve transportation (particularly on-road vehicle) safety, mobility, and emissions. That broad research topic is generally referred to as "intelligent transportation systems" or "ITS." V2V research developed out of ITS research in the mid-2000s, when NHTSA and CAMP began to look at the potential for DSRC as a vehicle communication technology, for the purpose of warning drivers of imminent crash risks in time to avoid them. NHTSA's decision to begin the rulemaking process to require V2V communications capability on new light vehicles thus represented the culmination of several decades of research by government and industry to develop this communications technology for vehicles from the ground up. In the interest of brevity, NHTSA refers readers to the V2V Readiness Report for a summary of the history of ITS research and NHTSA's work with CAMP and other partners prior to 2014.[31]

One element of the V2V research that took place prior to 2014 is the Safety Pilot Model Deployment. The Model Deployment was the culmination of the V2V research that had taken place in prior years. Using the Model Deployment, DOT deployed prototype V2V DSRC

[31] *See* Section II.B of the Readiness Report, available at http://www.safercar.gov/v2v/ (last accessed Dec 7, 2016).

devices on real roads with real drivers that interacted for over a year and provided the data that allowed DOT to evaluate the functional feasibility of V2V under real world conditions.

The Model Deployment was conducted in Ann Arbor, Michigan, and ran from August 2012 to February 2014. Sponsored by DOT and conducted by the University of Michigan Transportation Research Institute, the experiment was designed to support evaluation of the functionality of V2V technology. Approximately 2,800 vehicles – a mix of cars, trucks, and transit vehicles operating on public streets within a highly concentrated area – were equipped with integrated in-vehicle safety systems, aftermarket safety devices, or vehicle awareness devices, all using DSRC to emit wireless signals of vehicle position and heading information. Vehicles equipped with integrated in-vehicle or aftermarket safety devices have the additional design functionality of being able to warn drivers of an impending crash situation involving another equipped vehicle.

Data collected during the Model Deployment was used to support an evaluation of functionality of the V2V safety applications used in the Model Deployment - in effect, *whether* the prototypes and the system worked, but not necessarily *how well* they worked. Overall, the Model Deployment demonstrated that V2V technology can be deployed in a real-world driving environment. The experimental design was successful in creating naturalistic interactions between DSRC-equipped vehicles that resulted in safety applications issuing warnings in the safety-critical driving scenarios that they were designed to address. The data generated by warning events indicated that all the devices were interoperable, meaning that they were successfully communicating with each other.

The Model Deployment was the first and largest test of V2V technology in a real-world environment. The Model Deployment was a key step in understanding whether the technology worked, the potential of this technology to help avoid crashes, and increase the vehicle safety.

Besides explaining the history of the research that led to NHTSA's decision to initiate rulemaking to require V2V communications capability, the Readiness Report also described NHTSA's understanding of the current state of the research in mid-2014, and identified a number of areas where additional research could be necessary either to develop mandatory requirements for new vehicles equipped with DSRC, or to further develop information needed to inform potential future requirements for DSRC-based safety applications. The following sections summarize the agency's research-based findings in the Readiness Report; list the areas where the agency identified additional research as necessary; and explain the status of research conducted since the Readiness Report in response to those identified research needs.

2. Main topic areas in Readiness Report

Based on the agency's research and thinking at the time of issuance, the V2V Readiness Report comprehensively covered several key topic areas:

- What the safety need is that V2V can address, and how V2V addresses it;

- The legal and policy issues associated with requiring V2V for light vehicles, the secure operation of the technology, and the implications of these issues for privacy;
- A description of the technology required for V2V capability, the different types of devices, and the security needed for trusted communications; and
- Based on preliminary data, how much the technology may be expected to cost (both for purchasers of new vehicles, and for the entities who develop and build out the security and communications networks, in terms of initial capital investments), and the potential effectiveness (and thus, benefits) of certain V2V-based safety applications at helping drivers avoid crashes.

a) Key Findings of Readiness Report

The Readiness Report listed the key findings of the research up to that point, as follows:

- V2V (specifically, DSRC) devices installed in light vehicles as part of the Safety Pilot Model Deployment were able to transmit and receive messages from one another, with a security management system providing secure communications among the vehicles during the Model Deployment. This was accomplished with relatively few problems given the magnitude of this first-of-its-kind demonstration project.

- The V2V devices tested in the Model Deployment were originally developed based on existing communication protocols found in voluntary consensus standards from SAE and IEEE. NHTSA and its research partners participating in the Model Deployment (e.g., its vehicle manufacturers and device suppliers) found that the standards did not contain enough detail as-is and left too much room for interpretation to achieve interoperability. They therefore developed additional protocols that enabled interoperability between devices participating in the study. The valuable interoperability information learned during the execution of Model Deployment is planned to be included in future versions of voluntary consensus standards that would support a larger, widespread technology roll-out.

- As tested in the Model Deployment, safety applications enabled by V2V, examples of which include IMA, FCW, and LTA, have proven effective in mitigating or preventing potential crashes, but the agency recognized that additional refinement to the prototype safety applications used in the Model Deployment would be needed before minimum performance standards could be finalized and issued.[32] Based on the agency's understanding of how these prototype safety applications operate, preliminary effectiveness estimates in the Readiness Report indicated substantial ability to mitigate

[32] See, e.g., Nodine et al., "Independent Evaluation of Light-Vehicle Safety Applications Based on Vehicle-to-Vehicle Communications Used in the 2012-2013 Safety Pilot Model Deployment," USDOT Volpe Center, DOT HS 812 222, December 2015. Available at Docket NHTSA-2016-0126

crashes, injuries or fatalities in these crash scenarios. Also, the agency concluded that some safety applications could be better tailored to the safety problem that they are intended to solve (e.g., LTA applications currently trigger only when the driver activates the turn signal, but many drivers do not always activate their turn signals in dedicated turn lanes).

- The agency has the legal authority to mandate V2V (specifically, DSRC) devices in new light vehicles, and could also require them to be installed in commercial vehicles already in use on the road if we also required them for new medium and heavy duty vehicles. The agency also has the authority to mandate safety applications that are V2V-based, and to work with an outside entity to develop the security and communications infrastructures needed to support deployment of V2V technologies in motor vehicles.

- Based on preliminary information used for the report, NHTSA estimated that the V2V equipment and supporting communications functions (including a security management system) would cost approximately $341 to $350 per vehicle in 2020, and it is possible that the cost could decrease to approximately $209 to $227 by 2058, as manufacturers gain experience producing this equipment (the "learning curve" effect). These costs would also include an additional $9 to $18 per year in fuel costs due to added vehicle weight from the V2V system. Estimated costs for the security management system ranged from $1 to $6 per vehicle, and were estimated to increase over time due to the need to support an increasing number of vehicles with V2V technology. The estimated communications costs ranged from $3 to $13 per vehicle. Cost estimates were not expected to change significantly by the inclusion of V2V-based safety applications, since the applications themselves are software and their costs are negligible.

- Based on preliminary estimates used for the report, the total projected preliminary annual costs of the V2V system fluctuated year after year but generally indicated a declining trend. The estimated total annual costs ranged from $0.3 to $2.1 billion in 2020, with the specific costs depending upon the technology implementation scenarios and discount rates. The costs peaked to $1.1 to $6.4 billion between 2022 and 2024, and then gradually decreased to $1.1 to $4.6 billion.

- The analysis conducted for the V2V Readiness Report estimated that just two of many possible V2V safety applications, IMA and LTA, would on an annual basis potentially prevent 25,000 to 592,000 crashes, save 49 to 1,083 lives, avoid 11,000 to 270,000 MAIS 1-5 injuries, and reduce 31,000 to 728,000 property-damage-only crashes by the time V2V technology had spread through the entire fleet, if manufacturers implemented

them.[33] These two applications were used for analysis because they were illustrations of benefits that V2V can provide above and beyond the safety benefits of radar and camera based systems. Of course, the number of lives potentially saved would increase with the implementation of additional V2V- and V2I-based safety applications that could be enabled if vehicles were equipped with V2V communications capability.

b) Additional V2V-Related Issues that Required the Agency's Consideration

The Readiness Report also recognized that additional items need to be in place for a potential V2V system to be successful. These items were listed as follows:

- Wireless spectrum: V2V communications transmit and receive messages at the 5.85-5.925 GHz frequency. The FCC, as part of an ongoing rulemaking proceeding, is considering whether to allow "Unlicensed National Information Infrastructure" devices (that provide short-range, high-speed, unlicensed wireless connections for, among other applications, Wi-Fi-enabled radio local area networks, cordless telephones, and fixed outdoor broadband transceivers used by wireless Internet service providers) to operate in the same area of the wireless spectrum as V2V.[34] Given that Wi-Fi use is growing exponentially, "opening" the 5.85-5.925 GHz part of the spectrum could result in many more devices transmitting and receiving information on the same or similar frequencies, which could potentially interfere with V2V communications in ways harmful to its safety intent. More research is needed on whether these Wi-Fi enabled devices can share the spectrum successfully with V2V, and if so, how. In December 2015 and January 2016, the DOT, FCC, and the Department of Commerce sent joint letters to members of the U.S. Senate Committee on Commerce, Science, and Transportation, delineating a collaborative multi-phased approach that will be used to provide real-world data on the performance of unlicensed devices that are designed to avoid interfering with DSRC operations in the 5.85-5.925 GHz band.

- V2V device certification issues: V2V devices are different from other technologies regulated by NHTSA under the Federal Motor Vehicle Safety Standards, insofar as part of ensuring their successful operation (and thus, the safety benefits associated with them) requires ensuring that they are able to communicate with all other V2V devices participating in the system. This means that auto manufacturers (and V2V device

[33] The benefits estimated for this proposal vary from those developed for the V2V Readiness Report. Please refer to Section VII for details on the costs and benefits of this proposal.

[34] *See* Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, *Notice of Proposed Rulemaking*, ET Docket No. 13-49 (Feb. 2013). Under the FCC Part 15 rules U-NII devices cannot cause interference to DSRC operations and must accept interference from DSRC operations.

manufacturers) attempting to comply with a potential V2V mandate could have a significant testing obligation to guarantee interoperability among their own devices and devices produced by other manufacturers. At the time of the Readiness Report, it was an open question whether individual companies could meet such an obligation themselves, or whether independent testing facilities might need to be developed to perform this function. Based on the security design evaluated for the report, it was thought likely that an entity or entities providing the security management system would require that device manufacturers comply with interoperability certification requirements to ensure the reliability of message content. The agency currently believes the creation of a standardized test device should mitigate manufacturer to manufacturer communication variances to help ensure interoperability.

- Test procedures, performance requirements, and driver-vehicle interface (DVI) issues: Test procedures, performance requirements, and driver-vehicle interfaces appeared to work well enough for purposes of the Model Deployment (as compared to a true production, real-world environment), but NHTSA concluded that additional research and development would be necessary to produce FMVSS-level test procedures for V2V inter-device communication and potential safety applications.

- As a result of this item from the Readiness Report, NHTSA undertook additional research to examine the minimum performance measures for DSRC communication and system security.[35] The research included functional and performance requirements for the DSRC device, the results of which directly informed the development of this proposal. As we concluded in the Readiness Report, to eventually go forward with rulemaking involving safety applications, V2V and safety application standards need to be objective and practicable, meaning that technical uncertainties are limited, that tests are repeatable, and so forth. Additionally, the agency deferred consideration of whether standardization of DVIs would improve the effectiveness of safety applications, and whether some kind of standardization could have significant effects on costs and benefits.

- Standing up security and communications systems to support V2V: In order to function safely, a V2V system needs security and communications infrastructure to enable and ensure the trustworthiness of communication between vehicles. The source of each message needs to be trusted and message content needs to be protected from outside interference. A V2V system must include security infrastructure to credential each

[35] "Development of DSRC Device and Communication System Performance Measures" Booz Allen Hamilton, Final Report- May, 2016; FHWA-JPO-17-483 available at http://ntl.bts.gov/lib/60000/60500/60536/FHWA-JPO-17-483.pdf (last accessed Dec 12, 2016) and, CAMP research supporting SAE J2945-1, "On-Board System Requirements for V2V Safety Communications" April, 2016

message, as well as a communications network to get security credentials and related information from vehicles to the entities providing system security (and vice versa).[36]

- Liability concerns from industry: Auto manufacturers repeatedly have expressed concern to the agency that V2V technologies will increase their liability as compared with other safety technologies. In their view, a V2V system exposes them to more legal risk than on-board safety systems because V2V warning technologies rely on information received from other vehicles via communication systems that they themselves do not control. However, the decision options under consideration by NHTSA at the time of the Readiness Report involved safety warning technologies -- not control technologies. NHTSA's legal analysis indicated that, from a products liability standpoint, V2V safety warning technologies, analytically, are quite similar to on-board safety warnings systems found in today's motor vehicles. For this reason, NHTSA did not view V2V warning technologies as creating new or unbounded liability exposure for the industry.

- Privacy: NHTSA explained in the Readiness Report that, at the outset, readers should understand some very important points about the V2V system as then contemplated and understood by NHTSA. The system will not collect or store any data directly identifying specific individuals or their vehicles, nor will it enable the government to do so. There is no information in the safety messages exchanged by vehicles or collected by the V2V system that directly identifies the driver of a speeding or erratic vehicle for law enforcement purposes, or to third parties. The system—expected to be operated by private entities—will make it difficult to track through space and time specific vehicles, owners or drivers on a persistent basis. Third parties attempting to use the system to track a vehicle would find that it requires significant resources and effort to do so, particularly in light of existing means available for that purpose. The system will not collect financial information, personal communications, or other information directly linked to individuals. The system will enroll V2V enabled vehicles automatically, without collecting any information that identifies specific vehicles or owners. The system will not provide a "pipe" into the vehicle for extracting data. The system is designed to enable NHTSA and motor vehicle manufacturers to find lots or production runs of potentially defective V2V equipment without use of VIN numbers or other information that could identify specific drivers or vehicles. Our research to date suggests that drivers may be concerned about the possibility that the government or a private entity could use V2V communications to track their daily activities and whereabouts. However, NHTSA has worked hard to ensure that the V2V system both achieves the agency's safety goals and protects consumer privacy appropriately.

[36] Section II.F discusses NHTSA's Request for Information (RFI) regarding the development of a potential Security Credential Management System (SCMS).

- Consumer acceptance: If consumers do not accept a required safety technology, the technology will not create the safety benefits that the agency expects. At the time of the report, the agency believed that one potential issue with consumer acceptance could be maintenance. More specifically, if the security system is designed to require consumers to take action to obtain new security certificates – depending on the mechanism needed to obtain the certificates -- consumers may find the required action too onerous. For example, rather than accept new certificate downloads, consumers may choose instead to live with non-functioning V2V capabilities.[37]

3. Research conducted between the Readiness Report and this proposal

The findings of the V2V Readiness Report also yielded a series of research, policy and standards needs. The agency believed some of these needs were significant enough that they should be addressed to properly inform any potential regulatory action; such as this NPRM. The agency also identified some needs from the Readiness Report that could be addressed later to potentially support other aspects of V2Vdeployment such as safety applications. Following is a list of needs identified in the V2V Readiness Report and their current status. The agency has completed what it believes is the necessary research for to inform and support this proposal, although the agency is continuing to study these and other issues. The agency notes that Table II-4 shows the status of the research related to safety applications, which are not being proposed in this NPRM.

[37] As follow-up to other consumer acceptance topics, the agency undertook additional consumer acceptance research (both qualitative and quantitative) to better understand potential consumer concerns. This research was used to directly inform this proposal. *See* Section III for discussion of this research and how the agency used it to develop this proposal.

Table II-4 DSRC Performance Requirements and Compliance Testing Research (NPRM RELEVANT)

Readiness Report Research Need	Description	Research Projects Initiated to Address	Description	Completion Date
Standards Need V-1 SAE Standards Maturity	Currently Standards are being developed by outside standards organizations.	Crash Avoidance Metrics Partnership V2V Interoperability and V2V System Engineering Projects	Crash Avoidance Metrics Partnership providing results of DSRC device performance requirements to SAE standards development committee for SAE J2735 and J2945	April 2016
Research Need V-2 Impact of Software Implementation on DSRC Device Performance **Research Need V-3 DSRC Data Communication System Performance Measures** **Research Need V-5 BSM Congestion Sensitivity** **Research Need V-6 Relative Positioning Performance Test**	[V-2] V2V device software updates may be required over its lifecycle. NHTSA will need to determine how to ensure necessary V2V device software updates are seamless for consumers and confirmed. [V-3] The purpose of this research is to finalize the operational modes and scenarios, key functions, and qualitative performance measures that indicate minimum operational performance to support DSRC safety and security communication functions.	DSRC On-Board Unit Performance Measures Booze Allen and Hamilton Crash Avoidance Metrics Partnership - Documentation of On-Board Unit Requirements and Certification Procedures for V2V Systems (System Engineering Project) and V2V-Comminication Research project	BAH project will Develop performance measures for Dedicated Short Range Communication (DSRC) device; and develop security performance measures for the following, but not limited to Critical components on the DSRC device, Firmware on the DSRC device, Predominant elements in a Public Key Infrastructure (PKI). CAMP will develop a single comprehensive document summarizing the minimum level of Connected Vehicle (CV) V2V safety system on-board requirements and	BAH Completion date – Requirements October 2015/Test Procedures October 2015 CAMP System Engineering Completion date – Requirements Aug 2015/Test Procedures Sept 2015 CAMP Communications research completion date – August 2016

Research Need V-7 Vehicle and Receiver Positioning Biases **Research Need VI-7 Compliance Specifications and Requirements**	[V-5] Complete congestion mitigation and scalability research to identify bandwidth congestion conditions that could impair performance of safety or other applications, and develop appropriate mitigation approaches. [V-6] Research will be required to determine how to test relative positioning performance across GPS receivers produced by different suppliers and yield a generalized relationship between relative and absolute positioning. [V-7] Research to understand potential erroneous position reporting due to positional biases across multiple GPS receiver combinations. [VI-7] Development of performance requirements, test procedures, and test scenarios		certification procedures. CAMP V2V Communications Research Project will identify requirement in relation to BSM message congestion mitigation and misbehavior detection	

	to evaluate a device's compliance with interoperability standards, security communication needs; and to support safety applications.			

Table II-5 System, Security, and Acceptance Research (NPRM RELEVANT)

Readiness Report Research Need	Description	Research Projects Initiated to Address	Description	Completion Date
Policy Need IV-1 Road Side Equipment Authority	NHTSA will evaluate the need for DOT to regulate aspects of RSE operation and assess its authority for doing so.	Authority evaluation conducted for NPRM		Issuance of NPRM
Policy Need IV-2 V2V Device Software Updates	V2V device software updates may be required over its lifecycle. NHTSA will need to determine how to ensure necessary V2V device software updates are seamless for consumers and confirmed.	Crash Avoidance Metrics Partnership V2V System Engineering project and Crash Avoidance Metrics Partnership Security Credential Management System Proof of Concept project	The System Engineering project will investigate software update requirements from the vehicle perspective as the Security Credential Management Systems project investigates software update from the security system perspective. Both projects will identify requirements that will facilitate the software update of V2V devices.	Completion Date for Requirements – Sept 2015
Research Need V-1 Spectrum Sharing Interference	Evaluate the impact of unlicensed U-NII devices on the transmission and reception of safety critical warnings in a shared spectrum environment.	Testing spectrum sharing feasibility.	A test plan for testing unlicensed devices that would share the band with licensed DSRC devices has been developed. The testing will evaluate the feasibility of sharing spectrum with unlicensed devices.	The evaluation of spectrum sharing interference is pending the conduct of tests with representative U-NII-4 devices that operate in the 5.9 GHz (DSRC) frequency band. Testing could be completed within 12 months of receipt

				of prototype devices.
Research Need VII-1 Consumer Acceptance	Supplement the driver acceptance analysis completed per the Driver Clinics and Safety Pilot Model Deployment with further research that includes a focused assessment of privacy in relation to V2V technology	V2V Crash Avoidance Safety Technology Public Acceptance Review	This review needs to extend the current evaluation of driver acceptance to a broader public acceptance context and evaluate how public acceptance may impact and or influence the design, performance, operation, and implementation of this technology.	September 2015
Research Need VIII-1 V2V Location Tracking via BSM **Research Need VIII-2 V2V Identification Capabilities** **Research Need VIII-3 V2V Inventory of Privacy Controls** **Research Need VIII-4 V2V Privacy Risk Assessment** **Research Need IX-2**	[VIII-1] Assess the availability of information and technologies that facilitate linking data in the BSM to determine a motor vehicle's path [VIII-2] Understanding and quantifying risk of linking vehicle tracking or other information in the BSM to a specific vehicle, address, or individual via available resources (including but not limited to database matching or data mining)	Independent Evaluation of V2V Security Design and Technical Analysis of the Potential Privacy Risk of V2V Systems	The objective of this Task Order is to perform: (1) an independent and comprehensive technical analysis of the V2V security system design that is currently proposed specifically for a V2V connected vehicle environment; and (2) a technical analysis of the potential privacy risks of the entire V2V system that includes security but also focuses on the operation of V2V communications in support of crash avoidance safety applications.	March 2016

Cryptographic flexibility **Research Need IX-3 Independent Security Design Assessment**	[VIII-3] Inventory and assess the privacy controls applicable to the SCMS in connection with our comprehensive privacy assessment [VIII-4] A comprehensive privacy risk analysis of all aspects of the V2V system including infrastructure equipment, on-board vehicle systems, wireless and wired communications, as well as organizational and management issues. [IX-2] The chosen cryptographic algorithms are estimated to be resilient against brute force attack for a few decades with some susceptibility through an unanticipated weakness. In the future new algorithms could enable better performance but may require redesign of functions or operations within the SCMS. [IX-3] Independent evaluation			

	of CAMP/USDOT security design to assess alignment with Government business needs, identify minimum requirements, assess the security designs ability to support trusted messages and appropriately protect privacy, identify and remove misbehaving devices, and be flexible enough to support future upgrades.			
Research Need IX-1 Misbehavior Authority	Development of the processes, algorithms, reporting requirements, and data requirements for both local and global detection functions; and procedures to populate and distribute the CRL.	Crash Avoidance Metrics Partnership System Engineering project, Security Credential Management Proof of Concept project, and Communication Research Project	The CAMP System engineering project will investigate the implementation and device requirements for local (vehicle based) misbehavior detection and global (system-wide) misbehavior detection. The Communication Research project will research local and global misbehavior detection needs. The SCMS Proof of Concept will investigate implementation aspects from the security system perspective.	Initial Misbehavior Detection information to be completed December 2015.

Table II-6 V2V Safety Application Improvement and Performance Verification Research (NPRM IRRELEVANT)

Readiness Report Research Need	Description	Research Projects Initiated to Address	Description	Completion Date
Research Need V-4 Development of Safety Application Test Metrics and Procedures **Research Need VI-2 Safety Application Performance Measure Rationale** **Research Need VI-3 Practicability of Non-Ideal Driving Condition Testing** **Research Need VI-4 Fused and Non-Fused V2V Safety Application Test Procedures** **Research Need VI-5 Performance and Test Metric Validation**	[V-4] This research will take the performance measures and objective test procedures used during the research of V2V applications and develop FMVSS level performance measures and safety application objective tests. [VI-1] Assess the capability and capacity of possible refinements to reduce frequency of false positive warning while maintaining crash avoidance effectiveness. [VI-2] Develop a rationale to support each performance and test metric recommended for incorporation into an FMVSS. [VI-3] Evaluate test variations for non-ideal driving conditions (e.g., curved roads, turn signal use, weather, oblique intersections) and develop a rationale supporting the inclusion or exclusion of those test conditions.	Volpe False Alert Scenarios and Objective Test Procedures for Crash Avoidance Applications project and Vehicle Research and Test Center project	The Volpe project will support NHTSA development of false-positive warning objective test procedures in conjunction with development of objective test procedures and performance criteria for IMA, LTA, FCW, and BS/LCW applications. The results of this IAA will contribute to potential Federal Motor Vehicle Safety Standards (FMVSS) for these crash avoidance applications. The VRTC project will incorporate results and information from the Volpe project to develop Federal Motor Vehicle Safety Standards (FMVSS) for these crash avoidance applications.	Volpe Completion Date – December 2018 VRTC Completion Date – April 2019

	[VI-4] Develop test procedures that can be applied to systems relying solely on V2V information as well as "fused" systems, those relying on both V2V and other sources of information (e.g., on-board sensors). [VI-5] Conduct test validation to ensure that the performance and test metrics are objective, repeatable, and practicable.			
Research Need VI-1 False Positive Mitigation	Assess the capability and capacity of possible refinements to reduce frequency of false positive warning while maintaining crash avoidance effectiveness.	Volpe False Alert Scenarios and Objective Test Procedures for Crash Avoidance Applications project and	The Volpe project will support NHTSA development of false-positive warning objective test procedures in conjunction with development of objective test procedures and performance criteria for IMA, LTA, FCW, and BS/LCW applications.	Volpe Completion Date – December 2018
Research Need VI-6 DVI Minimum Performance Requirements	Determine DVI's impact on effectiveness of system and safety benefits applications to establish minimum performance for crash avoidance and objective test procedures.	V2V On-Road DVI Project	Testing DVIs for Intersection Movement Assist and Left Turn Assist for stopped vehicles.	VTTI Completion Date: Novemb 2016

D. V2V International and Harmonization Efforts

Section V.F of NHTSA's Readiness Report detailed key similarities and some differences between U.S., European, and Asian V2X implementation approaches. There are several organizations in Europe and Asia conducting activities related to V2V and V2I communications and the U.S. DOT has established ongoing coordination activities with these regions and their representing organizations. For Europe, these organizations include DG CONNECT and the CAR 2 CAR Communications Consortium (C2C-CC). DG CONNECT is the EU directorate responsible for conducting research and pilot projects related to connected vehicles and C2C-CC has been working closely with CAMP as part of the EU-US V2X Harmonization Program.

A number of commenters to the ANPRM/Readiness Report addressed the issue of global harmonization. Most commenters addressing the issue encouraged the agency to pursue global harmonization between the U.S., EU, and Asia-Pacific regions as a way to reduce costs,[38] and also to facilitate cross-border traffic, as between NAFTA countries.[39] A number of commenters discussed existing or under-development technical standards by bodies such as ETSI, ISO, and the EU-US Task Force on ITS, and called on NHTSA to support them,[40] and some commenters suggested that NHTSA work to develop a Global Technical Regulation (GTR) and facilitate harmonization through that approach.[41]

With regard to what specifically should be harmonized, commenters mentioned hardware,[42] software,[43] DVI,[44] and BSM,[45] although Cohda Automotive argued that global harmonization efforts have effectively already resulted in a single hardware platform being possible, and that different software could run in each region.[46] Some industry commenters cautioned, however, that NHTSA should not let harmonization objectives impede safety.[47] Mercedes expressed concern that harmonization should not just be global, but also consider the risk of a patchwork of differing State regulations for advanced technologies, and asked that NHTSA work with State DOTs to avoid this.[48]

NHTSA recognizes the value of implementing V2V in a globally-harmonized way. Consistency could reduce costs, complexity, and contribute to a successful, long-term sustainable

---

[38] Mercedes at 7; Alliance at 50; Automotive Safety Council at 3; Harley-Davidson at 2; Volvo Group at 3;
[39] Alliance at 50; Global at 19-20; Pennsylvania DOT at 7; TRW Automotive at 7;
[40] Mercedes at 7; Systems Research Associates, Inc., at 10; SAE International at 5; Delphi at 10; Continental Automotive Systems at 3.
[41] Automotive Safety Council at 3; Volvo Group at 4;
[42] Mercedes at 7.
[43] Mercedes at 7.
[44] Automotive Safety Council at 3; TRW Automotive at 7.
[45] TRW Automotive at 7.
[46] Cohda Wireless at 9.
[47] Alliance at 50, Global at 19-20.
[48] Mercedes at 8.

deployment. As discussed in the V2V Readiness Report, significant V2V research and development activities have been completed and continue in both Europe and Asia. Real-world deployments have been announced in both regions focusing on V2I systems to aid drivers and to attempt improvements in traffic flow.

Collaboration between organizations and governmental bodies in the U.S. and Europe has led to extensive harmonization of the criteria for hardware, message sets, security, and other aspects needed to support V2V between the two regions. It will be possible to use common radios and antennas in both regions. Harmonization could potentially be enhanced by this proposal by prompting solidification of the work focusing on security and message performance requirements for common applications. The connected vehicle applications being developed in Europe place a much stronger priority on mobility and sustainability compared to U.S. focus on safety applications.

Japan, Korea and Australia are the Asia-Pacific countries most involved in pursuing DSRC-based V2X communications. In Japan, MLIT's current V2X approach centers on the adaptation of their electronic tolling system operating at 5.8 GHz. Additionally, some Japanese OEMs (mainly Toyota) are actively supporting the deployment of V2X using 760 MHz communications. Development of message sets in Japan is not yet complete but appears to be moving in a similar direction as the message sets harmonized between Europe and the U.S. Korea currently uses the 5.835 – 5.855 GHz band for Electronic Toll Collection and DSRC experimentation. Korea has performed field tests for V2V communication in this band. Industry sources indicate that Korea may shift DSRC for ITS to 5.9 GHz to be more aligned internationally.

In Australia, Austroads is the association of Australian and New Zealand road transport and traffic authorities. This organization is currently investigating potential interference issues, and working with affected license holders to evaluate the feasibility of use of the 5.9 GHZ spectrum for V2X in Australia. Another agency, Transport Certification Australia, is leading the design for security requirements, supporting field deployments, and working with the Australian Communications and Media Authority (ACMA) on identifying requirements for spectrum usage. Because the Australian vehicle market is predominantly comprised of imports from the U.S., Europe, and Asia, these Australian agencies have joined in the international harmonization efforts to ensure that the vehicle brought into the country are interoperable with each other and with the new cooperative infrastructure equipment and applications emerging on the market.

Canada has reserved spectrum at 5.9 GHz for V2X and is watching developments in the U.S. closely.

Harmonization and joint standardization is performed under an Implementing Arrangement for Cooperative Activities. This memorandum between the U.S. DOT and the

European Commission established a collaborative relationship in 2009 and it was renewed in December 2014.[49]

The harmonization and collaboration on standards is governed by a Harmonization Work Plan that has generated a set of smaller, flexible task groups to focus on specific subjects. The completed and ongoing task groups and their status are the following:

- **Harmonization Task Group (HTG) 1 on Security Standards and HTG3 on Communications Standards** performed their analysis in 2011 with completion of results in 2012. HTG1 (which included experts from ISO, CEN, ETSI, IEEE) worked in coordination with HTG3 to identify the subset of available standards to provide assurance of interoperable security measures in a cooperative, interoperable environment. Because HTG 1 and HTG 3 issues were sufficiently interrelated and the HTGs had a significant overlap in membership, work on these topics was conducted jointly. The analysis documented how implementations of the protocol stack might not be interoperable because the specification of technical features from various Standards Development Organizations (SDOs) was different or incomplete. These differences presented interoperability challenges. HTG1 and 3 results provide guidance to the SDOs for actions to be taken that raise the assurance of security interoperability of deployed equipment. Vehicle connectivity through harmonization of standards and architecture will reduce costs to industry and consumers, in that hardware and/or software development costs will be spread over a larger user base, resulting in reduced unit costs. Differences between vehicles manufactured for different markets will also be minimized, allowing private-sector markets to have a greater set of global opportunities. A final outcome of the HTG1 and HTG3 work was recognition of the need to harmonize security policies and standards. To meet this need, a third HTG (HTG6) was established to explore and find consensus on management policies and security approaches for cooperative ITS.

- **HTG2 on Harmonization of US BSM and EU CAM**: The goal of HTG2 was to harmonize the vehicle-to-vehicle safety messages that had been developed within the EU and separately within the U.S. The group was able to harmonize on the hardware issues. However, differing U.S. and EU software approaches and institutional issues constrained the extent to which a single, cross-region safety

[49] "Continuation of the Implementing Arrangement between the U.S. Department of Transportation and the European Commission " http://www.its.dot.gov/press/2015/euro_commission.htm#sthash.URMW4OOH.dpuf (last accessed Dec 8, 2016)

message set could be developed. While a single message set did not result, the HTG was able to evolve the two messages in a manner such that simple software translation between the two message sets is sufficient to allow cross-compatibility. It was a significant step to be able to have the two message sets become substantially closer in nature. These advancements will facilitate deployment across multiple regions using similar or identical hardware and software modules.

- **HTG4/5 on Infrastructure Message Standards:** HTG 4/5 is currently in-progress. Its scope is to address the need for standardized Vehicle-to-Infrastructure message sets and interfaces, including:

    - Signalized intersections applications such as Signal Phase and Timing, Signal Request, Signal Status,

    - In-vehicle data message sets.

  At this point, there is general agreement on the data concepts in these message sets, but there remain differences in how the data is conveyed between the infrastructure and the vehicles. These differences are due to project and communications restrictions. For example, the U.S. is planning for additional message sets for enhanced functionality; whereas the European approach may limit the initial applications and simply add data elements to the messages over time. ISO Technical Specification 19091, a standard covering to V2I and I2V communications for signalized intersections, is currently under development and is incorporating both harmonized content and recognizing region-specific content--a practical compromise resulting from existing differences in signal standards. Overall, 19091 allows for substantial hardware congruity while acknowledging that fully identical message standards are not viable at this time.

- **HTG6 on Harmonized Development of a Cooperative-ITS Security Policy Framework**. HTG6 assessed security policy needs across international, regional, and local levels. Analysis was performed to determine optimal candidate guidelines for policy areas. HTG6's intent was to identify where harmonization is desirable by exploring the advantages and limitations of global versus local security policy alternatives, including economic benefits. Implementation of harmonized policies engenders and sustains public trust in the C-ITS system and applications, particularly with a highly mobile environment that expects C-ITS services to remain available as they cross borders as well as over time. The task group is identifying the largest set of common approaches and interfaces for harmonization, recognizing that there will be multiple instantiations of security entities within and adjacent to geographic/jurisdictional borders. Although

minimizing the number significantly decreases cost and complexity, decisions to own and operate security occur for diverse reasons, specifically because of differing jurisdictional requirements for security levels, privacy, cryptographic choices, or trust model choices. The group's analysis recognizes the benefits for commonality and identifies those policies and harmonized interfaces that support regional implementations that might diverge. At the time of developing this proposal, most of the reports from this activity are posted.[50]

The SCMS development activity has incorporated key outcomes of this activity, some of which include:

- Implementation of harmonized policies engenders and sustains public trust in the C-ITS system and applications, particularly within a highly mobile environment that expects C-ITS services to remain available as networks evolve over time and as services cross borders.
- To support cross-border/cross-jurisdictional operations of C-ITS applications, individual security systems (known as C-ITS Credential Management Systems or CCMS) require a defined range of harmonized processes as well as specific, secure data flows to support digital auditing and system transparency.
- Planning for inter-CCMS or intra-CCMS communications will require decisions when developing near-term operational systems but those decisions may have longer-term impacts on crypto-agility, system flexibility, and evolution of systems that must be considered from the start.
- Critical near-term steps for policy and decision makers to perform include:
    - Minimize the number of CCMS: Policy makers must determine the number of CCMS that will be operational within a local, regional, or national jurisdiction. Increasing the number of CCMS, in particular the root authorities, significantly increases complexity and cost.
    - Assess risk and set appropriate parameters for risk and privacy: No system will ever be without risk. Policy and decision makers must set acceptable levels of internal and external risk, as well as levels of privacy protection. Further, systems managers must assess these levels continuously throughout the lifecycle both of the security solution as well as end-entity (user) devices and applications. Risk and privacy levels come with trade-offs that will need to be assessed by policy makers.
    - Choose appropriate trust models: After system managers assess and categorize risk, they can identify policy and technical controls to mitigate risk. Collectively, these controls support the implementation of trust

[50] "Harmonized security policies for cooperative Intelligent Transport Systems create international benefits" October 16, 2016. https://ec.europa.eu/digital-single-market/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international (last accessed: Dec 8, 2016)

models that range from no trust among security entities to full trust that allows users ("trusted actors" that are accepted into the C-ITS security environment) to receive security services even after leaving their "native" system in which they are enrolled. Decisions are also required to establish criteria that define who are trusted actors and policies and procedures for certification, enrollment, removal in the event of misbehavior, and reinstatement.

- Establish Governance: These decisions include the identification and convening of key stakeholders who will require representation in ongoing decision-making. Once convened, this group will establish processes for decision-making, define criteria for new entrants into the governance process, assign roles and responsibilities, establish authority to provide governance and enforcement, and determine enforcement procedures.
- Implement harmonized processes: The HTG6 team identified the priority areas for harmonization in report HTG6-3 and identified the interfaces and data flows where the policies would be applied in HTG6-4. Policy makers will need to examine them to determine which ones are appropriate both to support their choice in trust models and throughout the CCMS lifecycle.

HTG group members comprise a small group of international experts who worked together intensively with co-leadership. Members are provided by the EC DG-CONNECT and U.S. DOT, and typically chosen from among the editors of many of the current cooperative ITS standards in the different SDOs providing direct linkages into those SDO activities, as well as representatives of the EU and U.S. DOT and the Vehicle Infrastructure Integration Consortium (VIIC), and expert representatives from roadway and infrastructure agencies, system integrators, and policy analysts. HTG6 expanded the membership beyond the EC and U.S. DOT to include Transport Certification Australia (TCA) plus observers from Canada and Japan.

As the U.S. is taking the lead in potential V2V deployment, whereas Asia and Europe are focusing primarily on V2I implementation, the agency expects that a finalized implementation driven by this proposal will set precedent and potentially adjust standards for V2V implementation globally.

E. V2V ANPRM

To begin the rulemaking process, NHTSA issued an ANPRM on August 20, 2014.[51] Accompanying the ANPRM, NHTSA also published a research report discussing the status of V2V technology and its readiness for application ("V2V Readiness Report").[52] NHTSA's goal in releasing these two documents in 2014 was to not only announce the agency's intent to move

[51] 79 FR 49270.
[52] Docket No. NHTSA-2014-0022-0001.

forward with the rulemaking process, but also to comprehensively collect all of the available information on V2V and present this information to the public to collect comments that would further help the agency refine its approach with regard to V2V.

1. Summary of the ANPRM

In the ANPRM and the accompanying V2V Readiness Report, we emphasized the capability of V2V to be an enabler for many advanced vehicle safety applications as well as an additional data stream for future automated vehicles.[53] We also stated our belief that a mandate to include DSRC devices in all vehicles would facilitate a market-driven approach to safety, and possibly other, application deployment.[54]

Current advanced vehicle safety applications (e.g., forward collision warning, automated braking, lane keeping, etc.) use on-board sensors (e.g., cameras, radars, etc.) to perceive a vehicle's surroundings. Because each type of sensor has advantages and disadvantages under different conditions, manufacturers seeking to incorporate advanced functions in their vehicles are increasingly relying on sensor fusion (i.e., merging information from different sources) to ensure reliable information is available to the vehicle when it makes crash-imminent decisions. When compared to on-board sensors, V2V is a complementary, and unique, source of information that can significantly enhance the reliability of information available to vehicles. Instead of relying on each vehicle to sense its surroundings on its own, V2V enables surrounding vehicles to help each other by communicating safety information to each other. In addition, V2V enables new advanced vehicle safety functionality because it enables vehicles to receive information beyond the range of "traditional" sensing technology.

One important example that we mentioned in the ANPRM is intersection crashes.[55] Because of V2V's ability to provide vehicles with information beyond a vehicle's range of perception, V2V is the only source of information that supports applications like Intersection Movement Assist (IMA) and Left Turn Assist (LTA). These applications have the unique ability to address intersection crashes, which are among the most deadly crashes that drivers currently face in the U.S.[56]

However, in spite of the benefits of the technology, we explained in the ANPRM that we did not expect that V2V technology would be adopted in the vehicle fleet absent regulatory action by the agency.[57] Due to the cooperative nature of V2V, we stated that early adopters of the technology would not realize immediate safety benefits until a sufficient number of vehicles

---

[53] 79 FR 49270.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*

in their geographical area have the technology.[58] In other words, early adopters incurring the costs to equip their vehicle to transmit BSM information about their vehicle would not realize the benefit of the V2V information environment unless other vehicles in their surroundings are also transmitting and receiving BSM information.

In the V2V Readiness Report,[59] we observed that, based on the data collected from the Safety Pilot Model Deployment Project, V2V systems work in real world testing. V2V-equipped vehicles successfully exchanged BSM information with each other and issued warnings to their drivers.[60]

We further discussed and summarized our preliminary information regarding many of the technical aspects of a potential rule including: the types of safety problems that could be addressed by V2V,[61] the potential technological solutions to those problems (V2V-based or otherwise),[62] the potential hardware/software component that could be used in DSRC devices,[63] the applications that could be enabled by V2V,[64] and preliminary design concepts for a security system for the V2V environment.[65]

The report also explored various important policy issues including: the agency's legal authority over the various aspects of the V2V environment (e.g., the vehicle components, aftermarket devices, etc.),[66] issues that may be outside the scope of NHTSA's activities,[67] privacy and public acceptance concerns over V2V technology,[68] and potential legal liability implications.[69] In addition, we began the process of analyzing the costs of a potential rule to require V2V capability in vehicles based on different technology assumptions and different scenarios for adoption.[70] While we acknowledged that there are a variety of potential benefits of V2V, we conducted a preliminary estimate of the benefits attributable to two V2V-specific safety applications.[71] Finally, throughout the V2V Readiness Report, we also identified various research and policy gaps in each of the substantive areas that we discussed.[72]

---

[58] *Id.*
[59] V2V Readiness Report. Docket No. NHTSA-2014-0022-0001. Page xv.
[60] *Id.* at xv.
[61] *Id.* at 15.
[62] *Id.* at 25.
[63] *Id.* at 65.
[64] *Id.* at 119.
[65] *Id.* at 158.
[66] *Id.* at 33.
[67] *Id.* at xvi.
[68] *Id.* at 133.
[69] *Id.* at 208.
[70] *Id.* at 216.
[71] *Id.* at 259.
[72] *See e.g., id.* at xix.

In the context of the V2V Readiness Report, the ANPRM asked 57 questions to help solicit comments from the public more effectively. [73] While the questions we asked in the ANPRM covered a variety of subjects, many of our questions covered issues relating to estimating costs and benefits.[74] For example, we asked the public about potential ways to obtain real-world test data concerning the effectiveness of V2V safety applications and whether we have identified the relevant potential crash scenarios for calculating benefits.[75] On the same subject, we asked if preferring certain technologies over others in the situation of a network good[76] such as V2V would lead to any detrimental impact.[77]

The ANPRM questions also covered policy issues such as legal interpretation of NHTSA's authorities under the Motor Vehicle Safety Act,[78] and how commenters view the public's potential acceptance/non-acceptance of V2V technology.[79] The ANPRM also posed technical questions such as, how can the agency mandate V2V can help ensure interoperability, whether the Safety Pilot Model Deployment sufficiently demonstrated interoperability, and whether standards under development by organizations such as IEEE and SAE could help ensure interoperability.[80]

We raised important questions regarding the potential sharing of the DSRC spectrum allocation by soliciting comments on potential sharing and, if so, ideas on how to share the spectrum safely.[81] In addition, we requested comment on the usefulness of our concepts for a potential security design (i.e., PKI)—including specific elements like the certificate revocation list (CRL), whether the system would create new "threat vectors," sufficiently protect privacy, how DSRC devices could be updated, and potential cybersecurity threats.[82]

2. Comments to the ANPRM

In response to the ANPRM, the V2V Readiness Report, and our questions, we received more than 900 comments.[83] The agency received responses to the ANPRM from a diverse set of commenters representing a wider range of perspectives than with other agency safety rules. They range from more traditional commenters to NHTSA safety rulemakings (e.g., automobile manufacturers/suppliers, trade associations, standards development organizations, safety

---

[73] 79 FR 49270, 49271.
[74] *Id. See also id.* at 49273-24
[75] *Id*. at 49271.
[76] A network good's value to each user increases when the number of users of that good increase (e.g., telephone). In other words, increasing the number of users creates a positive externality.
[77] *Id.*
[78] *Id.*
[79] *Id*. at 49273.
[80] *Id*. at 49272.
[81] *Id*.
[82] *Id*. at 49273.
[83] *See* Docket No. NHTSA-2014-0022.

advocacy groups, individual citizens, etc.) to newer participants in such rulemakings such as technology/communications companies, other state/federal agencies, and privacy groups. The comments also covered a wide variety of topics ranging from the technical details of V2V technology to the policy implications of any potential rule. While this document discusses the relevant comments in much greater detail when discussing each aspect of the proposal (in the sections that follow), the paragraphs here contain a sampling of the types of commenters and the major issues they raised.

While expressing general support, the automotive manufacturers stated their belief that the Federal government needs to assume a large role in establishing key elements of the V2V environment (e.g., establishing common operating criteria for V2V devices, establishing a security credentials system, preserving the 5.9 GHz spectrum for V2V safety, and mandating devices in new vehicles).[84] The automotive manufacturer commenters discussed their legal concerns (including concerns over practicability of an FMVSS if certain aspects of the V2V environment are missing and potential legal liability for manufacturers).[85] While generally agreeing with our assessment regarding the readiness of some of the industry technical standards to ensure that V2V communications work, the automotive manufacturer commenters also emphasized the importance of privacy and public acceptance to the success of the technology.[86] In spite of some of these open policy and technical questions, many automotive manufacturer commenters also agreed that a regulation or requirement defining key items needed for interoperability is necessary to realize the full potential benefits of V2V.[87]

Automotive suppliers generally expressed support for the technology as well. They further generally opined that the technology and standards for the technology are mature enough for initial deployment. For example, DENSO[88] stated that DSRC is a suitable technology for implementing V2V safety applications and that the current BSM is adequate to support those purposes. Continental further commented that V2V demonstrations thus far show that the system works and is interoperable.[89] Raising different points, Delphi commented that the coverage of a potential V2V rule should include more than just the vehicles contemplated in the ANPRM and that the technology should be developed in conjunction with the vehicle-resident systems.[90]

Safety advocacy groups also expressed support, but emphasized the importance of ensuring interference-free spectrum for V2V. For example, the American Motorcyclist Association stressed the need for interference-free spectrum to ensure the safety applications will

---

[84] *See e.g.,* Comments from the Alliance of Automobile Manufacturers, Docket No. NHTSA-2014-0022-0603
[85] *See id.*
[86] *See id.*
[87] *See e.g.,* Comments from Ford Motor Company, Docket No. NHTSA-2014-0022-0953.
[88] *See* Docket No. NHTSA-2014-0022-0655.
[89] *See* Docket No. NHTSA-2014-0022-0414.
[90] *See* Docket No. NHTSA-2014-0022-0266.

function. V2V, in their view, has the unique capability to address crashes that represent a significant portion of motorcycle crashes (e.g., left turn across path crashes).[91] They also emphasized the importance of a uniform human-machine interface for safety applications (regardless of whether the applications use V2V or vehicle-resident based information).[92] Other safety advocacy groups (e.g., the Automotive Safety Council) covered a large variety of topics (e.g., emphasizing the importance of interoperability, the ability of V2V to work in conjunction with vehicle-resident systems, and expressing concern that the security system described in the report would not sufficiently protect against all forms of "abuse" of the V2V environment).[93]

Two standards development organizations also submitted comments. The two organizations (SAE and IEEE) were involved in developing various standards incorporated in this proposed rule. Both generally expressed support for the agency's proposal and stated that—in spite of on-going research—the standards are mature enough to support deployment of DSRC devices and ensure that they are interoperable.[94] Where the standards organizations differed was their opinion concerning spectrum availability. SAE reiterated its concern that "interference-free spectrum" is critical for the V2V environment.[95] While IEEE suggested that spectrum sharing is feasible, they opined that DSRC deployment should not wait for further research on spectrum sharing.[96] Instead "acceptable sharing parameters" may be determined at a later date after DSRC deployment and further research.[97]

While expressing general support for the technology and NHTSA's efforts in this area, technology/communications device manufacturers expressed two general concerns. Through their trade associations,[98] such manufacturers raised questions about NHTSA's authority to regulate software and mobile devices.[99] In addition, individual companies (e.g., Qualcomm[100]) and other associations (e.g., the Wi-Fi Alliance[101]) expressed their opinion regarding the viability of spectrum sharing with unlicensed Wi-Fi devices and the ability of V2V to flourish alongside other technologies that will benefit automotive and highway safety. Finally, the Information Technology Industry Council stated its belief that NHTSA needs to ensure that connected

---

[91] *See* Docket No. NHTSA-2014-0022-0646.
[92] Consumers Union discussed the HMI and how warnings need to be effectively communicated to the driver. *See* Docket No. NHTSA-2014-0022-0533.
[93] *See e.g.,* Docket No. NHTSA-2014-0022-0511.
[94] *See e.g.,* Docket No. NHTSA-2014-0022-0597.
[95] *See id.*
[96] *See* Docket No. NHTSA-2014-0022-0693.
[97] *Id.*
[98] CTIA—The Wireless Association and the Consumer Electronics Association.
[99] *See e.g.,* Docket No. NHTSA-2014-0022-0483.
[100] *See* Docket No. NHTSA-2014-0022-0665.
[101] *See* Docket No. NHTSA-2014-0022-0644.

vehicle technologies are allowed to develop using different technological solutions (e.g., other communications mediums beyond DSRC).[102]

Other government agencies also submitted comments. The NTSB commented that both V2V and vehicle-resident crash avoidance technologies are important and they are complementary—especially when one (vehicle-resident) fills the gap during the deployment of the other (V2V).[103] State agencies also commented.[104] AASHTO also mentioned that interference-free spectrum is critical and commented that supporting future upgrades to the system through software rather than hardware changes would be important for state agencies.[105]

A significant number of commenters also raised privacy concerns with this rulemaking. In addition to a large number of individual commenters, organizations such as EPIC stated that, since a potential rule would create significant privacy risks, they recommend that the government take various actions to protect the information (e.g., establish when PII can be collected, when/where information can be stored, additional encryption methods, and require adherence to Consumer Privacy Bill of Rights).[106] In addition, Professor Dorothy Glancy expressed concern that NHTSA plans to conduct its privacy analysis after the ANPRM stage of the rulemaking process and is concerned that not all potential data collection is accurately portrayed in the ANPRM.[107] On the other hand, while the FTC agreed that privacy concerns could exist in the V2V environment related to (1) obtaining the vehicle location information and (2) pricing insurance premiums over the driving habits, it believes NHTSA has taken these concerns into account.[108]

Finally, many individual citizen commenters (in addition to the topics covered above) discussed their perception that this rulemaking proposes to mandate a technology that poses a potential health concern. The EMR Policy Institute[109] expressed similar concerns stating that NHTSA should postpone this rulemaking until the FCC changes their guidelines regarding human radiation exposure to wireless communications.

---

[102] *See* Docket No. NHTSA-2014-0022-0403.
[103] *See* Docket No. NHTSA-2014-0022-0267.
[104] State DOTs from also stress the need to have uniform HMI—serving a purpose similar to the MUTCD for traffic signs and signals. They also commented that other vehicle types that could benefit from V2V (e.g., vehicles with GVWR greater than 10,000) and mentioned the potential of other V2X applications (e.g., vehicle to rail, agricultural equipment, horse-drawn vehicles). Further they opine that mandate is needed to deploy quickly. *See e.g.*, Comment from PennDOT, Docket No. NHTSA-2014-0022-0371; TxDOT, Docket No. NHTSA-2014-0022-0218; Wisconsin DOT, Docket No. NHTSA-2014-0022-0507.
[105] *See* Docket No. NHTSA-2014-0022-0420.
[106] *See* Docket No. NHTSA-2014-0022-0689.
[107] *See* Docket No. NHTSA-2014-0022-0331.
[108] *See* Docket No. NHTSA-2014-0022-0502.
[109] *See* Docket No. NHTSA-2014-0022-0682.

F. SCMS RFI

Approximately 30 days after issuing the agency's Advance Notice of Proposed Rulemaking (ANPRM)[110] and V2V Readiness Report, NHTSA released a Request for Information (RFI)[111] regarding a Security Credential Management System (SCMS) that could support a national deployment of a V2V communication system. NHTSA was interested in hearing from entities interested in establishing components of an SCMS or the SCMS, itself. The RFI was issued separately from the ANPRM and V2V Readiness Report to give potential respondents additional time to review the more-detailed V2V Readiness Report content on the SCMS, allowing time for respondents to formulate informed responses to the Agency's questions about how an SCMS should be designed and whether they would be interested in developing or operating components or the SCMS, as a whole. As discussed in the ANPRM and V2V Readiness Report, we explained that NHTSA would not require the SCMS by regulation and did not expect to establish, fund or operate the SCMS.

Questions in the RFI covered topics such as potential governance structures for the SCMS, requests for estimates of necessary initial capital investment, how respondents believed the SCMS (or the components that they were interested in operating) could generate revenue and be financially sustainable (in order to ensure its uninterrupted operation), what respondents thought of the current SCMS design and, finally, the respondent's interest in standing up and operating some or all of the components of the national V2V SCMS.

NHTSA received 21 responses by the December 15, 2014 response closing date, and approximately 11 respondents indicated an interest in running some or all components of the SCMS. The remaining responses commented more generally on issues of potential governance and liability with two common themes: (1) that the Federal Government should take the lead in standing up and operating the SCMS; and (2) that the Federal Government should indemnify companies participating in the SCMS from liability.

The RFI respondents included vehicle manufacturers, software component developers and suppliers, cryptography experts, certificate management entities, satellite and cellular service providers and academia. Because the process of deploying cooperative V2V technology and supporting establishment of an SCMS both are unprecedented activities, the agency believed it was appropriate to meet with the subset of eleven respondents who expressed interest in operating aspects of the SCMS or the SCMS as a whole. These meetings ensured that the agency and the individual respondents shared a mutual understanding of each respondent's comments, their potential role in an SCMS, and the agency's views on the ways in which an SCMS could be established and deployed.

---

[110] 79 FR 49270 (Aug. 20, 2014).
[111] 79 FR 61927 (Oct. 15, 2014).

Meeting discussions covered a wide range of topics – including details of cryptography intricacies, certificate distribution methodologies, root storage and protection, to potential overall SCMS management. NHTSA found these meetings to be very beneficial in terms of introducing the agency to some new potential stakeholders and service providers different than the vehicle OEMs and suppliers with whom NHTSA typically. The diversity of RFI respondents exemplified the multi-stakeholder and cross-cutting nature of the V2V ecosystem.

Additional details on the SCMS RFI responses can be found in Section V.B.4.

III. Proposal to regulate V2V Communications

A. V2V Communications proposal overview

The agency believes that it will not be possible to begin to address the 3.4 million crashes identified in Section II.A, especially the intersection crashes and left-turning crashes, given today's vehicle-resident technology offerings. As described earlier, the limitations of current sensor-based safety systems, in terms of direction and distance, likely will not be able to address intersection and left-turning crashes, among other potential crash scenarios, as effectively as V2V communications could.

The agency's proposal to regulate V2V technology is broken into distinct functional components, some of which have alternatives that could potentially be employed "in-conjunction-with" or "in-place-of" the agency's proposal. The distinct functional components are: the actual communications technology itself (Section III.E), proposed messaging format and content requirements (Section III.E.2), , authenticating V2V messages (Section III.E.3), V2V device misbehavior detection and reporting (Section III.E.4), malfunction indication requirements (Section III.E.5), software and certificate updating requirements (Section III.E.6), and proposed cybersecurity related requirements (Section III.E.7).

B. Proposed V2V Mandate for new light vehicles, and performance requirements for aftermarket for existing vehicles

NHTSA's proposal would require that new light vehicles include vehicle-to-vehicle communication technology able to transmit standardized BSMs over DSRC as described in Section III.E below, beginning two years after issuance of a final rule and phasing in over the following three years at rates of 50 percent, 75 percent, and 100 percent, respectively. "Light vehicles," in the context of this rulemaking, refers to passenger cars, multipurpose passenger vehicles, trucks, and buses with a gross vehicle weight rating of 10,000 pounds (4,536 kilograms) or less.[112] The agency believes that this amount of lead time and phase-in is needed

[112] "Passenger cars," "multipurpose passenger vehicles," "trucks," and "buses" are defined in 49 CFR 571.3. Some commenters suggested that the agency's proposal also cover vehicles like motorcycles and horse-drawn buggies

based on the potential for device supply constraints to generate production-level quantities of devices required by automotive OEMs to meet the standard[113] and to allow flexibility for vehicle refresh and re-design cycles. The proposal also allows vehicles to comply using non-DSRC technologies that meet certain performance and interoperability standards.

In addition to requiring new light vehicles to be able to transmit and receive BSMs over DSRC, the proposal would also require that similarly-capable aftermarket devices achieve the same DSRC performance.

Besides being the first FMVSS to involve vehicles relying on information transmitted by other vehicles, this FMVSS would also be the first to incorporate elements of secure wireless communication protection directly into the performance requirements.[114] New motor vehicles are increasingly computerized, and given the importance of ensuring the availability and integrity of safety-critical systems, we considered which requirements could best be incorporated into an FMVSS and which should be part of the V2V security system instead. V2V security requirements are discussed in Section III.E.3 and Section III.E.7, along with a discussion of privacy and security in Section IV.

The agency has put forth this proposed rule on the basis that a fully-implemented V2V system, as currently envisioned, is a compilation of many elements that provide a data-rich technology platform that ensures secure and interoperable communications enabling safety warnings and advisories for drivers. As described in the V2V Readiness Report, V2V devices send out BSMs to alert other vehicles to their presence, and receive BSMs from other vehicles in order to determine whether to warn their drivers of an imminent crash situation. BSMs must be accompanied by message authentication capabilities so that the receiving V2V communication will allow suppliers and vehicle manufacturers to innovate and spur the market for applications that will provide consumers increased safety.

(Wisconsin DOT), or heavy vehicles (Bendix, among others). Both motorcycles and HVs were included in the Safety Pilot Model Deployment, but in very small numbers, and the agency believes that more research is needed than what is available at the time of this NPRM before we are ready to propose requirements for those vehicles. The agency will be making a decision on how to proceed with V2V capability for HVs at a later date. For buggies, these would not be considered motor vehicles, but we are optimistic that V2X capability may eventually be available for them.

[113] Impact of Light Vehicle Rule on Consumer/Aftermarket Adoption- Dedicated Short Range Communications Market Study, Intelligent Transportation Society of America, FHWA-JPO-17-487, available at http://ntl.bts.gov/lib/60000/60500/60535/FHWA-JPO-17-487_Final_.pdf (last accessed Dec 12, 2016)

[114] To be clear, the related performance requirements for V2V communication security will incorporate protections to ensure a secure vehicle communication that are distinct from other types of communications with the vehicle for other data transfers and interconnectivity. The performance requirements for V2V security communications do not and are not intended to provide comprehensive protection for other vehicle wireless communications or internal vehicle connectivity for operational functionality. That responsibility continues to belong to manufacturers.

The agency believes that a mandate for all light vehicles is necessary to achieve the safety goals of this proposal. The two vital pieces in order to achieve these crash avoidance benefits are (1) ensuring interoperable V2V communications, and (2) achieving a critical mass of communicating vehicles in the American fleet. NHTSA believes that this proposal is the only way to achieve these two pieces because of the lagging adoption of advanced safety technologies in the marketplace. As evidenced by the slow voluntary deployment of vehicle sensor-based advanced driving assistance systems, the agency believes that it will be even more difficult to achieve a critical V2V implementation level without a mandate due to the cooperative nature of the V2V system. If it cannot reach a critical deployment level within a certain timeframe, the safety benefits of V2V would drop dramatically, and manufacturers would have much less incentive to develop the safety applications (despite their relatively low costs) because they would not have a reason to make the initial investment to install the V2V communications equipment. This represents a classic "collective action" problem, of the sort that government regulation is designed to address. We do not believe that critical mass can be achieved, allowing the life-saving benefits of V2V to come to fruition, in the absence of a government mandate. We seek comment on these tentative conclusions.

NHTSA received a number of comments to the ANPRM and the V2V Readiness Report suggesting that V2V communication technology could be better encouraged through what the agency refers to as an "if-equipped" standard rather than a mandate for all new light vehicles – i.e., that NHTSA should simply set a standard saying "*if* a new vehicle is equipped with devices capable of V2V communications, then it should meet the following requirements." While both options are within the agency's regulatory authority, we continue to believe that requiring V2V communication technology for new light vehicles will be the quickest and most effective way to achieve fleet-wide V2V communication technology deployment and ensure the full safety potential of this technology is realized.

Allowing manufacturers to choose whether to apply V2V technology in new vehicles could have two main risks in terms of holding back potential safety benefits. First, it is uncertain how manufacturers would voluntarily deploy V2V capability. Manufacturers typically have implemented new vehicle-resident technologies in their more expensive vehicles first. If manufacturers take this approach for V2V, NHTSA believes that a segmented approach to implementation of V2V technology will not be enough to quickly precipitate the data-rich environment needed to support development of manufacturer-supplied safety applications, or to support the needed establishment of a V2V communications security system. Leaving the pace of that development to the market will, we believe, delay the life-saving benefits of those safety applications because the effectiveness of applications depends on receiving messages from all other vehicles. Second, if fewer vehicles are equipped with V2V, there may be less incentive for industry to develop a sufficient security system, which will feed into concerns from consumers regarding perceived potential privacy and cybersecurity issues. Taken together, the delayed effectiveness of the safety applications plus potentially increased concerns about security may lead manufacturers not to include V2V capability in a significant amount of vehicles at all. For these reasons, NHTSA proposes to require new light vehicles to be V2V-capable.

NHTSA and, we believe other stakeholders, will be working to educate consumers about V2V, and will ensure that the V2V system is designed to minimize security risks and protect privacy appropriately. We believe consumer education will alleviate fear of the unknown as V2V enters the vehicle fleet. Findings from our consumer research between the ANPRM and this NPRM are discussed below in Section IV, and NHTSA will be considering these issues carefully as we move forward.

While we are proposing a V2V communications mandate, we also seek further comment on the costs and benefits of an "if-equipped" option, particularly considering the substantial monetary and potential social costs of a mandate. Do commenters believe an if-equipped option would be a preferable approach, and if so, why? What costs and/or benefits should we consider relative to an if-equipped approach, and how do those costs and benefits compare to our analysis of the costs and benefits of a mandate? For instance, we seek additional comment on how an if-equipped option may potentially delay or lead to uncertainty in V2V technology development.

In addition, what benefits may accrue from a more gradual, market-based approach to a technology that has never before been widely deployed? What affect would such an approach have on the ability to iterate and test potential V2V technology solutions, including issues related to costs, reliability, security, and deployment? How would an if-equipped approach affect consumer choice and privacy protections? We also seek examples and information related to the success and failure of other network-reliant technologies, including those that evolved in the absence of a government mandate and those that were mandated and whether the example is applicable or not to a safety sensitive function.

C. V2V Communication Devices that would be subject to FMVSS No. 150

1. Original Equipment (OE) Devices on New Motor Vehicles

NHTSA's research thus far indicates that V2V communications technology is feasible for new light vehicles. The Safety Pilot Model Deployment demonstrated that interoperability is possible and directly informed the requirements in this proposed FMVSS and also in SAE standards such as J2735 and J2945. The agency is confident that V2V devices integrated into light vehicles consistent with these requirements will provide the technical foundation for national deployment of DSRC-based crash avoidance capability.

2. Aftermarket Devices

Many consumers may not be ready to purchase a new vehicle, but may be interested in having V2V capabilities in their current vehicles. NHTSA believes that it is likely that aftermarket products may be developed in response to consumer interest in V2V, and we strongly support the innovation and accessibility that aftermarket devices could foster, all potentially leading to expanded and earlier benefits from V2V communication technology. As the name suggests, "aftermarket" refers to products that the vehicle owner purchases and adds to his or her vehicle after the vehicle's manufacture. Aftermarket products are distinguished from

"original equipment," which is installed on the vehicle during its manufacture, prior to initial purchase. Allowing aftermarket products to participate in the V2V system will enable the technology to spread faster than if introduced through new vehicles only—thus accelerating safety benefits.

As part of setting standards for aftermarket V2V devices, however, NHTSA recognizes that some aftermarket products may not be able to populate optional BSM data elements if they do not have access to the CAN bus. Aftermarket devices will therefore need to use other methods to populate elements needed to calculate vehicle position in order to support crash avoidance warnings. Some data elements, such as turn signal indication, will not be able to be derived from other methods. As a result, the inability of some aftermarket devices to populate certain optional BSM data elements may impact the fidelity (ability to balance the level of false positive warnings) of safety applications that the aftermarket device supports. In the Safety Pilot Model Deployment, there were three separate types of "aftermarket" devices – some that were fully integrated into the vehicle just like original equipment; some that were connected to the vehicle for power, but did not have access to the vehicle's data bus; and some that also only connected for power, and could only transmit BSMs but could not receive them and could not deliver crash avoidance warnings. Based on the information we currently have before us, we think it is reasonable to assume that these three types of aftermarket devices could be available in the rulemaking timeframe.

For example, OEMs may choose to offer their own aftermarket V2V devices that can be retrofitted onto earlier vehicle models (retrofit means the devices can interface with the vehicle data bus), made by that OEM, at one of their retailers. For another example, V2V devices, which are not unlike today's dedicated aftermarket navigation systems (e.g., a Garmin or TomTom), could potentially be developed for drivers to purchase and have installed. The agency also foresees the potential for some form of a multi-use device containing a V2V-related application ("app") that could be brought into a vehicle ("carry-in") by a driver. A carry-in device could have the capacity to simply send a BSM without providing any warnings to the driver or potentially provide more capabilities in a potential V2V, or V2I, system. Moreover, in the future, there could be yet other types of aftermarket devices that have V2V capabilities not yet envisioned by NHTSA.

NHTSA does not wish to limit the development of different types of aftermarket devices, but we do seek to ensure that all devices participating in the system perform at a minimum or better performance level for V2V communication. This is important because, in order to ensure safe and secure crash avoidance benefits, all BSMs transmitted need to perform at a minimum performance level such that safety applications can identify imminent crash situations and issue warnings to the driver to avoid a crash. Therefore, the minimum performance requirements need to be the same for all devices with provisions that accommodates the optional data elements that can be used to perform better than the minimum.

The proposed requirements for any V2V devices recognize that, as DOT discovered in the Safety Pilot Model Deployment, installation can significantly impact how devices perform. The agency believes there is high probability that a certified device installer could complete the

installation for aftermarket safety devices. It is imperative that all V2V components be properly installed to ensure that an aftermarket device functions as intended. Whereas some vehicle owners may choose to replace their own brakes or install other components on their vehicles themselves, installation requirements for aftermarket V2V devices may not be conducive to a do-it-yourself approach. Improper installation of a GPS antenna has the potential to affect the proper population of BSM data elements. Faulty position data from a transmitting vehicle can result in false warnings, improperly timed warnings, etc. Moreover, an improperly installed aftermarket device may put all other V2V-equipped vehicles it encounters at risk until the given vehicle stops communicating, or until its messages are rejected for misbehavior.

The agency seeks comment on the potential need for certification of aftermarket V2V device installations. If so, please provide any potential recommendations of appropriate retail outlets, the certification mechanisms, and authorizers (vehicle manufacturers, device manufacturers, device retailers, others) that should be employed. Conversely, do commenters believe that future available technology may allow consumers to self-install V2V devices such as web-based tools, or other potential methods, that could verify accuracy of an installation? Research supporting this possibility would be very helpful.

D. Potential Future Actions

1. Potential Future Safety Application Mandate

NHTSA has concluded that V2V communication technology combined with V2V-based safety applications can provide significant safety benefits and potentially help drivers avoid thousands of crashes per year. We believe that by leading with a mandate for V2V communication technology, NHTSA will be able to foster industry development and deployment of new, beneficial safety applications. As previously discussed in the V2V Readiness Report and in the above discussion concerning the safety need, there are a number of these applications that the agency believes could be ready to be deployed soon after a V2V mandate is in effect. In particular, the agency has highlighted two specific applications, IMA and LTA.

The agency focused on these potential safety applications because prototypes of these applications were used during Safety Pilot Model Deployment, because we have sufficient data, and because they can be effectively enabled only by V2V. IMA warns drivers of vehicles approaching from a lateral direction at an intersection, while LTA warns drivers of vehicles approaching from the opposite direction when attempting a left turn at an intersection.

As discussed in the V2V Readiness Report, the agency has and will continue to investigate other potential V2V safety applications that could be enabled by V2V communications.[115] Depending on the market penetration of applications in response to this proposed mandate of the foundational V2V capability, the agency may later decide to mandate

[115] Six potential applications were mentioned in particular: IMA, FCW, DNPW, EEBL, BSW/LCW, and LTA.

some or all of the potential applications discussed in the Readiness Report, and perhaps future applications yet to be developed. If mandated in the future, applications would likely be incorporated into NHTSA's regulations as FMVSSs, and in the interests of clarity, each application mandate would likely be contained in its own FMVSS.

At this time, though, the agency does not have sufficient information to include with this NPRM proposed test procedures or performance standards for LTA and IMA or any other safety applications. To that end, we request comment on any additional information or research on IMA, LTA and any other applications that could inform and support an agency decision regarding whether to mandate safety applications with or shortly after a final rule requiring DSRC.

2. Continued Technology Monitoring

NHTSA's proposal to mandate V2V communications capability for new light vehicles is based upon the best currently-available scientific data and information. Consistent with its obligations under Executive Order (E.O.) 13563, Improving Regulation and Regulatory Review (Jan. 18, 2011), and E.O. 13610 on the retrospective review of regulations, NHTSA will review relevant new evidence and may propose revisions to a subsequent proposed or final rule as necessary and appropriate to reflect the current state of the evidence to provide an effective regulatory program. In obtaining that new evidence, NHTSA may consider collections of information that may trigger the Paperwork Reduction Act, and would notify the public of these collections through the separate Federal Register Notices required under that Act. NHTSA may also identify and pursue additional issues for new research or conduct further research with regards to existing issues addressed in this proposed rule. Such modifications may be necessary in the future to accommodate new systems and technology designs, and the agency would consider these modifications in consultation with the public through the notice and comment rulemaking process. We acknowledge that the research relevant for evaluating a new technology would vary depending on the type of technology considered.

E. Performance Criteria for Wireless V2V Communication

In order to ensure that vehicles broadcast basic safety messages to support potential safety applications, the agency is proposing performance requirements for DSRC-based V2V communications. As part of this, the agency is also requesting comment on alternative interoperable technology provisions that would allow other technologies to satisfy the mandate, as long as they meet performance and interoperability requirements, which are based on the capabilities of today's DSRC-based V2V communications.

The agency is proposing to require that V2V devices be capable of broadcasting V2V messages in an interoperable manner, i.e., that devices can both transmit and receive BSMs using V2V communications from all other vehicles equipped with a V2V communications technology. We believe that the requirements described below will ensure interoperability. We aim to ensure a uniform method for sending basic safety information about the vehicle. In this way, any

vehicle seeking to utilize the V2V information environment to deliver safety benefits would have a known and uniform method for doing so.

In order to create this uniform method, an FMVSS would need to contain requirements in a few areas. First, it would need to establish the content of the information to be sent to the surrounding vehicles (by not only specifying the type of information to send, but also the measuring unit for each information element and the level of precision needed). Second, the FMVSS would need to specify requirements for the wireless transmission of the content (i.e., how far, how often, etc.). Third, we may need to specify a standard approach to authenticate V2V messages that are received to improve confidence in message contents.

In addition to those three points, the FMVSS would also need to specify other aspects of performance for a V2V-communications system in order to support full-scale deployment and enable full functionality including security. The agency recognizes that some capabilities are not necessarily needed to support operations during the first few years of deployment, but would be required as the V2V vehicle fleet grows.

First, the devices regardless of the communication technology used would need a uniform method for dealing with possible occurrences of high volumes of messages(e.g.., potentially reducing the frequency or range of messages in high congestion situations. Second, to help identify and reduce the occurance of misconfigured or malicious devices transmitting BSM messages, the FMVSS may need to specify methods for identifying misbehaving devices. Finally, to support the above functions, vehicles in the V2V environment may need a methods for communicating with security infrastructure such as a SCMS (e.g., in order to obtain new security certificates or report misbehaving devices, and receive information about misbehaving devices).

In short, an FMVSS would explain: (1) what information needs to be sent to the surrounding vehicles; (2) how the vehicle needs to send that information; (3) how a vehicle validates and assigns confidence in the information; and (4) how a vehicle makes sure the prior three functions work in various operational conditions (i.e., broadcast under congested conditions, manage misbehavior, and update security materials). A variety of voluntary standards cover many of these aspects of performance. Our proposal below draws from these voluntary standards but also explains why a particular threshold or requirements from a voluntary standard is appropriate. Finally, we are proposing a test method for evaluating many of these aspects of performance. Having a clear test method helps inform the public as to how the agency would evaluate compliance with any final FMVSS.

Finally, we acknowledge that research is ongoing in a few of the areas we discuss in this section. While research continues in these areas, we have described for the public the potential requirements that we are considering, and the potential test methods for evaluating compliance with those requirements. We believe that the public comments that we will receive in response (coupled with the agency's ongoing research) will produce a robust record upon which the agency can make a final decision.

1. Proposed Transmission Requirements

Our purpose for proposing a standardized set of transmission requirements is in line with our vision for V2V as an information environment that safety applications can use. By creating a standardized method for transmitting the basic safety message, we are creating the information environment with one clear method for accessing it. Our current belief is that anyone who wants to implement safety applications should know how their system can obtain the V2V information as an input for their application.

In order to have a standardized method for transmitting the basic safety message we believe that a few aspects of performance need requirements. We tentatively believe that all devices should be required to transmit:

- with a sufficient power/range to guarantee reaching other DSRC devices, within a minimum radius, that would allow use of the basic safety message information reliably;
- on the same channel, and support using the same data rate(s); and
- at the times required for each data element so that people who have applications know when it will have information.

a) DSRC Transmission Range and Reliability

In order to ensure that surrounding vehicles within a certain range of each vehicle transmitting basic safety messages can reliability receive the messages, The proposal includes requirements for the transmission range of the messages. While the research to date has included various specifications for the antenna (e.g., power, polarization, location on the vehicle, etc.), we tentatively believe it more appropriate to measure the ability of the vehicle to transmit the packet to a specified device at a specified distance. In other words this transmission range and reliability requirement employs a more performance-oriented approach where our FMVSS would not specify requirements for the antenna itself.

By specifying the requirements in this fashion, we not only set requirements that can more closely follow real-world conditions, but also leave aspects of design open to manufacturer choice (e.g., antenna location on the vehicle). Our method here would simply seek to ensure that the transmission of the basic safety message travels the required distance and is readable by another DSRC device at that range (regardless of how the antenna is configured). Thus, we seek comment on our proposal. We currently believe that specifying the following three areas would be appropriate:

- the three-dimensional (latitudinal, longitudinal and elevation) minimum range that the basic safety message transmission would need to reach;
- a test device (and its specifications, e.g., its receive sensitivity) for testing the range and the locations to measure reception of the basic safety message; and

- the reliability of the reception of the basic safety message (i.e., how often is the message dropped) based on packet error rate (PER).

In addition, our current belief is that the agency would not need to establish specifications for the transmitting device itself. In other words, we request comment on our current belief that the following design-level requirements would not be necessary for an FMVSS:

- transmission power;
- antenna polarization; and
- antenna placement.

(1) Range

A basic safety message needs to travel far enough to support potential safety applications that we anticipate would take advantage of the information available through DSRC communications. Aside from the basic "open air" communication scenarios, it is important to also consider whether devices will be able to communicate with others that are on the same road but, perhaps, not at the same elevation or approach angles (i.e., the road elevation may change).

(a) Longitudinal/Lateral Range

Our strategy we considered regarding what minimum range requirement we should include for transmitting the basic safety message was to balance:

- the information needs for potential safety applications; and
- technical capabilities demonstrated.

In terms of information needs for the safety applications, our research to date used a minimum 300 m transmission range— while recognizing this range would diminish in urban and non "open air" environments. The applications tested in the Safety Pilot Model Deployment assumed vehicles were transmitting basic safety messages at the 300 m range. In particular, we believe that DNPW requires the longest communication range for effective operation because it addresses a crash scenario where two vehicles approach each other head-on. Using the target range of 300 m, two vehicles approaching at 60 mph would be afforded approximately 5.6 seconds for the DNPW application to detect the crash scenario and issue a warning. Based on this information, our current belief is that 300 m will serve the needs of the anticipated safety applications.

Based on the existing research, our proposal is to adopt 300 m as the minimum transmission range. We believe that this supports the needs of anticipated safety applications and can be operationally met given current technological capabilities; as demonstrated in Safety Pilot Model Deployment. Currently, we also do not anticipate any safety application requiring more range than 300 m. Thus, we tentatively do not see a reason to increase the minimum transmission range beyond 300 m.

Finally, we have not included a maximum range limit. Maximum transmission range can vary by the power of the transmission, and environmental conditions. While our current proposed requirements do not include establishing a maximum transmission range, we request comment on whether such a limit would be appropriate in conjunction with the other requirements the agency is considering.

We ask for comment on this proposed minimum. Is there any reason that the agency should require a maximum transmission range as well as a minimum? Should the agency choose a different minimum range requirement? What would be appropriate alternative minimum and maximum transmission range values and why? Please provide data to support your position.

(b) Elevation Transmission Performance

In addition to the 2-dimension range of the basic safety message transmission, we need to consider the potential changes in elevation on roadways. Thus, in addition to establishing a minimum distance that the basic safety message needs to travel, we also need to establish an elevation angle that the message needs to travel.

Safety applications may need information from vehicles at a higher elevation (because of changes in the slope of the roadway, for example). Thus, our current belief is that a proposal to regulate DSRC radio performance should also evaluate whether a vehicle transmitting the basic safety message can transmit said message at an angle that is sufficient to cover potential roadway elevation changes.

Our proposal would require that vehicles transmit the basic safety message not only to 300 m around a vehicle (in all directions—i.e., 360 degrees) but also at an elevation angle of +10 degrees and -6 degrees. We think that the elevation angle range of + 10 to -6 degrees 360 degrees around the vehicle is an appropriate range to ensure that the broadcast of the BSM can be received by vehicles in a 300m radius given most roadway characteristics such as changes in roadway grade was what was used to demonstrate capability in Safety Pilot Model Deployment. The agency is continuing to research a larger range of elevation angle (+/- 10 degrees) to determine actual transmission coverage range. In particular, if the range would be adequate to support transmission and reception of BSMs on roadway grades up to 15 degrees, which is the current design maximum for many States and localities (excluding San Francisco). However, currently it is not practicable to test the +/- 10 degree elevation angle range given current testing equipment.

We ask for comment on this proposed minimum. Should the agency choose a different minimum elevation angle requirement? What would be appropriate alternative minimum elevation angle range values and why? Please provide data to support your position.

(2) Testing the Elevation Transmission Range

In order to give context to our proposed requirement, we are also describing the method the agency would use in assessing the elevation angle range performance requirement (i.e., the

test procedure and type of test device). As discussed later in this document, the agency would test these requirements using test devices located within a specified area around the vehicle in a static test to determine whether the vehicle's basic safety message transmissions can reach the required range. In order to conduct this test, we need to define two pieces of information:

- the important characteristics of the test device for the purposes of evaluating this requirement; and
- the area around the vehicle where we can place this test device.

(a) Test Device

As further discussed in the test procedure section of this document, we anticipate that our test method would specify various aspects of the test device for the purposes of evaluating a vehicle's DSRC radio performance. However, for the purpose of evaluating this aspect (i.e., the transmission range) of DSRC radio performance, we believe the receive sensitivity of the test device is the characteristic that would need to be most clearly defined in order to test the transmission range objectively.

Based on the currently-available research, the agency would measure this using a test device with a sensitivity of -92 dBm. We believe that -92 dBm is an appropriate sensitivity for the test device receiving the basic safety message during the test because -92 dBm generally models what average devices (e.g., cell phones) use for their antenna sensitivity. We believe that it is a reasonable assumption that a vehicle seeking to obtain basic safety messages for its safety applications would be designed with, at minimum, this level of sensitivity.

Further, our understanding is that -92 dBm falls on the less-sensitive side of the range of an average wireless device's antenna sensitivity. We believe that using a less sensitive device within that range is appropriate in this instance because it means we are using a more stringent test condition that is still within the range of an average device antenna's sensitivity.

(b) Location of the Test Device

In addition to specifying the device, we also believe it is important to specify the location of the device relative to the vehicle being tested. We are proposing to define a zone around the vehicle where a test device is used to evaluate the ability of the vehicle to receive the basic safety message. Currently, the proposed zone is defined as 300 m 2-dimensional range with an elevation angle that can be set at +10 degree and -6 degrees.

For testing the 2-dimensional (longitudinal and lateral) range, the agency would specify an area within a circle around the vehicle that we may test. The test circle has the following characteristics:

- It is 1.5 m above the test surface.
- It is parallel to the test surface.
- It has a center point that is 1.5 m above the vehicle reference point.[116]
- The circumference of the circle is any point at a 300 m radius from its center point.

In other words, when conducting the compliance test, the agency test engineer may place the test device at any point that is 1.5 m above the ground and within the area of a circle whose center point is 1.5 m above the vehicle reference point and whose radius is 300 m.

For testing the elevation range of the vehicle's transmission, we tentatively believe it is preferable to use two slightly different evaluation methods for the upward elevation versus the downward range. For the upward elevation range, our proposal is that the test engineer may place the test device at any point along the following line:

- The line originates at a point that is 1.5 m above the vehicle reference point.
- The line rises at a +10 degree angle from the test surface[117] proceeding in any direction around the vehicle.[118]
- The line terminates at any point that is directly above the circumference of the circle used in the 2-dimentional range test.

On the other hand, for testing downward elevation range, the agency would place the test device at any point along the following line:

- The line originates at a point that is 1.5 m above the vehicle reference point.
- The line falls at a -6 degree angle from the test surface[119] proceeding in any direction around the vehicle.[120]
- The line terminates at any point where it intersects the test surface.

Test the downward elevation at a point that is likely closer to the vehicle than the upward elevation, we believe that this method would relieve some test complexities while still ensuring that the transmissions will reach surrounding vehicles under real-world roadway elevation changes. Further, we believe that the locations defined above (longitudinal, lateral, and

---

[116] Vehicle reference point is the same point that we defined in the basic safety message content requirements section, above.
[117] Note the line originates at a point that is 1.5 m above the test reference point, but (for simplicity) we are expressing the angle of the line by referencing the test surface (i.e., the ground, which is not where the line begins). The angle of the line could be expressed by referencing any plane that is parallel to the test surface.
[118] In other words, the line can travel in any direction (360 degrees) around the point 1.5 m above the vehicle reference point.
[119] *See* similar note, above.
[120] *See* similar note, above.

elevation) establish the limits of the potential test conditions in a way that would still enable the agency to measure at the extremities of the proposed range requirement.

As noted above, testing the elevation range would enable NHTSA to test for compliance at any point along those aforementioned lines. While we believe that -92 dBm is an appropriate sensitivity for our test device when it is located 300 m away from the tested vehicle, we request comment on whether the test device should still have a sensitivity of -92 dBm if NHTSA tests the vehicle performance closer to the vehicle along the aforementioned elevation testing lines. What would the appropriate function be to determine the sensitivity based on the test device's location along those testing lines?

We further request comment not only on the test method but also on whether there are other aspects of the test that the agency would need to define in order to clearly evaluate this aspect of performance.

(3) Reliability

The agency is proposing to require that a message packet error rate (PER) is less than 10%. We believe that 10% PER is an appropriate threshold and that vehicles will still be able to receive the basic safety messages so long as the PER is below 10%. The agency believes the PER metric at the proposed rate fulfills the need to evaluate how *reliably* a V2V device can transmit a message for a specified distance.

The Packet Error Rate (PER) is one way of quantifying how reliably a message can travel a given distance. In essence, it measures how often (i.e., the percentage of) parts of the message (i.e., packets) fail to make it to the destination. The research for V2V safety applications to date assumes that vehicles are transmitting the basic safety message to a range of at least 300 m around the vehicle with a PER of less than 10%.

A PER of less than 10% aligns with the ASTM standard E2213-03 (2003) 4.1.1.2 where "*(2)* DSRC devices must be capable of transferring messages to and from vehicles at speeds of 85 mph with a Packet Error Rate (PER) of less than 10 % for PSDU lengths of 1000 bytes and to and from vehicles at speeds of 120 mph with a PER of less than 10 % for PSDU lengths of 64 bytes." As such, the agency believes this specification, along with the agency's successful Safety Pilot Model Deployment work, makes it appropriate to include this as part of the performance requirements for DSRC devices. Overall, the agency did not observe any dropped basic safety messages (i.e., message did not reach a vehicle within range) due to a high PER, and we believe that the 10% PER threshold will continue to be appropriate in a more full-scale deployment. We request comment on our tentative conclusions and also request comment on what other potential PER thresholds would be more appropriate (and why).

(4) Aspects of Transmission Range Performance Indirectly Tested

We currently believe that testing the range (both 2-dimensional and elevation) and the reliability (PER) of the transmission with a specified test device (-92 dBm) in specified locations is sufficient to determine whether a vehicle would be able to deliver basic safety messages to vehicles around it in the real world (i.e., it would be sufficient for supporting the safety applications currently under active development). However, we recognize that there are a few aspects of performance covered by the V2V research to date that we have not included in this proposal. Our tentative conclusion is that the proposed requirements would cover these aspects of performance indirectly. Further, we believe that Proposal A would avoid unnecessarily restricting manufacturer design choices while still ensuring that the vehicle achieve the safety purpose of transmitting the basic safety message. These aspects of performance are:

- antenna location on the vehicle;
- antenna polarization; and
- transmit power.

(a) Antenna Location on the Vehicle

The agency and its research partners utilized antenna location mounting requirements on vehicles used in the Safety Pilot Model Deployment activity. However, our tentative conclusion is that it is unnecessary to specify requirements for antenna location. The location of the antenna on a vehicle can affect the ability of the vehicle to transmit the basic safety message to all the necessary locations around the vehicle. However, we believe that testing for reception of the basic safety message at the aforementioned locations around the vehicle would clearly show whether the location of the vehicle antenna is installed at an appropriate location where the vehicle structure would not interfere with the transmission of the basic safety message.

If the antenna location is appropriate enough to transmit the basic safety message to meet the needs of the safety applications, we tentatively see no need to further restrict the location of the antenna on the vehicle (as it is also an important styling decision for the auto manufacturer). However, we request comment on this tentative conclusion. Are there any reasons why the agency should establish requirements for the antenna location on the vehicle? What would these restrictions be? How can they be objectively defined on the vehicle? What data supports your conclusions?

(b) Antenna Polarization

We also tentatively believe that the agency does not need to establish performance requirements for the transmitting antenna's polarization. We are aware that the research to date generally recommended a nominal vertical polarization configuration for the DSRC antennas sending the basic safety message. The research recommended that configuration because vehicle

sheet metal can serve as the ground plane and can degrade reception of horizontally polarized waves at or near the horizon.

While we agree that using a non-optimal antenna polarization would lead to increased cost and complexity of the system (i.e., requiring more antennas in order to reach the same transmission coverage), we tentatively do not believe it is necessary to propose limiting such a design. We believe that, for cost considerations, manufacturers are likely to select an antenna polarization that would enable them to achieve the same performance with less antennas. However, so long as the vehicle can transmit the basic safety message to the required range under the conditions specified, we currently see no reason to preclude other antenna polarizations. We also request comment on this tentative conclusion.

(c) Transmit Power

Finally, the requirements and test method also do not directly test for the transmit power. Our current belief is that our test method sufficiently covers this aspect of performance by establishing the range at which the vehicle needs to transmit the basic safety message and the receive sensitivity of the test device. We note that the research to date has recommended various transmission power levels. For example, the SAE J2945/1 standard recommended a minimum radiated power of 15 dBm (under uncongested condtions). However, we believe that our aforementioned requirements would sufficiently test for this aspect of performance. In essence, by testing whether a device with a sensitivity of -92 dBm can receive messages from a vehicle 300 m away, we are testing whether the transmitting vehicle is doing so with sufficient power to deliver the basic safety message to the required distance.

We currently do not believe it is necessary to further specify the transmit power for vehicles covered by the proposal. Based on the manufacturer's choices regarding antenna location on the vehicle (and potentially other factors such as the body of the vehicle, etc.), a manufacturer may need to make different transmit power choices in order to transmit the message to the required distance. As with antenna location and polarization, we believe that the transmission power is sufficiently addressed (albeit indirectly) by the requirements. We believe that the requirements would establish an appropriate balance between affording the manufacturers design freedom, while still ensuring that they achieve the safety goal of transmitting the basic safety message far enough and reliably enough to support the safety applications. We seek comment on whether there is any reason for the agency to establish a requirement for the transmit power. What should the transmission power be and why?

(5) FCC Transmission Power Restrictions

The agency's proposal is not not specifying required transmission power levels for V2V devices. The FCC places restrictions on the transmission power levels of devices utilizing a given spectrum and our expectation is that DSRC devices operating in the designated bandwidth would meet the FCC defined operating specifications. However, we do not believe that our current proposal (i.e., our proposed minimum transmission range and the sensitivity of the test device) would require vehicles to transmit at a power that exceeds FCC regulations.

FCC Part 95L specifies a max EIRP limit of 33dBm for Private OBUs on channels 172, 174, 176, 178, and 184. Our understanding is that devices would be able to meet the these requirements at a power setting lower than the restricted level (Safety Pilot Model Deployment devices were set at a 20 dBm power level).

b) Channel and Data Rate

In addition to proposing requirements for the transmission range and reliability, we believe it is also important for DSRC-based V2V communications to utilize the same channel and data rate. The channel is a band of frequencies where the transmission occurs. Parties agreeing to use the same channel to communicate are like people that agree to call each other using a particular phone line. The data rate is the speed at which a sender is transmitting information through the channel.

The Federal Communications Commission (FCC) has statutory authority for allocating spectrum rights and designating band plans for commercial spectrum allocations, including the 5.9 GHz band. DOT defers to the FCC's authority with respect to spectrum rights and channel plans. Based on FCC rules and research to-date, all devices participating in the V2V information environment have utilized the same channel and data rate to transmit BSMs. In relation to DSRC, FCC has specified that BSM transmissions and reception will occur on channel 172, i.e. channel 172 will be dedicated to all BSM communications (safety-critical communications). Therefore, throughout this document, references to BSM transmissions and reception will refer to channel 172 while also recognizing the ongoing DOT-FCC-NTIA spectrum sharing studies and the FCC rulemaking concerning the 5.9GHz band as described in more detail below. Similar to our approach to transmission power, the agency believes that all BSM transmissions should occur on channel 172. Data rate is also important because a receiving device needs to know the speed at which the transmitting device is sending the information in order to process the information. Thus, in order to ensure interoperability of the devices in the V2V information environment, our current belief is that it is necessary to establish requirements for both the channel and the data rate.

As we discuss below, there are various options for both the channel and the data rate—each with advantages and disadvantages. While there are different choices available, each choice should be able to achieve the objective of ensuring interoperability across devices if it is implemented consistently by all devices. Thus, we are proposing to that all vehicles should transmit the basic safety message on Channel 172,via a dedicated radio at a data rate of 6 Mbps). We also request comment on whether there are other choices for these two aspects of performance that the agency should consider.

(a) Channel

(i) Proposed Channel Usage

The FCC currently divides the 5.9 GHz spectrum into seven, ten- megahertz channels consisting of one Control Channel (Channel 178); six Service Channels (Channel 172 for safety-

critical communications and Channels 174, 176, 180, 182, and 184 for non-safety-critical communications); and one five megahertz channel, which would be held in reserve. The FCC also allows combining Channels 174 and 176 or Channels 180 and 182 to produce two twenty-megahertz channels, (which would be Channel 175 and 181, respectively).

As we discussed in the sections above, we believe that devices participating in the V2V information environment need exchange messages on the same channel in order to receive each other's broadcasts (i.e., to hear the messages that others send). Up until now, the V2V devices transmitting basic safety messages in the V2V research have used Channel 172 (a 10 MHz channel). The research used a 10 MHz channel as the FCC's current rules for the V2V spectrum divide it into various 10 MHz channels.

Our tentative conclusion is that broadcasting on Channel 172 via continuous mode (radio set to channel 172, a 10 MHz band) is appropriate for devices in the V2V information environment. Thus, we believe that all vehicles should transmit their basic safety messages on the same channel (172). Our tentative conclusion is based on our understanding of the existing research and in alignment with the FCC spectrum allocation. The agency expects that all non-safety-critical communications will occur on the remaining channels allocated for DSRC use by the FCC. The research suggests that a 10 MHz band is sufficient for transmitting the basic safety message to the necessary 300 m range at a sufficient level of reliability PER of less than or equal to 10%.

We seek comment on all related issues we should take into account when considering this proposal, as well as any other potential alternatives.

(ii) Potential Channel Sharing or Re-channelization

NHTSA and the U.S. DOT are committed to finding the best method to develop, successfully test, and deploy advanced automotive and infrastructure safety systems while working to meet existing and future spectrum demands. DOT supports sharing so long as it does not interfere with safety of life communications. In the summer of 2015, recognizing the emerging need to perform further research on DSRC properties in order to prepare for studies on sharing, DOT worked collaboratively with the FCC and NTIA to develop a spectrum research plan. This plan (the "DSRC-Unlicensed Device Test Plan") is posted on DOT's website and details a comprehensive set of research opportunities. The plan will allow FCC, NTIA, and DOT to collectively tailor research on DSRC devices in the presence of unlicensed devices to understand the prospective impacts within real-world environments.[121] The overall goals and objectives of this research are as follows:

- Overall Goals as listed in the DSRC-Unlicensed Device Test Plan
  1. Understand the impacts of unlicensed devices operating in the DSRC band.
  2. Develop the capability to evaluate proposed band sharing mechanisms.
  3. Define requirements necessary for sharing mechanisms to prevent interference.
  4. Collaborate with the NTIA and FCC to provide Congress with results on impacts to DSRC operations from proposed sharing mechanisms.

- Specific Objectives and Goals as listed in the DSRC-Unlicensed Device Test Plan

  1. Develop the capability to do accurate and relevant experimental evaluations of band sharing and interference between unlicensed devices and DSRC devices.
  2. Characterize the existing radio frequency (RF) signal environment in and near the DSRC band.
  3. Measure the effect of unlicensed devices on the background noise level.
  4. Measure the impact unlicensed device transmissions have on receiving DSRC messages.
  5. Measure DSRC suppression caused by Clear Channel Assessment (CCA) of DSRC devices in the presence of unlicensed device transmissions.
  6. Measure other impacts on DSRC channel quality of unlicensed device transmissions (e.g., signal to noise (S/N), packet error rate (PER), etc.).
  7. Determine the minimum received power levels at which DSRC and unlicensed devices can sense the other.
  8. Investigate how interference and detection (determined in the previous objectives) varies if the bandwidth of the overlapping unlicensed device transmission changes.
  9. Measure the impact of DSRC operations on unlicensed device performance recognizing that the two radios may form an interactive system.
  10. Investigate mitigation possibilities once potential U-NII-4 devices designed and programmed to share the band with DSRC are available.

This DOT testing effort is part of a larger collaborative testing and modelling effort with the FCC and DOC, encouraged by Congress, to ensure appropriate interference-avoidance and spectrum rights allocation in the 5850-5925 MHz (5.9 GHz) band. Congress called upon DOT to lead, in close coordination with FCC and DOC, the development of 5.9 GHz Dedicated Short Range Communications (DSRC) technology, vehicle safety testing, and DSRC capabilities testing. Furthermore, Congress called upon NTIA to study the possibility of allowing unlicensed operations in the 5.9 GHz band. The U.S. Department of Transportation (DOT), the U.S. Department of Commerce (DOC), and the Federal Communications Commission (FCC) each have core, yet interdependent, roles to play in advancing this research.

Recently, the FCC issued a Public Notice to refresh its record regarding its draft proposal to allow sharing of the 5.9 GHz band by U-NII devices.[122] As part of its Public Notice, the FCC has solicited comments on the two proposed sharing techniques developed by the IEEE DSRC Coexistence Tiger Team (i.e., "Detect and Avoid" and "Re-Channelization"), as well as on other potentially viable approaches to sharing in the band without causing harmful interference to V2V operations.

The FCC described the two proposed sharing approaches as follows: 1) Detect and avoid, under which unlicensed devices would monitor the existing DSRC channels, and if they detected any transmitted DSRC signal, they would avoid using the entire DSRC band. After waiting a certain amount of time the unlicensed device would again sense the DSRC spectrum to determine if any DSRC channels are in use or whether it could safely transmit; and 2) Re-Channelization, under which the DSRC spectrum would be split into two contiguous blocks: one for safety-related communications and one for non-safety-related communications, by moving the control channel and the two public safety channels to the top portion of the band. Additionally, the remaining four DSRC service channels would be reconfigured at the lower end of the band as two 20 megahertz channels rather than maintaining four 10 megahertz channels. The segments designated for safety-related communications would remain exclusive to DSRC, and the remaining spectrum would be shared between the DSRC service channels and unlicensed devices.

We seek comment on the costs and benefits of each sharing proposal, and whether and how we should consider each of these approaches relative to this proposed rule.

(b) Data Rate

In setting a data rate, one is balancing between two competing interests: (1) the speed at which one wants to transmit the information, and (2) how far the information can travel (and how reliably it can travel that distance). In other words, if we send more information in a smaller amount of time, the information cannot reliably travel as great of a distance.

In the context of our rulemaking, our proposal for data rate considers the following technical questions:

- How far do we need the message to travel?
- What is an acceptable PER (i.e., how reliably do packets need to make it to a receiving device in order to ensure that a safety application can function)?
- What bitrate do current systems and voluntary standards under development use? If a final rule used a different set of requirements, how significant would this change be?

---

[122] https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-68A1_Rcd.pdf

In the sections that follow, we first discuss the competing considerations for our data rate proposal. Using the information that we have from our discussion on data rate, we then discuss our proposal for the channel.

(i) Proposed Requirement is 6 Mbps

The agency is proposing to require devices to transmit at 6 Mbps. We believe it is reasonable to expect that transmitting basic safety messages at the 6 Mbps rate can easily cover the necessary range assuming 300 m at a very low PER of 10%. The available research from both CAMP and BAH support this initial conclusion, as described later in this section. Further, while we are requesting comment on changing the bitrate, we note that the current systems and voluntary standards under development all will be able to support multiple bitrates within the ranges examined (i.e., device developers would not need to redesign the current hardware to support a new bitrate).

Finally, while the theoretical analysis by BAH suggests that increasing the bitrate would help to mitigate congestion mitigation, we are unsure given the lack of real-world testing whether altering the bitrate and channel bandwidth is necessary given that the agency is considering other channel congestion mitigation strategies. These strategies involve adjusting the number of basic safety messages that devices would transmit per second and the power/range of those transmission when channel congestion is detected by a device. More detail on these strategies is found in Section III.E.1.b)(b)(ii). The agency is continuing to refine congestion mitigation approaches including device density in real-world conditions, beyond those tested in the specific Safety Pilot testing and Safety Pilot Model Deployment.

We request comment on our potential approaches to conclusions and our questions above. To support the commenting process, we are also presenting alternative choices for bitrate in the section that follows and we seek comment on those alternatives.

(ii) Alternatives for Data Rate Requirements

The BAH research suggested alternate bitrate possibilities that would change based on the level of congestion on the channel. Their rationale behind this approach is that, when the channel is not busy, the transmitting device should use a lower bitrate that can more reliably send the message. However, when the channel congestion is detected, the device should use a higher bitrate to send the message quicker and vacate the channel as soon as possible. This is a logical strategy because when a vehicle is in a congested environment (e.g., a traffic jam[123]); the vehicle does not need to transmit the message as far because the relevant cars are the ones that are fairly close by. In other words, in this scenario, it is important to transit the message fast (not far).

---

[123] In relation to communications congestions the use of the term "traffic jam" refers to the analysis presented via the ANPRM that identified a major interchange that includes overpasses as an extreme scenario with the possibility of approximately 800 V2V vehicles transmitting BSMs in the range of one V2V vehicle.

Based on this logic, BAH recommended in its research that devices transmit in the following manner:

- when the Channel Busy Ratio[124] is below 50%, transmit the BSM at a data rate of 9 Mbps;
- when the channel busy ratio exceeds 50%, transmit the BSM at a data rate of 18 Mbps and continue to transmit the BSM at a data rate of 18 Mbps until the Channel Busy Ratio falls below 20%.

While we have proposed to use a standard 6 Mbps bit rate, we request comment on the recommendation from BAH and specifically would seek data regarding the following questions:

- Is it appropriate to change the bitrate based on channel busy ratio if the performance within the relevant range is relatively similar across the bitrates under consideration? Would it be more advantageous to use 18 Mbps at all times?
- For changing message bitrates, our understanding is that the transmitting device sends a basic safety message with a header (the first part of the message) always transmitted at 6 Mbps. Our understanding is that the header instructs the receiving device to switch to another bitrate for the remainder of the message. How does this process impact the speed at which devices in the V2V information environment can transmit and receive basic safety messages?
- Is there any information on how much time one would save between transmitting a basic safety message at 6 Mbps versus 18 Mbps (and other bitrates)? In other words, many more messages can be transmitted within a given timeframe if one were to change the bitrate?
- We note that 3 Mbps, 6 Mbps, and 12 Mbps are bitrates that device makers are required to support when they are building a device according to the IEEE 802.11 voluntary standard. The standard affords the option to support other bitrates but does not require it. Is there any information on how many devices support bitrates other than 3 Mbps, 6 Mbps, and 12 Mbps?
- What would the impact be on current systems and voluntary standards under development if the agency were to use a different bitrate (from 6 Mbps) in a final FMVSS?
- BAH suggests that all radios now support 6 and 9 Mbps transmission. (Section 4.3.1 of BAH Report). Is there any information on whether current DSRC radios can support 18 Mbps and dynamically switch between the two bitrates based on channel congestion ratio? What's the cost to implement this change?

[124] Channel busy ratio describes how congested the channel is. When the ratio is 50%, it means that for a 100 ms timeframe, the device sees that there is someone else within range that is transmitting for 50 ms of the 100 ms.

(iii) Existing Research on the Impact of Different Potential Data Rates

There are currently two bodies of research available to the agency on the impact that different bitrates can have on the range and reliability of the transmission of the basic safety message, CAMP and work performed by BAH funded by the agency. In essence, the CAMP research showed that there is a small difference in PER between a 6 Mbps and 12 Mbps data rate at 300 m, the assumed minimum range for V2V communications. The BAH research shows that there was a difference in PER between 6 Mbps, 9 Mbps, 12 Mbps, and 18 Mbps. However, most of these differences occurred at a distance exceeding 500 m.

(a) Increasing Data Rate

CAMP conducted a test involving real devices in an outside environment. VSC-A Report Appendix I[125] showed that, given a dedicated DSRC transmission channel, using a 12 Mbps data rate somewhat degraded the ability of the message to reach its destination when compared with a 6 Mbps data rate. In their research, they used a vehicle broadcasting basic safety messages and placed it in different locations around various radios that attempted to receive the vehicle's basic safety messages during the test. When the researchers placed the vehicle close to the radios, there seemed to be little degradation in whether the radios could receive the messages (regardless of bitrate). Using the 6 Mbps data rate, 58 receiving radios picked up the basic safety messages. Using 12 Mbps, 57 receiving radios were still able to pick up the basic safety messages. However, when they placed a vehicle at the "far edge" of the range of the receiving radios, 55 radios received basic safety messages at 6 Mbps versus only 45 at 12 Mbps. See Figure III-1 and Figure III-2, below.

[125] See Section 3 in Appendix I, http://www.nhtsa.gov/Research/Crash-Avoidance/Vehicle%E2%80%93to%E2%80%93Vehicle-Communications-for-Safety (last accessed: Dec 8, 2016)

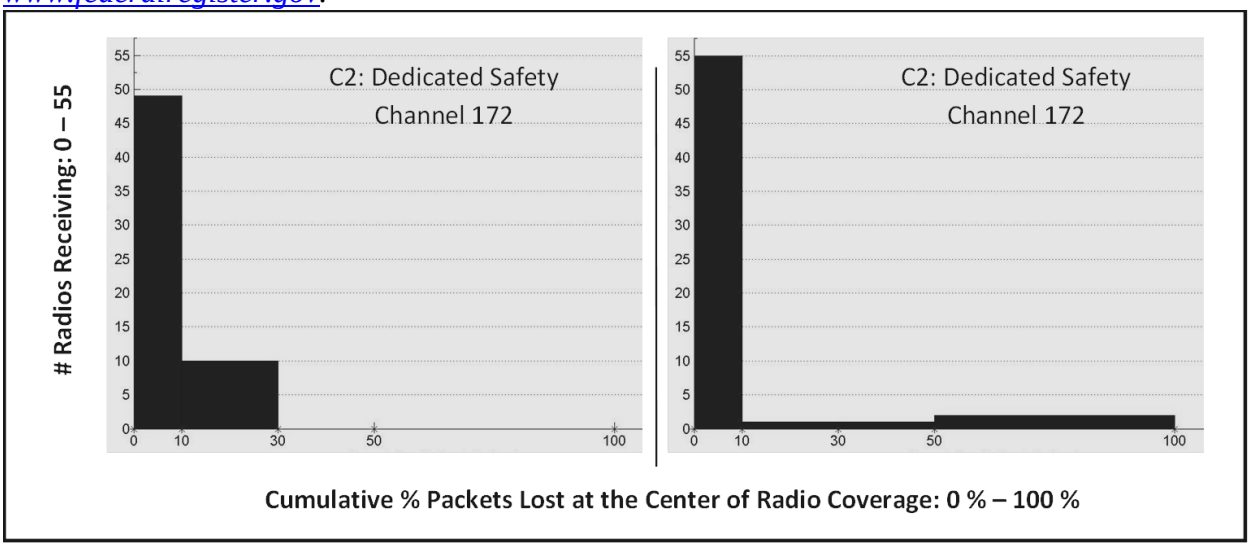

Figure III-1 Cumulative Packet Losses at Center

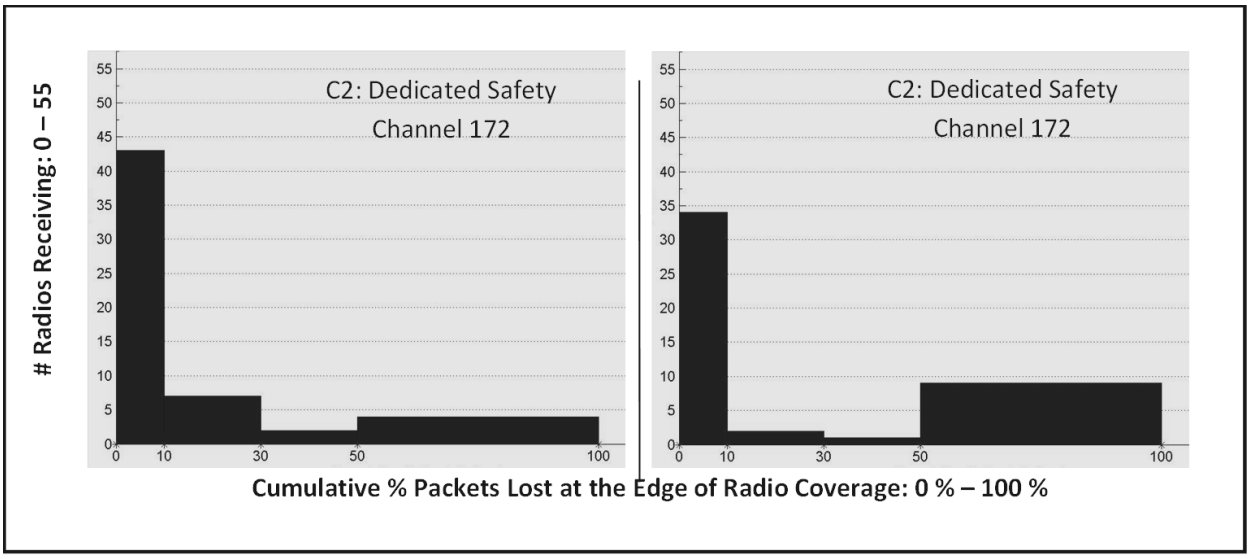

Figure III-2 Cumulative Packet Losses at Edge

In addition, the VSC-A research explored the potential impact of using 12 Mbps as opposed to 6 Mbps within a 300 m test range. As evident in the figure below, when using 6 Mbps, nearly all the devices (up to the 300 m test range) received the messages with a very low PER. However, when switching to 12 Mbps, we observe a small increase in the number of devices that could not receive the messages with a low PER between the range of 100 and 300 m.

The research also examined the impact of different bit rates based on transmission power (i.e., if we transmit with more power, how would the 6 and 12 Mbps bit rates affect the ability of the receiving device to obtain the basic safety message? In the CAMP research, radios were able

to receive packets at a somewhat lower transmission power when they were being transmitted at 6 Mbps as opposed to 12 Mbps (i.e., packets failed to reach their destination when the power was -90 dBm when they were transmitted at 12 Mbps versus -94 dBm when they were transmitted at 6 Mbps).

(b) Differing Bitrates

BAH also conducted research comparing the impact of data transmission rate to the reliability and range of the transmission. In their research, involving transmissions sent on a flat and open road at a test facility, 18 Mbps (they also tested 6 Mbps, 9 Mbps, and 12 Mbps) did not perform as well (i.e., a higher PER at a shorter distance) as the lower bitrates. However, their field test indicated that the ability of the transmission to successfully deliver the packet remained rather constant (regardless of the bitrate tested) up to 500 m.[126]

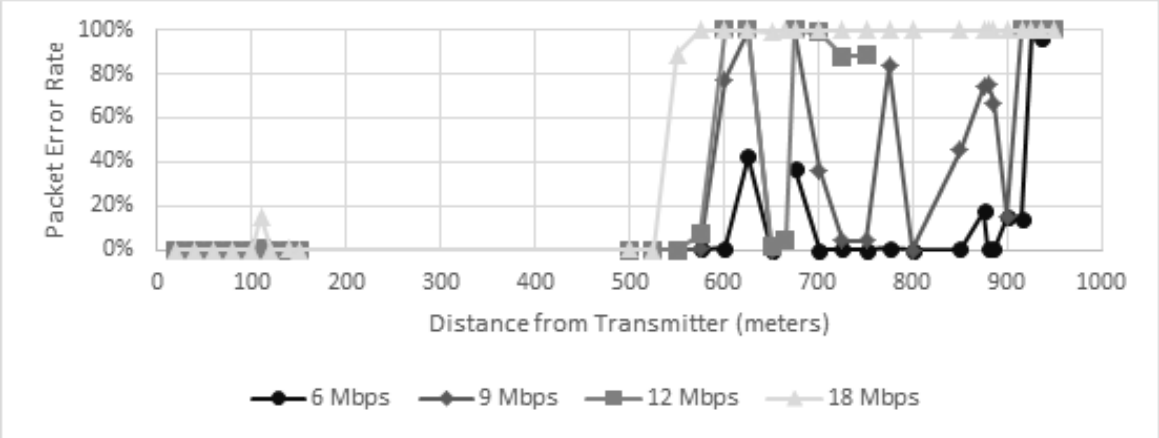

Figure III-3 Packet Error Rate based on Distance

In BAH's report, they surmise that the wide variation of PER at distances above 500 m for all bitrates is attributable to multipath fading.[127] They conclude that an 18 Mbps bitrate seems more susceptible to multipath fading than other, lower bitrates (i.e., the 18 Mbps bitrate might be more sensitive to environmental changes).

[126] *See* BAH DSRC Phase II Report Section 4.3.3.2.

[127] Wireless transmission of information through radio signals often travel to a receiver not only through a direct path, but also through reflections off of other objects in the environment. When the objects move and the direct path between the transmitter and the receiver change, the signal may fade in a variety of ways. Thus, the changing environmental conditions (in addition to some of the other

c) Other Aspects of DSRC Transmission Performance

Thea agency recognizes there other BSM transmission performance parameters that will be necessary for real-world implementation. These parameters are found in the applicable application specifications for DSRC message content and performance parameters. The agency does not see a reason to establish requirements for these parameters based on currently available information. However, we request comment and any supporting information from the public on whether there may be advantages to establishing requirements in these areas to support the safety applications and/or ensure interoperability within the V2V information environment.

(1) Age of BSM transmission

The age of the BSM transmission is monitored by the data element, DE_DSecond. The DSecond data element provides a time value when a BSM is populated with data there may be a lag between the time the data is collected and populated in the BSM—and when the BSM is actually sent. We are proposing that the device should not transmit a BSM if the data within the BSM is over 150 milliseconds old. In the test procedure section in this document, we are specifying a test device for receiving basic safety messages from the tested vehicle. Our rational is that the requirements and test methods requires the device to transmit a timely BSM.

- The system shall set the DE_DSecond with a value corresponding to milliseconds within a minute of the UTC time when the BSM Part I vehicle location data is determined by the positioning source. [MPR-BSMTX-DATAACC-008]
- DE_DSecond shall be accurate to within 1 ms of the corresponding UTC time. [MPR-BSMTX-DATAACC-009]
- DE_DSecond shall have a value less than 150 ms from the UTC time at which the BSM is transmitted (i.e., the age of the time used in DE_DSecond shall be less than 150 ms). [MPR-BSMTX-DATAACC-010]

Note: Other measurements present in the BSM should be aligned to DE_DSecond insofar as possible in the implementation. Since other measurements present in the BSM do not have an absolute time stamp, it is not clear how this is done in practice. Nevertheless, practical implementations to date have used the most recent measurement updates known to the transmitter at the time when the BSM is composed.

(2) Reception

In addition to the issue of transmitting the basic safety message, the V2V research to date also included potential requirements covering the reception of the basic safety message. The potential requirements in this area include the ability of the vehicle to:

- receive a basic safety message given a particular test device's transmission power and distance from the vehicle;

- translate the 0's and 1's received over the wireless airwaves into the basic safety message (i.e., using the appropriate protocol suite to interpret and unpack the wireless signal into the basic safety message content); and
- authenticate the signature of the basic safety message to confirm that the information is from an authenticated source (i.e., to determine that the message is actually from a vehicle).

While the research (e.g., the V2V safety pilot) included many of these aspects of performance, we tentatively believe that it is unnecessary to separately evaluate the vehicle's ability to receive the basic safety message as a number of indirect methods determining if a vehicle received the information exist in the transmission requirements already, namely congestion detection and mitigation.

Although this may be counterintuitive, we believe that directly evaluating the reception of the basic safety message is best conducted under conditions where the vehicle is using the information from the basic safety message for a particular purpose. For example, when there is a safety application, the receiving and processing the basic safety message transmissions leads to a response from the vehicle (e.g., a warning). In these conditions, the vehicle's reception of the basic safety message is indirectly (and, we believe, sufficiently) tested by exposing the vehicles to basic safety messages with certain information (e.g., information about a vehicle on a collision course with the tested vehicle) and then measuring the vehicle's response (e.g., whether it issues a warning at the appropriate time).

As this proposal does not include requirements for applications, the agency would need to require vehicles to output a log or record of the basic safety messages that they received within a given amount of time in order to assess whether the vehicle is able to complete the three tasks mentioned above. However, we tentatively believe it's unnecessary at this time to include additional requirements to check a vehicle's ability to receive basic safety messages. By requiring the vehicle to mitigate congestion, we believe that the vehicle must incorporate the ability to receive the message.

Regardless of methods employed, congestion mitigation requires the vehicles to determine the local vehicle density inside a given radius as part of the determination of the maximum time between messages. To do this, the vehicle not only has to have the ability to understand the base channel busy ratio, but also decode the message enough to expose the various temporary IDs of the received BSMs to get an accurate vehicle count. To decode the message far enough to get the temporary IDs, the vehicle needs to be able to interpret the BSM and all of its sub-layers.

We also believe that automakers implementing safety applications would ensure that the vehicle would have the capability to receive the basic safety message (including receiving the transmission and processing the transmission to obtain the message) and authenticate the message. Because the performance of an automaker's safety application in a vehicle would rely on the vehicle's ability to reliably receive basic safety messages, we believe that automakers

implementing safety applications would also have a strong incentive to implement an appropriate receive capability in their vehicles.

However, we request comment on our tentative conclusion. We seek comment on whether there is any reason that the agency should include direct requirements for receiving the basic safety message (independent of the vehicle's capability to utilize the information for a safety application, congestion control, Misbehavior detection, or other intended uses). Further, we request comment on what performance the agency should assess and how the agency should assess such performance (i.e., how does the agency test the reception of information when the vehicle is not expected to do anything in response to that information?). Finally, the agency seeks comment on whether there is a need to specify requirements for DSRC devices to have message reception filtering for interference from operation in the adjacent unlicensed spectrum. Please provide substantive data and clarifying reasons why or why not this is necessary along with potential filtering strategies that could be employed, if the commenter believes message reception filtering is necessary.

One potential way to establish direct requirements and measure performance of those requirements would be to require vehicles to:

- store all basic safety messages received within a certain amount of time (e.g., 5 minutes during the test); and
- output the data through a specified interface or collection of interfaces (e.g., OBD-II).

To test this performance, we would use a test device to generate basic safety messages near the tested vehicle. Access the tested vehicle using the specified interface in the standard and download the basic safety messages received file. Verify that the basic safety messages received by the tested vehicle match the basic safety messages transmitted by the test device. We request comment on whether this is a viable method for establishing requirements for this aspect of performance.

(3) Message Packaging and Protocol Suites

Finally, another important part of ensuring interoperability of any network is for all the devices participating in the network to agree to the same communications method (i.e., speak the same language). For electronic devices communicating over a network, the method of taking information and packaging that information (i.e., in multiple steps, converting it into a string of 1's and 0's) so that it can be sent across a wireless (or wired) network is called a protocol stack. Each step in the protocol stack packages the information for the next step. The transmitting device and the receiving device need to agree upon one method of packaging information so that the transmitting device knows how to package the information into 1's and 0's and then the receiving devices knows what to do with the received 1's and 0's in order to extract the information transmitted.

DSRC communications within the 5.85 to 5.925 MHz band are governed by FCC 47 CFR Parts 0, 1, 2 and 95 for onboard equipment and Part 90 for road side units. In reference to the OSI model, the physical and data link layers (layers 1and 2) are addressed primarily by IEEE 802.11p as well as P1609.4; network, transport, and session layers (3,4 and 5) are addressed primarily by P1609.3; security communications are addressed by P1609.2; and additional session and prioritization related protocols are addressed by P1609.12.

Further, a variety of communication performance standards specific to the V2V communications and BSM transmission/reception are defined in SAE J2945 while data element and data frame definitions and coding requirements are defined in SAE J2735.

Devices adhering to these standards know how to package the basic safety message for transmissionover the DSRC 5.9 GHz spectrum. They also know how to interpret and unpack transmissions over that spectrum in order to obtain the basic safety message. While our proposed rule does not include explicit requirements for vehicles transmitting basic safety messages to utilize the methods for packaging the basic safety message in IEEE 802.11 and 1609, our proposed performance test (in effect) would require vehicles to do so.

As further discussed in the test procedure section in this document, we are specifying a test device for receiving basic safety messages from the tested vehicle. Our proposed test device would utilize the method for unpacking the basic safety message that is specified in 802.11 and 1609. Thus, in essence, vehicles transmitting the basic safety message will need to package the message utilizing the same method in order to deliver the message to the test device in our test. If the vehicle is unable to transmit a message packaged in a way that can be unpacked by our test device (i.e., using the IEEE method), the vehicle would fail our proposed performance test.

In this manner, we believe we are specifying a protocol stack that would ensure that devices following the packaging method of the protocol stack would be able to transmit and receive basic safety messages on the DSRC 5.9 GHz spectrum. We request comment on our tentative conclusion. Does the agency need to specify any additional areas of performance in order to ensure interoperability of the devices? In other words, what aspects of the packaging of the data for transmitting cannot be tested by our proposed test method? How does that impact device interoperability and how would the agency test it?

d) DSRC-based communication- Applicable Industry Standards

(1) Standards and DSRC V2V Technology

Vehicle to Vehicle technology incorporates many components to facilitate crash avoidance capabilities. The basis for Vehicle-to-Vehicle crash avoidance is the communication of safety information among vehicles. Figure III-4 identifies the various components that a DSRC-based system would include; the DSRC radio, GPS receiver, Memory, Safety Applications, Vehicle internal communications network, System Security, and the Driver-Vehicle interface.

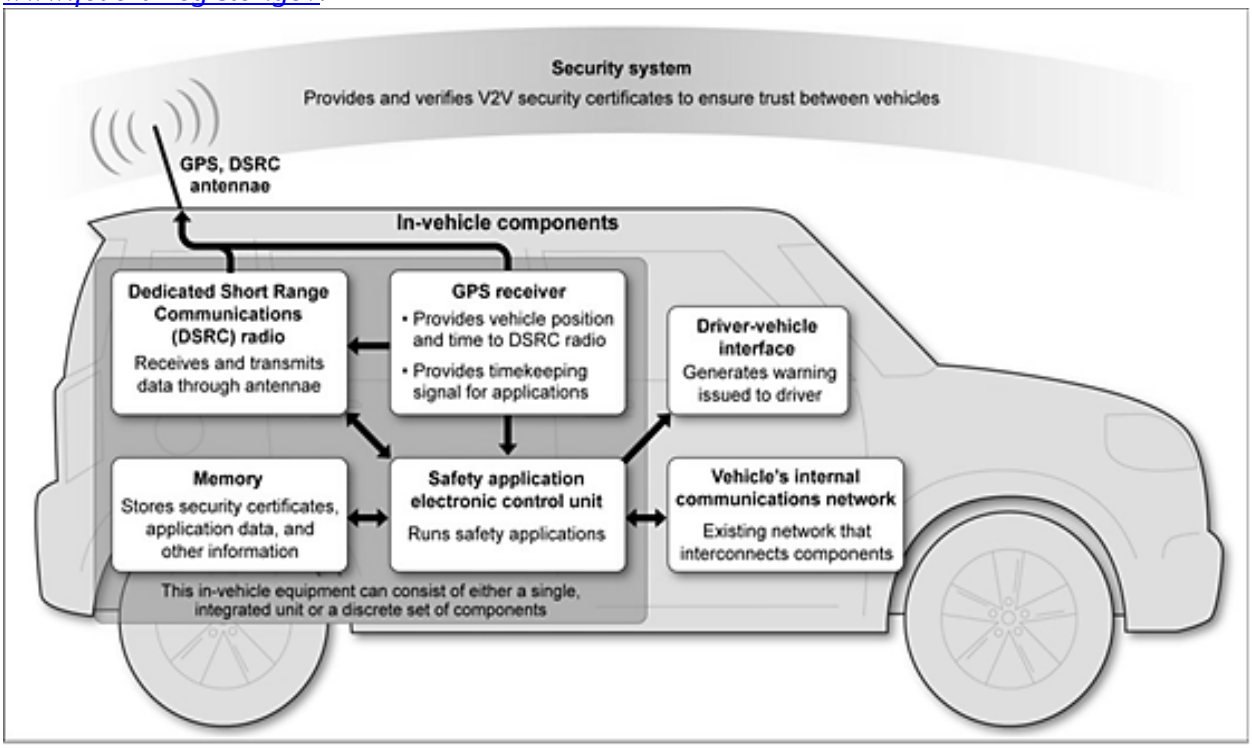

Figure III-4 V2V System Components utilizing DSRC

To support the V2V wireless communications, a set of voluntary consensus standards will need to continue to be developed. These standards define such things as how devices are to communicate over an identified frequency; how to exchange information including instructions for sending and receiving messages; how to structure, format, and understand message content; and the data elements making up the message content.

We expect that V2V communication will be covered by a family of integrated standards from different organizations that deal with different aspects of wireless communications and message exchange. Such standards will facilitate V2V device developers and implementers successfully exchanging safety messages and security information (e.g. interoperability). The standards will help ensure interoperability meaning any device identified as a V2V device communicates and interprets the messages in the same way.

(2) Voluntary Consensus Standards

Voluntary consensus standard: The term "voluntary" distinguishes the standards development process from governmental or regulatory processes. All interested stakeholders participate, including producers, users, consumers, and representatives of government and academia. Voluntary standards are also made mandatory at times by being incorporated into law by governmental bodies.

A voluntary consensus standards body is defined by the following attributes:

- *openness;*
- *balance of interest;*
- *due process;*
- *an appeals process;*
- *consensus, which is defined as general agreement, but not necessarily unanimity, and includes a process for attempting to resolve objections by interested parties, as long as all comments have been fairly considered, each objector is advised of the disposition of his or her objection(s) and the reasons why, and the consensus body members are given an opportunity to change their votes after reviewing the comments.*[128]

Voluntary consensus standards follow a rigorous, industry inclusive development process where each standard is developed by an established committee that consists of volunteer representative from interested stakeholders. Examples of such organizations include the Institute of Electrical and Electronic Engineers (IEEE), ASTM International, SAE International (SAE), and the American National Standards Institute (ANSI). Each committee establishes membership protocols regarding voting criteria, structure and format guidelines, and how information is contributed. The committees draft the standards and, once drafted, the standards are presented to the organizations membership for review, comment, and balloting[129]. If the standard is balloted and accepted, the standard is published. If needed, there are processes for a standard to be revised or updated as technology evolves. We anticipate that such bodies will develop the standards that provide the information to develop and implement interoperable V2V communications, but again stress that our performance requirements may permit technologies other than DSRC to perform V2V communications in the future.

In relation to DSRC V2V Communications, to date two voluntary consensus standard organizations have developed separate, however, interrelated standards based on DSRC-enabled V2V communications. These organizations are the Institute of Electrical and Electronic Engineers (IEEE), and the Society of Automotive Engineers (SAE). IEEE has developed two standards, IEEE 802.11p and IEEE 1609.x. IEEE 802.11p establishes how compliant devices will transmit and receive messages using the 5.9 GHz frequency. IEEE 1609.x defines the protocols for radio channel operations, message exchange, and message security. SAE has also developed two standards, SAEJ2735 and SAEJ2945. SAEJ2735 specifies the BSM message set,

---

[128] See "Standards Glossary" IEEE, https://www.ieee.org/education_careers/education/standards/standards_glossary.html (last accessed Dec 12, 2016)

[129] For a description of the IEEE ballot process, see http://standards.ieee.org/develop/balloting.html (last accessed Dec 12, 2016)

its data frames, and data elements. SAEJ2945 establishes minimum performance requirements for the BSM data elements in various messages.

The set of standards for DSRC detail the procedures, protocols, and message content to support the broadcast (special communication capability of DSRC) and receipt of the Basic Safety Message and the linked communications needed to transfer security materials to establish a more secure V2V communications environment.

(3) Computer and Wireless communication reference model

To facilitate the communication needed from devices (hardware) to the applications (software) the International Organization for Standards (ISO) established the Open System Interconnect reference model (OSI). The OSI reference model consists of seven layers that define the different stages data must go through to travel from one device to another over a network[130]. Each layer has unique responsibilities including passing information to the layers above and below it.[131] The combination of layers represents protocol stacks. This structure and nomenclature of the OSI reference model is used in the V2V related standards. The Standards cover how data is communicated and interpreted from one V2V device to another device and processed to be used by crash avoidance applications; analogous to how your wireless router transfers data via the internet to an application on your computer such as a web browser.

The layers represent levels of interfaces to enable the bits that represent data to be properly transported and interpreted. The layers are illustrated in Figure III-5. The first layer starts at the bit/hardware device level and indicates how the steam of raw information is sent to the next layer. In relation to V2V this would be the DSRC radio level. In addition to the raw information, layer 2 organizes data packets into network frames that are transported across the V2V wireless network. These first two levels are covered by IEEE 802.11p. The next 3 layers are covered by IEEE 1609.x. Layers 3, 4, and 5 handle the addressing and routing of messages, management of the packetization of data and delivery of packets, and the coordination of message transmissions and authorization (security). Layer 6, session layer, and layer 7, application layer, are covered by SAE J2735 and SAE J2945 and provide for the conversion of incoming data for use by the application and interface protocols with the applications. [132] These layers and associated standards represent the DSRC protocol stack that developers use to design and produce interoperable devices.

---

[130] See "How stuff works - How OSI Works" http://computer.howstuffworks.com/osi1.htm (last accessed: Dec 12, 2016)
[131] See "Physical Layer", http://www.linfo.org/physical_layer.html (last accessed: Dec 12, 2016)
[132] See "OSI reference model (Open Systems Interconnection)" http://searchnetworking.techtarget.com/definition/OSI (last accessed: Dec 12, 2016)

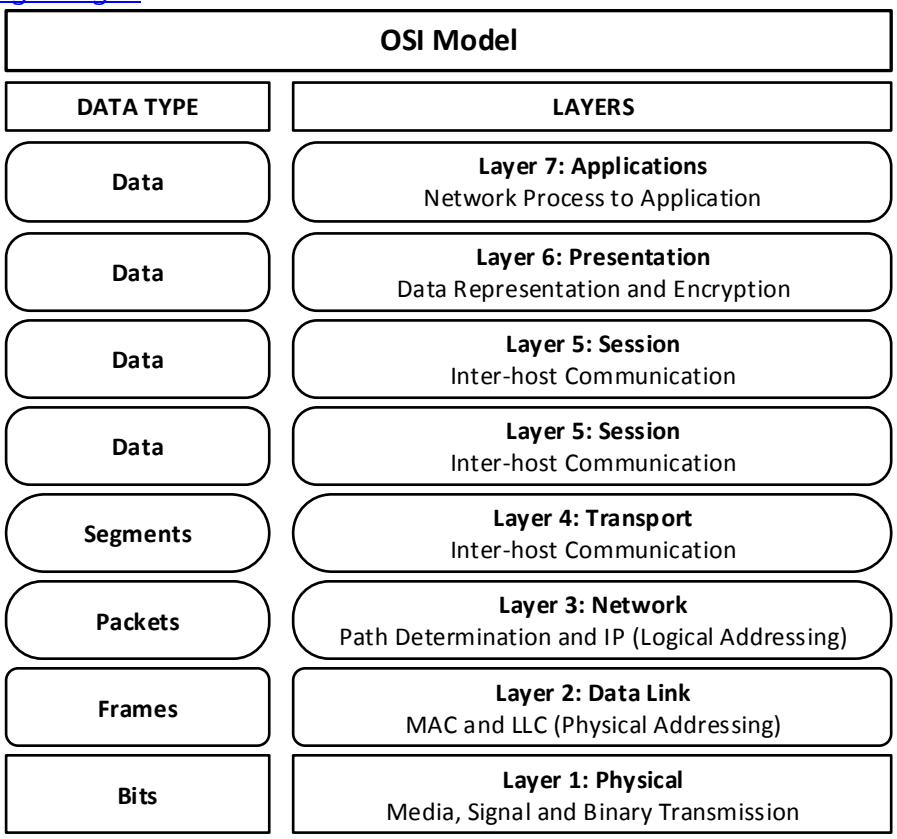

Figure III-5 OSI Stack

(4) DSRC-based V2V device Communication Standards

As indicated previously, SAE and IEEE have developed and established standards for DSRC. The DSRC protocol stack and related standards are illustrated in Figure III-6.

Working from the bottom of Figure III-6 and starting with the physical layer, the IEEE 802.11-2012 – IEEE Standard for Information technology-Telecommunication and information exchange systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications was published 29 March 2012. The standard covers operations of Wi-Fi devices. A specific section of the standard, 802.11p, covers DSRC communication for V2V and V2I devices that use the 5.9 GHz frequency. The standard describes information exchange between system local and metropolitan networks at the device radio level.

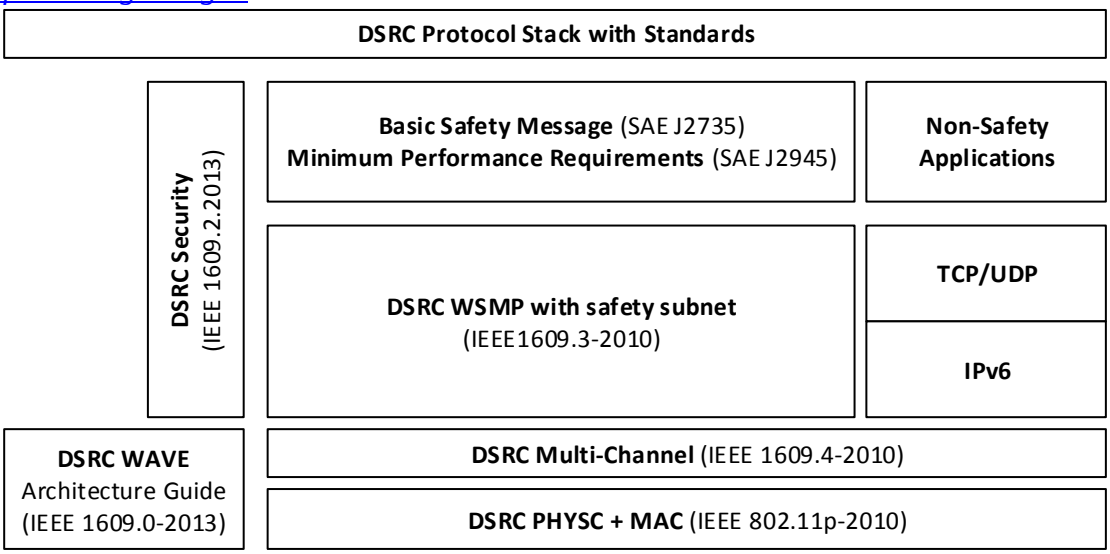

Figure III-6 DSRC Protocol Stack

From the device (hardware) level of 802.11, the IEEE 1609.x family of standard establishes the protocols for Wireless Access in Vehicular Environments (WAVE). These standards support the network, transport, and session OSI layers. The 1609 standards that are relevant to DSRC include the following:

- 1609.0 – Guide for Wireless Access in Vehicular Environments (WAVE) Architecture – This section of the standard describes the full set of 1609 standards and their relationships to each other and other relevant standards such as 802.11. The guide was published 11 December 2013.
- 1609.2 – Security Services for Application and Management Messages – Describes the secure message formats and processing for use by WAVE devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions. The V2V security design is based on this standard and incorporates an expanded application of Public-Key infrastructure to secure V2V communications and appropriately protect privacy. This standard is associated with Layer 5, session layer, and Layer 6, presentation layer. This standard was published 26 April 2013.
- 1609.3 – Networking Services – In relation to Layers 3 and 4, network and transport, this standard describes the Internet Protocol (IP), User Datagram Protocol (UDP), and the Transmission Protocol (TCP) elements of the internet model and management and data services for WAVE devices. This standard was published 13 July 2012.
- 1609.4 – Multi-Channel Operations – This standard crosses layers 2 through 5 to support multi-channel operations of the DSRC radio. Wireless radio operations that include the use of other channels need to provide instructions concerning the

operation of the control channel (CCH), the service channel (SCH), interval times, priority access, channel switching, and routing. The current design for a V2V DSRC device uses two radios. One radio is tuned to channel 172 for transmission and reception of the safety-critical communication of the BSM. The second radio uses multi-channel operations to set the CCH and SCH, and use the other channels to support other messages transmission such as the messages associated with security materials. This standard was published 7 February 2011, however, a draft corrigendum that corrects errors is pending publication.

- 1609.12 – Identifier Allocations – For the WAVE system this standard describes the use of identifiers and the values that have been associated with the identifiers for use by the WAVE system. This standard was published 21 September 2012.
- Layers 6, Presentation, and Layers 7, Application, are supported by the two SAE standards that define the elements and the minimum performance requirements for the BSM data elements.

SAE J2735 – DSRC Message Set Dictionary specifies a message set, and its data frames and data elements specifically for use by application intended to utilize the 5.9 GHz frequency. For crash avoidance safety, the standard identifies the Basic Safety Message (BSM). The standard includes an extensive list of BSM data elements divided into two parts. Part one includes elements that are transmitted with every message. Part two includes elements that are included in the transmission when there is a change of status. The BSM is exclusive to the support of crash avoidance safety applications. Section III.E identifies the BSM elements that are identified as minimum performance requirements for V2V devices.

SAE J2945 – DSRC Minimum Performance Requirements – This standard resulted from research indicating a need for a separate standard that would describe the specific requirements for the data elements that would be used in the BSM. The standard will also cover other DSRC messages; however, the first part of the standard will specify the performance requirements for the BSM data elements. The draft of the first part of the standard is being developed using results of V2V research. The standard for BSM performance requirements is scheduled to be completed and balloted late 2015.

The standards explained above represent voluntary consensus standards that have been developed by standards development organization. These standards are not regulatory. These standards, however, do provide a basis of investigation as to what is needed in relation to identifying the minimum performance requirements that if met ensure the proper and safe functionality of V2V DSRC device that will result in the avoidance of crashes.

(5) Relevance to DSRC-based communications

The SAE and IEEE standards supporting DSRC discussed are not performance requirements *per se*. Performance requirements and standards are interrelated and indicate, at different levels, how a system or device must function. Performance requirements are developed to indicate how a device or system needs to perform. In terms of V2V, performance

requirements are associated with an installed device and are viewed from the top of the design and development process. Performance requirements may incorporate various standards that are identified in Section III.D, however, most of the standards are related to sub-systems and components that support the development of design specifications. The higher level performance requirements indirectly verify lower level standards were used by verifying the design performs at the integrated system level.

Figure III-7 illustrates our understanding of the hierarchical relationship associated with performance requirements and how standards are used at different component design specification levels. The bulk of the V2V related standards support primarily support product development specifications at the Controller Spec level and the Component Technical Spec level. The specifications are verified at each level by different component test and sub-system tests. The Auto OEMs conduct tests at the system level to verify design and system operations. After installation, OEMs conduct vehicle integration tests to verify installation and system operation in relation to design specification and regulation identified performance requirements. Once the integration is verified, the Auto OEMs verify compliance with the performance requirements. This hierarchy demonstrates how top level performance requirements supported by standards provide the information to successfully design and implement V2V components that will be interoperable and meet identified system level performance requirements.

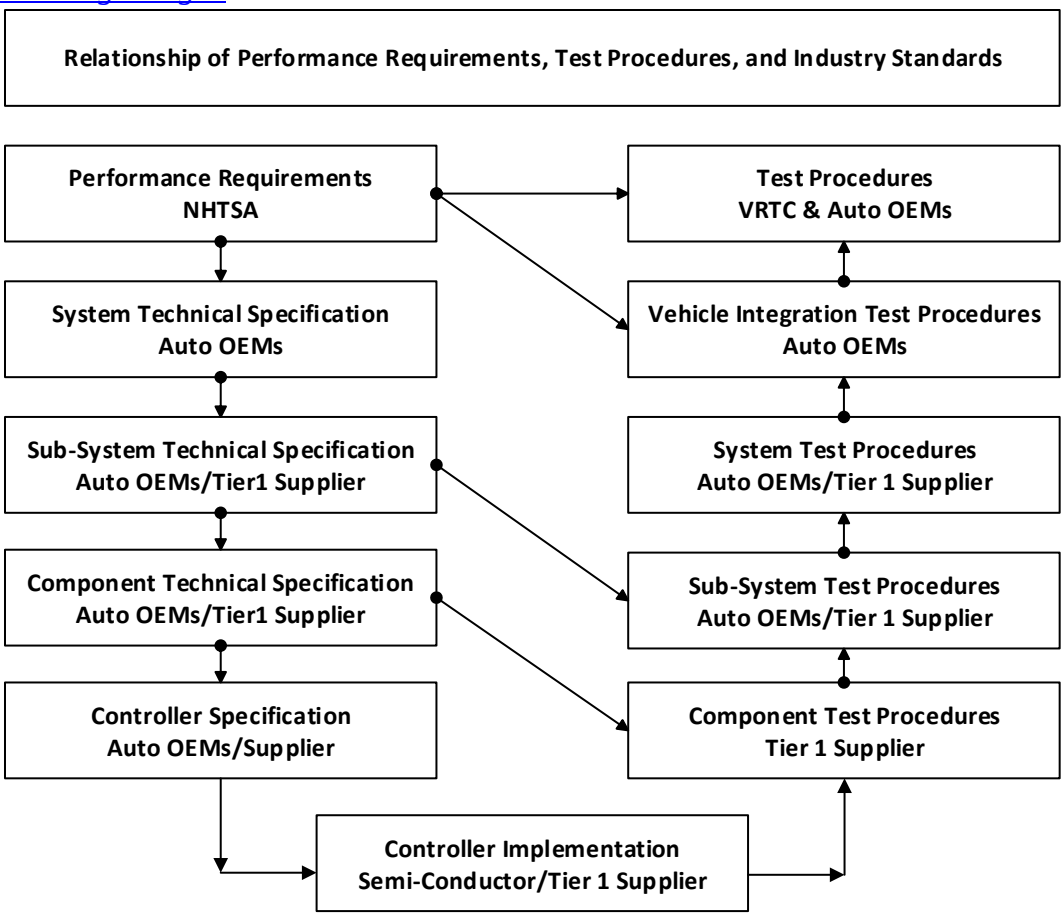

Figure III-7 Relationship of Performance Requirement to Production Product

The voluntary consensus standards provide information that support both performance requirements and design specifications, and are the bridge for connecting the requirements to the specifications. In relation to the NPRM, the work performed by NHTSA in relation to performance requirements is to identify, and define performance requirements and verification tests that will indicate that V2V device have been designed and implemented such that these devices will operate to provide the DSRC communications and security that will support crash avoidance applications.

(6) Summary of DSRC-based BSM Transmission Requirements

Table III-1 Summary of BSM Transmission Requirements

Requirement	Proposal	Basis	Relationship to Standards	Reason
Range (longitudinal & lateral)	Minimum 300m; 360 degrees around vehicle	CAMP – application tested in SPMD also calculation of range	SAE J2945/1	The setting is based on the need to provide accurate and timely safety alerts.

		needed for DNPW		The setting was obtained by extensively testing commercially available equipment and automotive sensors in a wide variety of driving environments.
Range (Elevation)	At elevation angle of +10 degrees and -6 degrees	CAMP and BAH research and testing capabilities	SAE J2945/1	Same as above
Reliability	Packet Error Rate < 10%	CAMP and BAH	SAE J2945/1	Same as above
BSM Radio Channel	All BSM transmissions and receptions on 172 (safety-critical communications).	FCC rules.	SAE J2945/1	Same as above
Data Rate	6 Mbps	CAMP and BAH research – CAMP research shows PER degradation using 12 Mbps. BAH research indicates problems after 500m, also BAH test done under "open field" conditions.	SAE J2945/1 (one of the bitrates included in 802.11)	Same as above – Also Current developers support a 6 Mbps data rate. More data and testing is needed to change the data rate and determine if a changing rate can be used and support crash avoidance.
Transmission Frequency	10 times per second under non-congested conditions	CAMP – trade-off between long inter-packet delays experienced by V2V safety applications and heavy wireless channel utilization.	SAE J2945/1	Accepted among experts to support V2V crash avoidance
Staggering Transmission Time	Random transmission of BSMs every 100 +/- ms between 0 and 5 ms	Mitigate channel congestion if all devices transmitted at same time – CAMP and BAH research	SAE J2945/1	Due to accuracy of devices need to mimic the stagger experienced during SPMD to avoid message collisions to facilitate efficient channel usage

e) Alternative (Non-DSRC) Technologies

This section is intended to recognize and support the continual progression of communication technology. It proposes alternative interoperable technologies performance requirements grounded in today's DSRC technology, which would enable the deployment of potential future V2V communications technologies that meet or exceed the proposed performance requirements, including interoperability with all other V2V communications technologies transmitting BSMs.

This section provides performance-based requirements that would support transmitting the basic safety message via alternative interoperable technologies. The proposed requirements are limited to the transmission of the BSM only. Potential security and privacy requirements and alternatives are discussed in those respective sections of this proposal.

Alternative technologies would need to meet the same message transmission requirements as DSRC-based devices, minus any DSRC-specific requirements such as channel or data rate specifications.

(1) Transmission Range and Reliability

Alternative technologies would need to support the same message transmission range and reliability requirements as DSRC-based devices, minus any specific references to DSRC.

(i) Range

Alternative technologies would need to support the same message transmission range requirements as DSRC-based devices, minus any specific references to DSRC.

(ii) Longitudinal/Lateral Range

Alternative technologies would need to support the same message transmission longitudinal and lateral range requirements as DSRC-based devices, minus any specific references to DSRC.

(iii) Elevation Transmission Performance

Alternative technologies would need to support the same message transmission elevation performance requirements as DSRC-based devices.

(2) Testing the Elevation Transmission Range

Alternative technologies would need to support he same message transmission elevation test requirements as DSRC-based devices.

(a) Test Device

Alternative technologies would need to support the same message transmission elevation transmission performance test device requirements as DSRC-based devices, minus any reference to DSRC.

(b) Location of the Test Device

Alternative technologies would need to support the same message transmission elevation test device location requirements as DSRC-based devices.

(3) Reliability

Alternative technologies would need to support the same message transmission reliability requirements as DSRC-based devices, minus any reference to DSRC.

(4) Aspects of Transmission Range Performance Indirectly Tested

Alternative technologies would need to support the same message transmission range performance indirect tests as DSRC-based devices.

(a) Transmit Power

Alternative technologies would need to identify the same transmit power as DSRC-based devices, where applicable for a specific communication medium.

(5) Channel and Data Rate

A final rule will need to indicate the range at which the vehicle needs to transmit the basic safety message and the receive sensitivity for alternative technologies.

(6) Transmission Timing

Alternative technologies would need to meet the same transmission timing requirements as the DSRC-based proposal minus any DSRC-specific requirements, such as channel and data rate. In keeping with the more general nature of the standards for alternative technologies, specifying aspects such as channel congestion or the need for staggering or synchronizing message transmission is assumed not to be needed and assumed to be handled by any protocol or communication medium used for V2V communication.

(a) Default Transmission Frequency

Alternative technologies would need to support the same message transmission frequency as DSRC-based devices, 10 times per second (10 Hz).

(b) Staggering Transmission Time

Alternative technologies would need to address the same issues for staggering transmission timing as DSRC-based devices, minus any direct reference to DSRC.

(7) Other Aspects of Alternative Interoperable Technologies

Alternative technologies would need to address the same issues for staggering transmission timing as DSRC-based devices, minus any direct reference to DSRC.

(a) Age of BSM transmission

Alternative technologies would need to support the same message age monitoring requirements as DSRC-based devices.

(b) Reception

Alternative technologies would need to support the same message reception requirements as DSRC-based devices, minus any references to message congestion mitigation, misbehavior detection, and DSRC-specific messaging content.

Additionally, NHTSA does not seek comment on the need to specify requirements for reception interference from operation in the adjacent unlicensed spectrum given this would be spectrum dependent.

(c) Interoperability

V2V devices using alternative technologies would need to be capable of transmitting and receiving an established message from other V2V devices, regardless of the underlying technology (i.e. the BSM that has specified content of information, but also the measuring unit for each information element and the level of precision needed) Interoperability with DSRC-based devices would, in particular, be necessary. We seek comment on what test procedures or other safeguards would be required to ensure interoperability.

2. Proposed V2V Basic Safety Message (BSM) Content

At the core of this proposal is the basic safety information that we believe vehicles need to send in order to support potential safety applications. In order to realize the safety benefits discussed above, safety application designers need to know what consistent set of information will be available, what units will be used to express that information, and the level of accuracy that each information element will have. This uniform expression of the basic safety information is important because a safety application needs to rely on the information in the messages and assume that the information is accurate to within a given tolerance. The requirements proposed in this section are consistent across any potential communication technology employed in V2V communications.

To date, the automotive industry (through SAE) has been developing voluntary consensus standards[133] to help standardize these details of the basic safety message. The general approach of our proposal is to incorporate the data elements from the current draft SAE standards in order to facilitate interoperability between devices that would comply with the proposed FMVSS and any potential future developments of the SAE standards. Further, we are considering each data element and associated tolerance requirements for each of those elements in the context of addressing the safety need of avoiding crashes. Each of the data elements we are proposing to require provide values that collectively contribute to the calculations of possible vehicle interactions and evaluating the imminent crash potential of these interactions. Moreover, the required and optional data elements would create a data-rich environment that can be used to not only identify imminent crash situations, but also ensure the drivers can be given advanced warning of these situations so these drivers can take appropriate evasive action to avoid crashes. Based on our analysis, we are proposing requirements for some, but not all, of the data elements in the SAE standards. However, in order to preserve interoperability with vehicles that may choose send additional data elements, we are generally proposing to permit vehicles to transmit a data value that either conforms to the SAE standard or is the SAE-specified "data unavailable" value.

Finally, we are also proposing to exclude certain data elements from being transmitted as a part of the BSM. We are proposing this limitation in order to balance the privacy concerns of consumers with the need to prove safety information to surrounding vehicles.

While we request public input on any of the issues discussed in this section, we especially would like input on whether we have appropriately selected (1) the data elements to include/make optional/exclude, and (2) the tolerance levels for each data element.

(1) Required Data Elements and their Performance Metrics

In the work completed by SAE thus far,[134] the automotive industry separated the information transmitted in the basic safety message into two parts (Part I and Part II). As we explained in the Readiness Report, Part I information is core information intended to be sent in every basic safety message. Part II is additional information intended to be sent as needed. In this section, we cover data elements from both Part I and II that our proposed requirements would include the performance metrics for each.

(a) Message Packaging

Before reaching the actual elements that support safety applications, the basic safety message needs certain preliminary elements that help a receiving device to know what it is

[133] E.g., SAE Standard J2735, J2945.
[134] SAE J2735 and J2945

receiving. The three elements that fall into this category are the Message ID, the Message Count, and the Temporary ID. We tentatively believe that all three of these elements are necessary as they allow the receiving device to interpret the digital code it is receiving and the safety information inside the message. The three elements provide the information needed for the device to properly process a sequence of messages that delivers vehicle position and motion data needed to interpret possible crash situations.

(i) Message ID

The first element is the Message ID. This data element explains to the receiving device that the message it is receiving is a basic safety message. SAE Standard J2735 specifies that this data element is one byte from 0 to 15.[135] Each number represents a different type of message that could be sent over DSRC. We are proposing to V2V devices sending basic safety messages transmit a "2" as the Message ID. Based on SAE Standard J2735, "2" indicates to the receiving device that the content of the message is a basic safety message and that it should interpret the data accordingly.

(ii) Message Count

The second element here is the Message Count. In SAE Standard J2735, the Message Count assigns each basic safety message a number in sequence between 0 and 127.[136] Once the device's Message Count reaches 127, the idea is that the next message it sends would have a Message Count of 0. This count helps the receiving device know that it has all the messages sent by the sending device and which order to put them in. For example, if I receive messages 11, 13, 14, and 15 from a particular device, I will know that they are in order but I will know that I am missing message 12 from that particular device. The agency's proposal would require that vehicles follow the requirements of the SAE standard and assign the Message Count for each message in sequence between 0 and 127. We believe that this Message Count data element will enable safety applications that receive these messages to appropriately put the messages in order and be aware of any missing messages that could affect the overall information being processed by the safety application software.

(iii) Temporary ID

Finally, the Temporary ID is a four-byte string array randomly-generated number that allows a receiving device to associate messages sent from the same device together. While the identity of the sending device is not important for a safety application to take appropriate actions during a crash-imminent situation, it *is* important for a safety application to know that it is

[135] SAE Standard J2735, page 171.
[136] *Id.* at page 212.

receiving, for example, ten messages from one device rather than five messages from two devices. In other words, the Temporary ID balances the safety need of associating basic safety messages with each other (to know if they originate from the same device), with the privacy need to avoid tracking/identifying particular users.

In order to accomplish these goals, we propose that vehicles transmit a Temporary ID as specified in SAE Standard J2735. Based on the SAE standard, the Temporary ID is a randomly-generated four-byte sequence of numbers selected from 4,294,967,296 combinations.[137] There are many acceptable techniques to generate a random sequence of numbers for the Temporary ID and it does not need to be specified; however, the performance can be tested. Further, the randomly-generated ID is changed to another randomly-generated ID every five minutes, when the BSM security certificate changes. Having the ID and the certificate change at the same time reduces some of the risk that a relationship between the ID and certificate could be developed to track a device. Given the current research available, changing security certificates at five minute intervals helps to reducing the risk of tracking which helps to protect consumer privacy. Additional research is being conducted to further investigate the ability or limitation of the five minute time period to mitigate the potential for tracking and protect privacy.

(b) Time

In addition to the data elements necessary for packaging the basic safety message, the Time data element is critical because all of the information within the basic safety message (e.g., the vehicle location, speed, etc.) being used to enable safety applications needs to be expressed in the context of time. Based on time, the safety application is able to determine when a surrounding vehicle was in a given location and assess where that vehicle may go. Thus, it is important for the Time element not only to be expressed precisely but also using a uniform system among the devices participating in the V2V information environment.

In order to accomplish this purpose, we propose a standard system for vehicles to express time in the basic safety message and a requirement for the accuracy of the time. DSRC-based devices would be required to adhere to SAE Standard J2735[138] and devices would be required to use the UTC[139] standard for time. The UTC standard is widely accepted. It is also the predominant standard for time for internet devices and GPS devices—two groups of technologies that are closely related with V2V devices. Thus, we believe that the UTC standard is an appropriate standard method for expressing time. Further, we tentatively believe that the UTC

[137] *Id.* at page 252.
[138] *Id.* at page 62.
[139] Coordinated Universal Time International Telecommunications Union Recommendation (ITU-R TF.460-6),
[139] *See* BAH Report Section 4.3.6.2pubrec/itu-r/rec/tf/R-REC-TF.460-6-200202-I!!PDF-E.pdf

method for expressing time contains an appropriate level of accuracy—including a method for accounting for leap seconds.[140]

In addition to using the UTC standard, we propose to require vehicles to transmit the Time data element to an accuracy of 1 ms (i.e., within +/- 1 ms of the actual time). Given the proposed requirements for transmitting the messages, we believe that requiring the time information accompanying each basic safety message to be within 1 ms of the actual time is appropriate. As further discussed below, we are proposing that vehicles transmit a basic safety message 10 times a second (unless specific conditions require otherwise). In the discussions that follow, we are also proposing that vehicles broadcast the messages (in order to help avoid vehicles broadcasting at the same time) at a staggered time (a random value of +/- 5 ms from every tenth of a second). Given these requirements where the broadcast time of a message can vary by as little as 1 ms, we tentatively believe it is appropriate to require that the Time data element be accurate to within 1 ms.

(c) Location

This set of data elements form the foundation of the basic safety message because it is the information that enables all the safety applications being developed to utilize the V2V information environment. The location information of the surrounding vehicles enables a safety application on a vehicle to know whether a crash imminent situation exists or is likely to exist in the near future. For example, an application such as IMA would use location information of surrounding vehicles to determine whether another vehicle is heading into the intersection and likely to cause a crash.

For location, longitudinal and lateral (2D) data, and also vertical (elevation) data would be required. We acknowledge that longitudinal and lateral data are more commonly used in V2V safety applications (since vehicle travel is mostly two dimensional). However, elevation also is important in a number of respects. For example, safety applications such as FCW or LDW can potentially take into account elevation information for merging traffic in on-ramp situations. Further, applications currently under development such as IMA are already taking elevation into account to differentiate cross traffic that is on an overpass from situations where the cross traffic is on the same plane of travel (i.e., could potentially lead to a crash).

(i) Vehicle Position Reference Point

In order for vehicles to accurately communicate their position in a basic safety message to each other, all vehicles need to agree to a single point on the vehicle as the reference point. Without such a point, the reported position for each vehicle could vary by meters depending on the size of the vehicle and the point on the vehicle that the message is reporting. Thus, we are

[140] See "Leap Seconds" http://www.endruntechnologies.com/leap.htm (last accessed Dec 12, 2016)

providing a proposed definition for a vehicle reference point—based upon which the agency would evaluate the compliance of the vehicle location information in the basic safety message.

Our proposal is to define the vehicle reference point as the theoretical point projected on the surface of the roadway that is in the center of a rectangle oriented about the vehicle's axis of symmetry front-to-back. This rectangle encompasses the farthest forward and rearward points and side-to-side points on the vehicle, including original equipment such as outside side view mirrors on the surface of the World Geodetic System-84 (WGS-84) ellipsoid (see Figure III-8). The position reference is obtained from measurements taken when the vehicle is situated on level ground/roadway, i.e. where there is no difference in grade in any direction and all tires contact the ground/roadway evenly. This position provides the BSM position reference of the center of the vehicle along all axes that can be used to determine the outer perimeter of the vehicle in relation to vehicle movement. The position reference is also used to configure the GPS antenna if the antenna cannot be placed at the vehicle's center point.

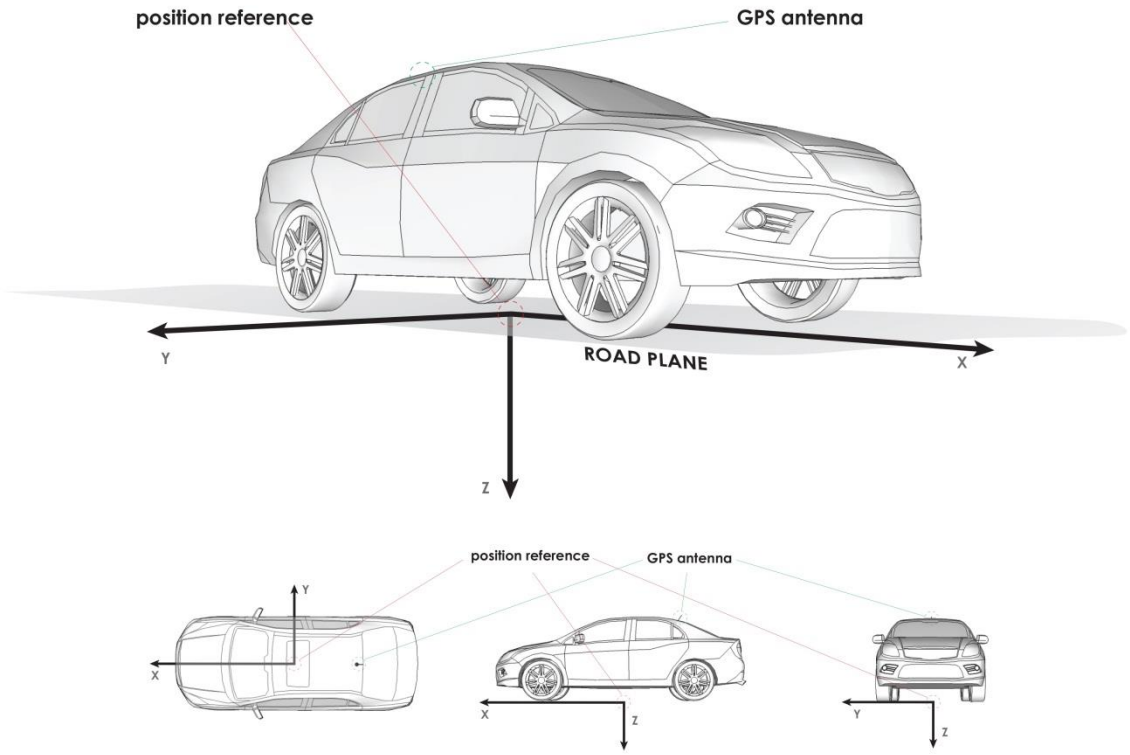

Figure III-8 Vehicle Positioning in World Geodetic System-84 (WGS-84) ellipsoid

(ii) Longitude and Latitude

Longitude and latitude position would require that vehicles report a position that is within 1.5 m of their actual position at a Horizontal Dilution of Precision (HDOP)[141] less than or equal to 1.5 within the one sigma absolute error. For the 2D location we tentatively believe that 1.5 m is appropriate because it is half of the width of a lane of traffic. Therefore, if vehicles provide position data within this level of accuracy, safety applications should be able to determine whether another vehicle is within its lane of travel. Further, the requirement to stay within the 1.5 m of tolerance at an HDOP smaller than five, within the one sigma absolute error, accounts for some of the variation in position that may occur with GPS due to failure to receive signals from a sufficient number of satellite signals.[142] If the HDOP is larger than five, there is a high probability that the accuracy of the position of the vehicle will not be accurate enough to support the 1.5m of position. As we anticipate that most vehicles, if not all vehicles, will use GPS to ascertain their location, we currently believe that it is appropriate to account for this potential error in our proposed location requirement in the basic safety message. Our engineering judgment is that an HDOP smaller than five within the one sigma absolute error appropriately accommodates the potential variation in GPS and provides a monitoring function that can be measured to determine if the GPS within the DSRC device can calculate a position at an accuracy level that supports the 1.5m relative position accuracy needed for DSRC crash avoidance.

(iii) Elevation

Due to the different situations in which elevation is relevant, vehicles would be required to report elevation in the basic safety message with an accuracy of three meters—rather than 1.5.[143] In terms of elevation, our tentative belief is that the information does not need to be as exact as the longitude and latitude location. Our proposal currently uses three meters (approximately 10 feet) because it provides sufficient distance to distinguish between a vehicle crossing an overpass versus those that are on the same level as the vehicle with a safety application. Further, our current judgment is that reporting the elevation with greater specificity

---

[141] HDOP is a measure of the geometric quality of a GNSS satellite configuration in the sky. HDOP is a factor in determining the relative accuracy of a horizontal position based on the number of visible satellites. The smaller the DOP number, the better the geometry and accuracy. HDOP less than 5 is a general rule of indicating a good GNSS condition that can provide the desired level of accuracy. However, a lower DOP value does not automatically mean a low position error. The quality of a GPS-derived position estimate depends upon both the measurement geometry as represented by DOP values, and range errors caused by signal strength, ionospheric effects, multipath, etc.

[142] As noted above, there are other factors that may lead to degradation of the GPS information—e.g., ionospheric interference, multipath, etc.

[143] We would measure the elevation data element under the same conditions as the longitudinal/lateral data element—i.e., the accuracy needs to be 3m when the HDOP is less than 5 within the 1 sigma absolute error.

would be counter-productive for certain safety applications. The elevation should be relative to each vehicle being interacted with within 300M. A tolerance of 3m (10ft) provides for low bridges but takes into account changes in grade that change as vehicles close on each other. Therefore, in specifying the elevation tolerance, we tentatively believe that we are balancing the competing safety interests.

(d) Movement

In addition to knowing the vehicle's position, a safety application should also consider the characteristics of that vehicle's movement. Rather than extrapolating these characteristics (with less accuracy) based on the position information, safety applications currently under development already consider movement information about the surrounding vehicles in determining whether a crash-imminent situation exists. For the basic safety message, we tentatively believe that speed, heading, acceleration, and yaw are the most relevant pieces of information about a vehicle's moment.

We are proposing characteristics for message content related to speed, heading, acceleration, and yaw rates. Essentially, we propose to measure the rate at which the sending device's location is changing and also any changes to that rate at which a device's location is changing. Because a safety application is generally concerned with the potential future locations of the device (rather than just its present location), it is likely that safety applications will utilize this type of information.

For example, through combining the speed and heading information with a devices's current location, a safety application can calculate whether a surrounding vehicle can collide with the safety application's vehicle. Further, having information about the vehicle's acceleration will make that prediction more accurate because it tells a safety application whether the vehicle is speeding up or slowing down. Yaw rate also affects the predicted location of the vehicle because it measures the rate at which the vehicle's direction is changing (i.e., the rate at which the vehicle's face is pivoting towards the left or the right). The tendency of the vehicle to change direction during its travel (like acceleration) also affects the ability of a safety application to predict its location.

(i) Speed

We are proposing that vehicles report their speed in the basic safety message accurate to within 0.28 m/s (1 kph). We tentatively believe that this is the appropriate accuracy for the Speed data element based on the agency's experience in the Safety Pilot Model Deployment, where systems reporting speed information accurate to within 1 kph effectively supported the tested safety applications. We are not aware of any instances during the Model Deployment where an application warned at the incorrect time (i.e., false positive) or failed to warn (i.e., false negative) due to any inaccuracies in the Speed data element. As the available information indicate that the 1 kph tolerance requirement is technically feasible and that it supports the safety applications, we tentatively believe that it would also be an appropriate requirement for a final regulation.

We note that the basic safety message requirements in SAE J2735 state that the speed is reported in increments of 0.02 mph. We currently believe that it is appropriate, in addition to the tolerance of 1 kph established above, to also specify the incremental units to be used by the vehicle in reporting its speed. While it may not be technically feasible to report the speed information with a tolerance of only 0.02 mph, we believe that (by requiring the vehicle to report speed in incremental units of 0.02 mph) we can capture better information about the vehicle's change in speed. Further, by establishing these consistent requirements, vehicles will be able to better rely on the information they are receiving from the surrounding vehicles. As with our rationale for the tolerance of 1 kph in the preceding paragraph, our rationale for proposing that vehicles report the speed information in increments of 0.02 mph is based on our experience in the Safety Pilot testing. In the Safety Pilot, vehicles reported information using these specifications and it provided effective information for the safety applications tested in that program.

We request comment on these tentative conclusions. Is there any data that suggest that the agency should adopt a different tolerance level for the speed information reported in the basic safety message? Is there similar data for the incremental values for reporting speed that we propose to require?

(ii) Heading

Heading in relation to BSM and crash avoidance is defined as the "actual" heading in relation to the vehicle position reference point (explained above) that indicates the course of the vehicle's motion regardless of the vehicle's orientation to that motion, i.e. where the front of the vehicle is pointing. Knowing the "actual" vehicle heading is needed in order to accurately identify conflict and imminent crash situations.

For Heading, the agency would require different levels of accuracy based on the vehicle's speed. We tentatively believe that this is appropriate because we anticipate that most vehicles will be determining vehicle heading using GPS information. We recognize that the accuracy of GPS-determined heading varies based on speed. We also tentatively believe that heading information might not be as critical at lower speeds. Therefore, we believe it is appropriate to provide more flexibility at lower vehicle speeds. Thus the requirements for heading need to support V2V crash avoidance would read as follows:

- when the vehicle speed is greater than 12.5 m/s (~ 28 mph), it is required to report vehicle heading accurately to within 2 degrees; and
- when the vehicle speed is less than or equal to 12.5 m/s, it is required to report the vehicle heading accurately to within 3 degrees.

We tentatively believe that 2 degree accuracy for speeds above 12.5 m/s is appropriate because research indicates that at approximately 12.5 m/s (28 mph) sensors and vehicle dynamics can accurately report heading within 2 degrees. At speeds less than 12.5 m/s the research indicates that the sensors and vehicle dynamics cannot reliably report vehicle heading within 2 degrees, but can reliably and accurately report within 3 degrees of accuracy. Given that

at lower speeds vehicles travel less distance and driver-initiated evasive actions can be more effective at the lower speeds, our tentative conclusion is also that a three degree accuracy is appropriate for speeds below 12.5 m/s.

In addition to providing different requirements for accuracy at different speeds, we tentatively believe it is appropriate to require that vehicles "latch"[144] the GPS information at very low vehicle speeds. In other words, when the vehicle speed is very low (and a GPS cannot accurately determine the heading) we are proposing to require that the basic safety message transmit the last heading information prior to the vehicle dropping below a given speed.

In this case, the agency is proposing to require the system to latch the heading when the vehicle drops below 1.11 m/s (~ 2.5 mph). We tentatively believe that 1.11 m/s is an appropriately low threshold where, at speeds lower than 1.11 m/s, the heading information is not as crucial because the vehicle is not changing its location at a significant pace. For reference, a NHTSA 2006 study measured the idling speed of the vehicles (i.e., speed when vehicle is in gear and no brake or throttle is being applied). Of the vehicles that NHTSA measured in that study, the idling speed ranged from 4.0 mph to 7.0 mph.[145]

Further, the agency is proposing to require vehicles to unlatch their heading information (and transmit a heading value that is within 3 degrees of its actual heading) when its speed exceeds 1.39 m/s[146] (~ 3.1 mph). As a vehicle's speed increases towards its idling speed, we propose requiring that the vehicle calculate its heading and report that information in the basic safety message.

(iii) Acceleration

For Acceleration, the agency would require vehicles to report horizontal (longitudinal and lateral) acceleration with an accuracy of 0.3 m/s^2 and vertical acceleration to 1 m/s^2. The requirement is based on the need to provide accurate and timely safety alerts for the crash scenarios and corresponding potential safety applications identified in Table III-2. The requirement was obtained by extensively testing commercially-available equipment and automotive sensors in a wide variety of driving environments, and the numbers were proven to

---

[144] "Latch" in this context refers to a software operation that holds a value in memory and attached to a specific variable as long as a specified condition is reached and maintained.

[145] *See* Mazzae, E.N., Garrott, W.R., (2006) Experimental Evaluation of the Performance of Available Backover Prevention Technologies. National Highway Traffic Safety Administration, DOT HS 810 634.

[146] The speed threshold for unlatching the vehicle heading is different from the speed threshold for latching. The reason for the latching speed to be lower than the unlatching speed is because a system should not need to latching and unlatch the vehicle heading repeatedly when the vehicle speed is hovering around a given threshold speed (e.g., 1.11 m/s). By having different (but similar) speeds for latching and unlatching, the system will be able to latch the speed once when the vehicle is decelerating and unlatch once when the vehicle is accelerating without having to repeat the action multiple times if there are vehicle speed fluctuations during the vehicle's general acceleration or deceleration trend.

be reasonable based on the equipment and sensor capabilities, while also supporting safety alerts from the appropriate safety application at timings that would enable a driver reaction sufficient to avoid the corresponding crash scenario.

(iv) Yaw Rate

Finally, for Yaw Rate, the agency would require vehicles to report this information to an accuracy of 0.5 degrees per second. The requirement is based on the need to provide accurate and timely safety alerts for the crash scenarios and corresponding potential safety applications identified in Table III-2. The requirement was obtained by extensively testing commercially-available equipment and automotive sensors in a wide variety of driving environments, and the numbers were proven to be reasonable based on the equipment and sensor capabilities, while also supporting safety alerts from the appropriate safety application at timings that would enable a driver reaction sufficient to avoid the corresponding crash scenario.

Table III-2 Potential Safety Applications Reliant on Acceleration and Yaw Rate Information

	EEBL	FCW	BSW/ LCW	IMA	LTA	CLW

Lead Vehicle Stopped		✓				
Control Loss without Prior Vehicle Action						✓
Vehicle(s) Turning at Non-Signalized Junctions				✓	✓	
Straight Crossing Paths at Non-Signalized Junctions				✓		
Lead Vehicle Decelerating	✓	✓				
Vehicle(s) Changing Lanes – Same Direction			✓			
Left Turn Across Path – Opposite Direction					✓	
Lead Vehicle Stopped		✓				
Control Loss without Prior Vehicle Action						✓
Vehicle(s) Turning at Non-Signalized Junctions				✓	✓	
Straight Crossing Paths at Non-Signalized Junctions				✓		
Lead Vehicle Decelerating	✓	✓				
Vehicle(s) Changing Lanes – Same Direction			✓			
Left Turn Across Path – Opposite Direction					✓	

(e) Additional Event Based Information

In addition to the information discussed thus far, the agency would require additional data conveying the transmitting vehicle's path history, future predicted path, and exterior lights status to also be transmitted as part of the Vehicle Safety Extension (Part II) for V2V safety communications. The data element, Event Flags, shall also be transmitted as long as a defined event is active. For exterior lights status and other, similar data where access to the vehicle databus may be necessary, the agency assumes all integrated devices will have access this information. Aftermarket, standalone devices may or may not be able to access this information.

(i) Path History

Path history, which provides an adaptable, concise representation of a vehicle's recent movement over some period of time and/or distance, consists of a sequence of positions selected to represent the vehicle's position within an allowable error. The path history can be used not only by safety applications on the transmitting vehicle, but also by other vehicles, which can use this information to predict the roadway geometry and for target vehicle classification with reference to the roadway.

For the Path History (PH) data frame, the agency would require that the vehicle use a history of its past GNSS locations (as dictated by GNSS data elements including UTC time, latitude, longitude, heading, elevation, etc.), sampled at a periodic time interval (typically, 100 ms) and interpolated in-between by circular arcs, to represent the vehicle's recent movement over a limited period of time or distance.

Path history points should be incorporated into the Path History data frame such that the perpendicular distance between any point on the vehicle path and the line connecting two consecutive PH points shall be less than 1 m. In this way, the points present in the path history will concisely represent the actual path history of the vehicle based on the allowable position error tolerance (1 m) between the actual vehicle path and its concise representation. Objective testing of applications as part of the VSC-A Project showed that a PH error tolerance of 1 m satisfies the needed accuracy for target vehicle classification and meets the performance requirements of the safety applications that were developed and demonstrated.

For the subset of the available vehicle path position data elements, a minimum number of PH points necessary to satisfy the required error tolerance between the vehicle path and its PH representation (1 m) should be selected to populate the Path History data frame. Populating the Path History data frame with the minimum number of PH points possible offers significant savings in over-the-air wireless bandwidth when transmitting the PH information to other vehicles wirelessly. Additionally, vehicles should report the minimum number of PH points so that the represented PH distance (i.e., the distance between the first and last PH point) is at least 300 m and no more than 310 m, unless initially there is less than 300 m of PH. We believe that this range is appropriate because the operational range for DSRC is approximately 300 m, and the maximum required signal range for safety applications currently under development is 300 m. However, if the number of PH points needed to meet both the error and distance requirements stated above exceeds the maximum allowable number of points (23), the Path History data frame shall be populated with only the 23 most recent points from the computed set of points. Effectively, the distance requirement shall be relaxed in order to reduce over-the-air bandwidth.

Lastly, to ensure the most accurate representation of the vehicle's current trajectory, the Path History data frame shall be populated with time-ordered PH points, with the first PH point being the closest in time to the current UTC time, and older points following in the order in which they were determined. And, so as to permit safety applications to operate properly, the Path History data frame shall not include any additional data elements/frames in the BSMs intended for vehicle safety communications.

(ii) Path Prediction

Not only is it important to determine where a vehicle has been, it is also useful for safety applications to know where a vehicle is headed, or its future path. This future trajectory estimation can significantly enhance in-lane and out-of-lane threat classification.

Trajectories in the Path Prediction (PP) data frame are represented, at a first order of curvature approximation, as a circle with a radius, R, and an origin located at (0,R), where the x-axis is aligned with the transmitting vehicle's perspective and normal to the vehicle's vertical axis. The vehicle's (x,y,z) coordinate frame follows the SAE convention. The radius, R, will be positive for curvatures to the right when observed from the transmitting vehicle's perspective, and radii exceeding a maximum value of 32,767 are to be interpreted as a "straight path" prediction by receiving vehicles.

The radius, R, can be derived using various means, including map databases, vision systems, global positioning, etc. Alternatively, simple physics equations can be used to compute a curvature based on instantaneous dynamics information (vehicle speed and rate of change of heading, or yaw rate) provided by the vehicle. This curvature can then be extrapolated forward (as a continuous radius of curvature) to provide an estimate of the vehicle's likely intended future trajectory, or path. To minimize the effect of sensor noise and in-lane driver wandering, however, it is also necessary to use low-pass filtering techniques (time constant greater than 2 ms typically) in instances where the radius is derived from instantaneous vehicle information, such as from rate sensors and velocity.

Confidence in the predicted path based on the rate of change of the vehicle dynamics can also be computed in order to infer non-steady-state conditions, such as those stemming from lane changes, curve entry and exit points, curve transitions, and obstacle avoidance, where large changes in vehicle yaw rate occur over a short period of time. In such situations, path estimations may be largely inaccurate and, as such, confidence levels would be low. Conversely, a high confidence value would be reported during steady-state conditions (straight roadways or curves with a constant radius of curvature).

When a deviceis in steady state conditions over a range from 100 m to 2,500 m in magnitude, the agency is proposing to require that the subsystem populate the PP data frame with a calculated radius that has less than 2% error from the actual radius. The agency believes that this range and error rate is appropriate to ensure the effectiveness of safety applications that rely on such information. For the purposes of this performance requirement, steady state conditions are defined as those which occur when the vehicle is driving on a curve with a constant radius and where the average of the absolute value of the change of yaw rate over time is smaller than 0.5 deg/s^2.

After a transition from the original constant radius (R1) to the target constant radius (R2), the subsystem shall repopulate the PP data frame within four seconds under the maximum allowable error bound defined above.

Lastly, when the transmitting vehicle is stationary, we propose requiring that a device report a "straight path" radius of value 32,767 and confidence value of 100%, which corresponds to a value of 200 for the data element.

(iii) Exterior Lights

For the Exterior Lights data element, the agency is proposing to require that the subsystem shall set the individual light indications in the data element to be consistent with the vehicle status data that is available. If meaningful values are unavailable, or no light indications will be set, the data element should not be transmitted.

The data element, Exterior Lights, provides the status of all exterior lights on the vehicle, including parking lights, headlights (including low and high beam, and automatic light control), fog lights, daytime running lights, turn signal (right and left), and hazard signals. This information can be used not only to enhance the operation of safety applications running on the transmitting vehicle, but it can similarly be used by other vehicles within range of receiving messages sent by the transmitting vehicle.

(iv) Event Flags

The data element, Event Flags, conveys the sender's status with respect to safety-related events such as antilock brake system (ABS) activation, stability control activation, hard braking, and airbag deployment, among others. Similar to that mentioned for the Exterior Lights data element, the additional information conveyed in the Event Flags data element can serve to augment the other BSM information used by applications when determining whether to issue or suppress warnings. Furthermore, because the inclusion of the Event Flag data element suggests that an unusual, safety-related event has occurred, vehicles receiving a message containing an Event Flag element may choose to process it differently than a message that does not.

The Event Flags and respective criteria the agency proposing to require in the BSM are defined in SAE J2735 as follows:

- ABS Activation: The system is activated for a period of time exceeding 100 ms in length and is currently active.
- Stability Control Activation: The system is activated for a period of time exceeding 100 ms in length and is currently active.
- Hard Braking: The vehicle has decelerated or is decelerating at a rate of greater than 0.4 g.
- Air Bag Deployment: At least one air bag has been deployed.
- Hazard Lights: The hazard lights are currently active.
- Stop Line Violation: The vehicle anticipates that it will pass the line without coming to a full stop before reaching it.
- Traction Control System Activation: The system is activated for a period of time exceeding 100 ms in length and is currently active.
- Flat Tire: The vehicle has determined that at least one tire has run flat.
- Disabled Vehicle: The vehicle considers itself to be disabled.
- Lights Changed: The status of the external lights on the vehicle has changed recently.

- Wipers Changed: The status of the front or rear wipers on the vehicle has changed recently.
- Emergency Response: The vehicle is a properly authorized public safety vehicle, is engaged in a service call, and is currently moving. Lights and/or sirens may not be evident.
- Hazardous Materials: The vehicle is known to be carrying hazardous materials and is labeled as such.

If a stated criterion is met, the sender shall set the Event Flag to 1. If, and only if, one or more of the defined Event Flags are set to 1, the subsystem shall transmit a BSM with the corresponding Event Flags within 250 ms of the initial detection of the event at the sender. The Event Flags data element shall be included in the Vehicle Safety Extension data frame for as long as an event is active. Messages containing Event Flags may also include related optional data. When one or more criteria associated with an event are no longer satisfied, the sender shall set the flag to zero in any Event Flag data element that it sends.

The agency is requesting comment on the appropriateness of each of the Event Flags and corresponding criteria described above.

(f) Vehicle based motion indicators

In addition to describing the location and the motion of vehicles, the device can use other pieces of information to verify state and motion, if the device has access. The agency assumes all integrated devices will have access this information. Aftermarket, standalone devices may or may not be able to access this information. This type of information in the basic safety message can collectively identify operational status and motion that can be used to confirm calculated position and future position of surrounding vehicles. Thus, it helps safety applications determine whether a potential crash imminent situation could exist.

Two pieces of information help fulfill this objective. They are the Transmission State and Steering Wheel Angle data elements. The Transmission State provides an indication concerning the operational direction of the vehicle in relation to its reference point. This information puts the speed, heading, location, etc. information into context. The steering wheel angle (which is not the same as the vehicle heading because this indicates the direction of the steering wheel control itself and not the vehicle) is a data element that indicates which way the wheels are turned, providing another possible indication of direction (in some cases the vehicle's wheels can be turned, however, the vehicle could be skidding in a different direction.).

(i) Transmission State

This data element would require that vehicles report whether they are in a gear in the forward or reverse (or neutral) direction. We tentatively believe that the relevant information for a safety application is whether the vehicle is in gear to begin moving; and if so, whether it will do so in the forward or reverse direction. Thus, our proposal currently does not include any requirement for reporting the gear ratios of the vehicle.

(ii) Steering Wheel Angle

This data element would require that vehicles report the direction of the steering wheel angle to within 5 degrees of the actual steering wheel angle. Here, we are seeking to use another element to confirm actual heading of the vehicle. Thus, the Steering Wheel Angle data element describes the movement of the steering wheel itself (i.e., it does not consider how such movement would affect the direction of the tires). Taking into account steering wheel angle provides a check of the position and motion calculations based on the actual state of the vehicle. We tentatively believe that expressing the steering wheel angle to an accuracy of 5 degrees is sufficient because we believe that a 6 degree change in steering wheel direction provides an indication of vehicle direction.[147] In other words, steering wheel angle changes of less than 6 degrees can be small adjustments in steering used to maintain current heading. However, steering wheel angle changes greater than 6 degrees result in a measurable change in actual heading of the vehicle. Thus, we tentatively conclude that an accuracy of 5 degrees would be sufficient to confirm (check plausibility) actual heading of the vehicle; i.e. if the actual heading is left are the wheels also turned to the left.

(g) Vehicle Size

This data element is also an element that is fundamental for a safety application's determination of whether a crash scenario might occur. In addition to knowing where a vehicle is, the characteristics of its motion (to predict where the vehicle will be in the near future), and some aspects of the driver's intent, a safety application needs to know how large the vehicle is in order to know whether a crash might occur. However, we also acknowledge that this data element has more potential privacy impacts than other data elements. As further discussed in this document, the V2V information environment uses multiple strategies to omit as much potentially identifying information as possible in the basic safety message, security credentials, etc. However, we acknowledge that if the vehicle size information is too specific, it could potentially facilitate an effort to identify basic safety messages to a particular vehicle over time. The agency believes the performance metric for this data element balances not only the safety need for accurate information about the vehicle size, but also the privacy needs of the driver.

Thus, we tentatively believe that having a 0.2 m tolerance is an appropriate balancing of those competing interests. This level of specificity meets the need to identify the physical extent of the vehicle for crash avoidance given that vehicle size is to be rounded up which will still provide for the appropriate calculation of a warning such that the driver can take appropriate action to avoid a crash. The additional size for some vehicles will only present an insignificant

[147] NHTSA's past research used 6 degree changes in steering input to indicate a situation in the research project where the test driver intended to conduct a maneuver. *See* NHTSA Light Vehicle Antilock Brake System Research Program Task 5.2/5.3: Test Track Examination of Drivers' Collision Avoidance Behavior Using Conventional and Antilock Brakes, DOT HS 809 561, March 2003, page 32.

amount of additional warning time (0.0022 seconds at 25 mph to 0.007 seconds at 65 mph using a 3 second time to collision baseline) that will be transparent to all drivers.

In addition to considering different tolerances for the vehicle length and width data elements, another option is to use vehicle size categories or only express the vehicle length and width in increments of a given value. For example, requiring that the vehicle length be expressed in only increments of 0.2 m would mean that a vehicle with a 10.12 m length and a vehicle with a 10.01 m length would have the same value of 10.2 for the vehicle length in the basic safety message. This type of requirement could have the advantage of aggregating many different vehicles into particular size categories and potentially help discourage identifying a basic safety message to a particular vehicle. We request comment on these potential options (i.e., not only the potential tolerances for these data elements but also the potential to use size categories).

(h) Optional Data Elements

SAE J2735 also contains a variety of additional data elements that the agency is not proposing requirements for in this notice. We tentatively believe that these data elements are elements that may be useful in safety applications that may be used by various suppliers to enhance the operation of an application to issue a warning or suppress a warning. While these data elements will add more information on a status of the vehicle (especially with regard to whether a vehicle is under control), we do not currently have enough information to determine how such information might be applied to an application and thus tailor such information to that application (or applications). Thus, we tentatively believe it is premature to propose requirements for these data elements but are preserving the possibility for these data elements to potentially be employed to ensure future interoperability as technology evolves. The agency is proposing to require that devices either adhere to SAE J2735 for these data elements, or transmit the "unavailable" data value for each of these elements (in accordance with SAE J2735) These data elements are:

- Brake applied status
- Traction control state
- Stability control status
- Auxiliary brake status
- Antilock brake status
- Brake boost applied
- Location Accuracy

(i) Excluded Data Elements

When identifying the data elements to include in the BSM, the agency considered those that would be needed to support possible future applications and the suppression of warnings to reduce the number of false positive warnings. The use of some applications may be limited only

to authorized vehicles – for example, only law enforcement and emergency vehicles might have access to an application providing traffic signal priority or pre-emption for emergency or enforcement purposes. To support identification of authorized vehicles, the agency considered including in the BSM optional elements such as the Vehicle Identification Data Field, which includes: VIN string, Owner code, Temporary ID, and Vehicle type. These data elements could identify and verify an emergency or law enforcement vehicle to a traffic control device for signal preemption purposes. However, our privacy experts identified VIN and other data elements directly linked to specific private vehicles and their owners as potential sources of privacy risk to individuals.

To help reduce the privacy risk that could stem from the transmission of information that could be used to associate V2V messages with individual consumers, our proposal excludes certain data elements from transmission as part of the BSM. Specifically, V2V transmissions via DSRC or any future interoperable V2V communications technology may not include data directly identifying a specific private vehicle or individual regularly associated with it, or data reasonably linkable or linkable, as a practical matter, to an individual.[148] NHTSA intends for the terms "reasonably linkable" and "as a practical matter linkable" to have the same meaning, specifically: capable of being used to identify a specific individual on a persistent basis without unreasonable cost or effort, in real time or retrospectively, given available data sources.

NHTSA seeks comment on these tentative conclusions. Specifically, we request comment on our proposed exclusion from the BSM of data elements that directly identify, or are reasonably linkable or linkable as a practical matter, to a private individual. Do commenters have thoughts on whether, as a practical matter, any data element (or combination of data elements) currently proposed as part of the BSM is reasonably linkable to an individual on a persistent basis? We seek comment on whether this aspect of NHTSA's proposal appropriately balances consumer privacy with safety – or whether, by declining to identify definitively those data elements that are, or may be, "reasonably linkable" to an individual (and therefore must be excluded from the BSM under NHTSA's proposal), NHTSA will undermine the NPRM's overarching goal of establishing a standardized data set for the BSM and providing adequate data for safety applications.

(2) Proposed BSM Data Initialization Requirements

In addition to the content of the basic safety message, we are aware that participants in the V2V Safety Pilot have included data persistency performance in their on-board V2V systems in order to minimize the time needed for vehicles to begin transmitting basic safety messages after the vehicle starts up.

---

[148] See FN 3 above.

The advantage of doing so is that when the vehicle starts up, it already has information about its last known location, heading, etc. that was accurate when it shut down. The premise is that upon device startup, the device could begin transmitting sooner rather than waiting for new information, such as receiving a new heading or calculating path history, both of which would require the device to acquire GPS data and start moving. In many instances, this would reduce the time to initialize the first (after startup) transmission of the BSM. As the vehicle most likely did not travel while it was shut down, the information it saved during shut down should still be accurate upon startup. However, there could be scenarios when the last known heading and path history will be inaccurate, such as when parking "head" or "tail" in (higher frequency) or if the vehicle has been towed (hopefully, very low frequency).

NHTSA recognizes that the practice of saving vehicle data over vehicle on-off-on events is typically used to enhance feature performance, improving consumer acceptance. However, NHTSA does not believe at this time that a minimum requirement for data persistency is needed, nor that we need to identify specific data elements that should be stored upon shutdown and retrieved at startup.

Based on the available information, we currently agree with the research to date that minimizing the time it takes for a vehicle to begin transmitting the basic safety message is desirable as it helps ensure that vehicles will be providing information into the V2V environment as soon as possible after they begin moving. We also agree with the research to date that including data persistency performance in vehicle V2V systems is a good way to accomplish this task.

Instead, the agency's proposal would require that vehicles begin transmitting basic safety messages within a specified amount of time after startup without specifying the method that a manufacturer would choose to meet that requirement. While a manufacturer may use data persistency techniques to meet the performance requirement, we believe that this method for achieving the safety goal appropriately gives the manufacturer more design flexibility.

While the basic safety message transmitted from one vehicle can be useful to other vehicles when the vehicle is stationary, we currently believe that (at a minimum) the vehicle should begin transmitting basic safety messages at a time when we might reasonably expect people to begin driving their vehicle after getting into it. In other words, our current thinking is that the vehicle should begin transmitting before the vast majority of drivers begin driving the vehicle.

The proposed requirements are that a vehicle shall begin transmitting the basic safety message within 2 seconds after a vehicle key on event has occurred. This proposed requirement is based on the final performance requirement associated with FMVSS No. 111 for rear visibility systems. While a V2V system and rear visibility system are not identical, the agency believes the research and decisions leading to finalizing the two second system startup requirements are fungible to V2V and the overarching safety goal.

In NHTSA's rear visibility rulemaking, our naturalistic driving data indicated that 90% of drivers do not select reverse and begin the backing maneuver less than 4.25 seconds after opening the vehicle door.[149] While in this case, the safety technology proposed for the vehicle is not one that would only be used when the vehicle is traveling in reverse, we believe that the data is a reasonable proxy for when drivers would put the vehicle in gear (forward or reverse) and begin driving. Since our safety goal in this situation is to ensure that the vehicle is transmitting the basic safety message before the vehicle begins to move, we believe that using a performance requirement based on the rear visibility rule's image response time requirement (and test procedure) would be appropriate.

While based on FMVSS No. 111, this proposed requirement for V2V initialization time would need to adjust the test procedure in a few ways to account for the characteristics of a vehicle's V2V system. First, we note that vehicle's V2V system needs to be active whether the vehicle is moving in reverse or moving forward. Thus, the test procedure and requirements should not be based solely on reverse gear. Second, while the temperature condition of the test would affect the rear visibility system display's response time, the temperature condition is not as relevant for a vehicle's V2V system. Instead, the test should specify environmental conditions that approximate the level of access to characteristics of its surrounding environment that a vehicle would normally have to populate the information in the basic safety message (e.g., open sky access to GPS signals, potential saved location/heading information from the basic safety messages prior to vehicle shutdown, etc. Thus, the preconditioning test applied to the vehicle would need to be modified in these ways.

In summary, NHTSA is proposing to require that, after a conditioning procedure, vehicles begin transmitting basic safety messages with the required content and at the required frequency within 2.0 seconds after the driver puts the vehicle into the forward or reverse gear. The conditioning procedure would specify that the vehicle is under open sky conditions as in our test procedure for evaluating the content of the basic safety message. Then the procedure would specify that the test technician:

- drives the vehicle in any heading at any speed for five minutes;
- stops the vehicle and deactivates the vehicle for any amount of time between 30 minutes to an hour;
- checks to ensure that the V2V system components are in a powered off state;
- opens the driver's door to any width,
- closes the driver's door;
- activates the starting system using the key; and
- selects any gear (forward or reverse) at any time not less than 4.0 seconds and not more than 6.0 seconds after the driver's door is opened. The driver door is open

[149] *See* 79 FR 19220.

when the edge of the driver's door opposite of the door's hinge is no longer flush with the exterior body panel.

We acknowledge that this procedure may not be representative of a small number of real-world scenarios. For example, if a vehicle is in a parking structure like a garage, it might not have access to open skies. However, for these instances we do not think that there is any practicable way for the vehicle to ascertain its position quickly using GPS. Thus, we cannot determine a way to ensure that a test specifying those conditions would be a practicable test. We also note that the proposed procedure does not include moving the vehicle between shut down and startup. While vehicles might be moved when shut off, we think those are special circumstances (e.g., when the vehicle is towed). Those conditions are a small portion of real-world scenarios and they are situations where the driver is likely to spend more time with the car active before encountering other vehicles (e.g., when starting up in a towed vehicle lot, the vehicle may not interact with other moving vehicles until it reaches the roadway).

We request comment on our proposal for helping to ensure that vehicles begin broadcasting basic safety messages before a vehicle begins to move. More specifically, NHTSA requests comments in relation to whether a data persistency requirement is needed, and specifically in relation to:

- Supporting the interoperability of V2V devices;
- The performance of BSM transmission and how data persistency can be used to properly reduce the time of the initial transmission; and
- The possible impacts to crash avoidance functionality.

Please provide any supporting evidence that the agency can used to make an informed decision.

(3) Summary Table of BSM Content Requirements

Table III-3 Summary of BSM Content Requirements[150]

Requirement	Proposal	Basis	Applicable Standards	Reason
Message Packaging	Message ID – (2) for BSM Message Count – sequence No. Temp ID – random No. from specific	Preliminary elements need to ID, process, and sequence BSMs	SAE J2735	Allows device to interpret message and obtain safety information.

[150] NHTSA intends for the BSM Content Requirements identified in Table III-3 to be in accordance with the proposal's overarching requirement that BSMs may not contain data elements linked or reasonably linkable to an individual.

	device			
Time	Use UTC standard to set time	UTC is accepted standard for setting universal system time	SAE J2735, J2945/1	Need time standard to related messages to time critical conflict situations
Position (Longitude & Latitude)	Longitude and Latitude within 1.5m of actual position at HDOP < 5 and 1 sigma absolute error	Per CAMP research to develop relationship between measurable absolute position and relative position	SAE J2735, J2945/1	Provides for accurate relative vehicle position need to support crash avoidance – (CAMP
Position (Elevation)	3m (10 feet) (more difficult to calculate than lat/long)	Accurate elevation reduces false positives - SPMD	SAE 2735, J2945/1	3m provides for low bridges and changes in grade for crash avoidance
Movement (Speed)	Accurate within 0.28 m/s (1 kph)	Same as EDR rule – tighter accuracy then identified by CAMP. Changed to be consistent with existing standard	SAE J2735, J2945/1	The setting is based on the need to provide accurate and timely safety alerts. The setting was obtained by extensively testing commercially available equipment and automotive sensors in a wide variety of driving environments.
Movement (Heading)	Speed > 12.5 m/s accuracy within 2 degree – Speed > 12.5 m/s within 3 degrees	Research indicates that above 12.5 m/s sensors and vehicle dynamics can support 2 degrees – under 12.5 m/s can support 3 degrees.	SAE J2735, J2945/1	Same as above
Movement (Acceleration)	Longitudinal & Lateral accuracy 0.3 m/s^2 - Vertical accuracy 1 m/s	CAMP research and testing	SAE J2735, J2945/1	Same as above
Movement (Yaw rate)	Accuracy within 0.5 degrees per second	CAMP	SAE J2735, J2945/1	The setting is based on the need to provide accurate and timely safety alerts. The setting was obtained by extensively testing commercially available equipment and automotive sensors in a wide variety of driving environments.
Vehicle Motion Indicator (Transmission)	Report if vehicle is in forward or reverse gear, or neutral	CAMP	SAE J2735, J2945/1	Same as above
Vehicle Motion Indicator (Steering Wheel Angle)	Report the direction of steering wheel angle within 5 degrees of actual	CAMP	SAE J2735, J2945/1	Same as above

Vehicle Size	Vehicle length and width within 0.2m tolerance	CAMP and MITRE privacy research	SAE J2735, J2945/1	Balance the need to know the physical extent of the vehicle for crash avoidance and still protect privacy
Excluded Data Elements: No data elements directly or, as a practical matter, linkable to a specific individual or vehicle (including but not limited to VIN string, Owner code, Temporary ID, Vehicle Type)	Mandate that these optional data element cannot be populated for device in privately owned light vehicles.	MITRE privacy research	SAE J2735, J2945/1	To protect consumer privacy by reducing privacy risk
Path History	Provides concise representation of vehicles recent movements with accuracy of min 23 points and required to be transmitted with BSM	CAMP research to support crash avoidance	SAE J2735, J2945/1	Use in calculations to identify vehicle conflict situations.
Path Prediction	Perpendicular Distance – 1M; Radius error – 2%; Transmission Time 4s	CAMP research	SAE J2735, J2945/1	The setting is based on the need to provide accurate and timely safety alerts. The setting was obtained by extensively testing commercially available equipment and automotive sensors in a wide variety of driving environments.

3. Message Signing and Authentication

a) Purpose and Safety Need for Confidence in the BSM

As discussed previously, V2V safety applications can utilize the data in the basic safety message (such as position, heading, and speed) about other vehicles around it to determine whether it and another vehicle are in danger of crashing. In other words, a safety application would determine whether it is necessary to take action (e.g., issue a warning) based on the information coming from another, nearby vehicle. Even in a warning system, it is important for safety applications to have accurate information available to make their decisions. Incorrect

warnings can (at worst) directly increase safety risks and (at minimum) affect the driver's acceptance of the warning system. If the driver of a V2V-equipped vehicle receives a large number of warnings when there is no crash imminent situation (i.e., false warnings), then the driver may lose confidence and not respond appropriately when there is a true crash-imminent situation.

Thus it is important that the safety application can place as much confidence as possible in the data contained within BSM messages and detect when messages are modified or changed while in transit. To help improve the level of confidence in BSM messages the agency's primary message authentication proposal describes a Public Key Infrastructure (PKI) approach to message authentication.

In addition two alternatives are presented for comment. This first alternative for message authentication set out for comment is less prescriptive and defines a performance-basedbased approach rather than a specific architecture or technical requirement. The second alternative set out for comment stays silent on message authentication and does not specify a message authentication requirement, leaving authentication at the discretion of V2V device implementers.

b) Public Key Infrastructure Proposal

The agency is proposing to mandate requirements that would establish a message authentication approach based on a Security Credential Management System (SCMS) that uses Public Key Infrastructure (PKI) digital signatures to sign and verify basic safety messages. This would include requiring devices to sign each message, send a valid certificate with each message, and periodically obtain up-to-date security materials.

(1) How does the Public Key Infrastructure Validate Messages?

When transmitting a BSM, the sender uses a security certificate issued by a certificate authority to digitally sign each BSM. The security certificate is composed of the following elements:

- A date range describing the validity period for the certificate
- A Public key corresponding to a private key
- Digital signature from a certificate authority

When a nearby device receives a properly formed BSM, it can use the certificate included in the BSM to verify that the digital signature in the BSM is valid. Furthermore, the receiving device can also verify that the security certificate included in the BSM is valid as well. The receiving vehicle can verify that digital signature on the certificate included in the BSM is digitally signed by the certificate authority that issued it to the sending device. The receiving device should already have a copy of the authorizing certificate for the authority stored on-board. In the event that it does not, the receiving device would need to request the authorizing

certificate from the sending device. Once the authorizing certificate is obtained, the receiving device can verify that the certificate authority is valid and the certificate used to sign the BSM is also valid. This process can be repeated for any number of certificate authorities that are in the PKI hierarchy, up to the root certificate authority, which authorizes the entire system. This process allows receiving devices to verify a sender'scredentials. For detailed information on the proposed Security Credential Management System, see the following two reports:

- Hehn, T., et. al., "Technical Design of the Security Credential Management System", 2014, http://www.nhtsa.dot.gov
- Hehn, T., et. al., "Cost Model and Design Alternatives for the Security Credential Management System", 2014, http://www.nhtsa.dot.gov

The SCMS organization certifies that a device is indeed authorized to participate in the V2V environment and then issues credentials to the device. Thus, a receiving device can have more confidence in the information contained in a BSM message because it knows that the SCMS previously confirmed the sender is an approved device and issued these credentials.

In addition to the SCMS device certification, a device also needs to properly sign the basic safety message. The following sections discuss how the device utilizes the certificates from the SCMS and how the agency can confirm that devices are doing so.

(a) Signing the Basic Safety Message for Transmission

The process for signing the basic safety message involves the use of two "keys," one public and one private. [151] The signature process uses the private key and an original string of numbers as inputs to generate an encoded string of numbers (an otherwise meaningless set of numbers). The public key associated with that private key is then used by the signature verification process to reverse the signature process (i.e., take the encoded string of meaningless numbers and reverse it to generate the original string of numbers). Therefore, the receiving devices takes the information from the sending device and (using the characteristics of these equations) can verify the signature of the sender.[152]

The agency employed this signing process in V2V devices used throughout its research activities and was proven through the Safety Pilot Model Deployment activity. Devices in these activities have been signing the basic safety message and constructing the security credentials of

[151] The V2V device generates the private key & public keys. The public key is sent to the SCMS to incorporate into a certificate that is signed by the PCA. The private key is always kept secret with the V2V device. The private key is vital to the signing process and must be kept secured at all times.
[152] See "Using the Elliptic Curve Digital Signature Algorithm effectively" http://www.embedded.com/design/safety-and-security/4427811/Using-the-Elliptic-Curve-Digital-Signature-Algorithm-effectively, Feb. 2, 2014 (last accessed Dec 7, 2016)

the message by combining the message content with the certificate, the signature, and the time stamp of the information.

Table III-4 shows how the public key, private key, and signature fit together with the other parts of the basic safety message.

Table III-4 Basic Safety Message Key Components

Certificate		**Signature**	
Pseudonym Certificate ● Public Key ● Signature of the Pseudonym Certificate Authority Validity Period ● Says when certificate effective and when expires.	**Message Content** (i.e., the speed, heading, location, etc. information that supports the safety applications)	Produced from the following steps : ● Compute hash of the Message Content and Timestamp. ● Use your private key to create an encoded string of numbers. ● The encoded string of numbers is your signature.	**Timestamp** (i.e., when the information is transmitted.])

When the transmitting device sends a basic safety message it assembles each of the parts of the message in Table III-4 above. The vehicle uses a combination of the message content, timestamp, and a private key to generate the signature. The device also attaches the certificate to the message. The certificate includes the public key, corresponding to the private key used to sign the message, the validity period of the certificate, and the signature from the Pseudonym Certificate Authority. The pseudonym certificate contains the signature of the PCA from the SCMS allowing message receivers to verify the pseudonym certificate. The validity period is used to determine if the certificate is valid or if the receiving device should reject the credentials if they are expired.

The vehicle constructs the signature by using the message content and the time stamp portions of the message as inputs into the following process:

(a) Create a hash[153] of the message content and timestamp (i.e., a shortened version of the message content/time stamp that is fixed length--e.g., 32 characters). A standard NIST formula (SHA-2)[154] governs the creation of the hash.
(b) Input the hashed contents through an Elliptical Curve Digital Signature Algorithm[155] (the equation that creates the encoded string of numbers). The resulting number is the "digital signature."

[153] A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes.
[154] See "Secure Hashing" http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html (last accessed Dec 7, 2016)
[155] See FIPS publication 186-4 at "FIPS Publications" http://csrc.nist.gov/publications/PubsFIPS.html (last accessed Dec 7,2016)

(b) Verifying the signature upon receipt

A device receiving the basic safety message performs the following sequence of steps in order to verify the signature:

(a) Generate the hash of the basic safety message content and timestamp using the same NIST defined formula used for generating the signature.
(b) Input the message hash, public key, and digital signature into the signature verification function (ECDSA) to verify the BSM digital signature is valid.
(c) Verify the pseudonym certificate (from the sending device) is within the validity period.
(d) Verify the digital signature of the pseudonym certificate back to the root certificate authority ensuring the SCMS issued the credentials.
(e) Verify the pseudonym certificate is not listed on the Certificate Revocation List.

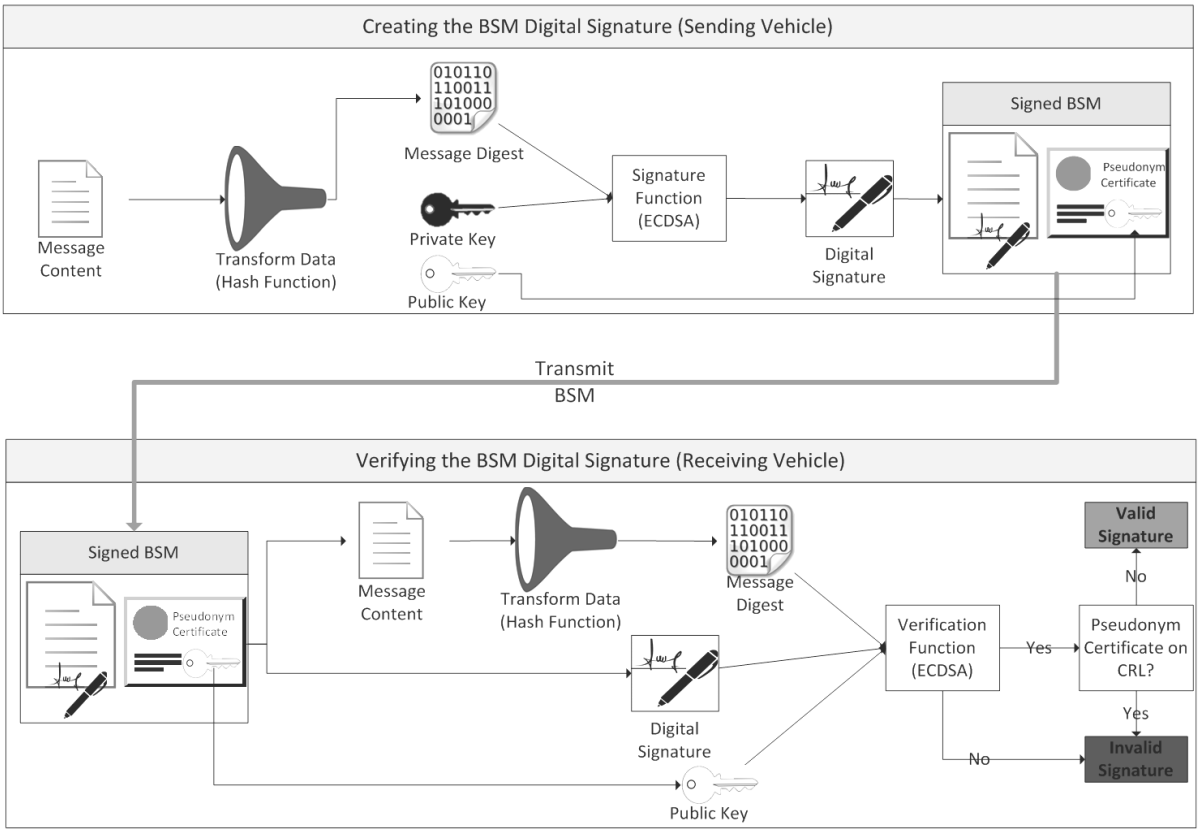

Figure III-9 BSM Digital Signature Generation

As discussed in the next section, the agency is considering a potential test method that would mimic many of the functions of the receiving device in order to assess whether devices are

properly signing their messages with valid credentials when they are transmitting basic safety messages.

(2) Potential Requirements and Testing for Message Signing and Authentication

The agency is currently considering evaluating a device's ability to properly sign the basic safety message by utilizing a test device to receive basic safety messages during a static test. The test device would perform the key functions described above to verify the authenticity of the sender and of the message. Following is discussion of the general testing framework and the potential performance requirements that the agency is considering within the context of such a test.

(a) Potential Message Authentication Test Method

The agency currently envisions testing message authentication for compliance as executing a message security and signage protocols test in a static test environment (i.e. a "security credentials test"). The test would be conducted using a vehicle resident V2V device and an agency developed test device positioned in close proximity to each other.

In effort to replicate real-world conditions, the agency's current strategy is to define a test device that can perform the following functions as described in SAE J2945/1 v1.0[156] (which itself references specific clauses and sections of relevant IEEE P1609 and 802.11 standards).

- If the full pseudonym certificate is included in the BSM, then the device will need to extract the public key from the pseudonym certificate of the test vehicle
- If the certificate digest (hash of the full certificate) is included in the BSM, then the device will need to perform a look-up in cached memory of the full certificate and then extract the public key from the pseudonym certificate of the device under test.
- Confirm that the public key and the credentials in general are indeed from the SCMS (i.e., verify the the pseudonym certificate authority all the way up to the root certificate authority).
- Use the public key to verify the signature section of the basic safety message (i.e., execute the ECDSA verification algorithm).

In terms of specific procedures, we tentatively believe that using many of the test conditions from our static test evaluating the transmission range and content of the basic safety message would be appropriate. In essence, we believe that the same test could be used to also

[156] See "On-Board System Requirements for V2V Safety Communication" at http://standards.sae.org/j2945/1_201603/ (last accessed Dec 7, 2016)

evaluate whether the vehicle is appropriately signing its basic safety messages. Tentatively, we believe that including the following additional step in the static test would be sufficient to evaluate this area of performance.

- Collect basic safety messages from a transmitting device for at least 100 minutes and repeat the test at least seven days later.[157]
- Using the messages collected in this test, the agency's test device should be able to verify the device under test is properly signing the basic safety message.
- The data collected should also reveal that the device under test is sending the required certificate (from the pseudonym certificate authority) or the certificate digest.
- The agency's test device should also be able to determine whether the device under test is using credentials issued by the appropriate authority (i.e., is the root certificate ultimately one that is authorized by the SCMS?).
- Finally, the test duration timeframes of this additional step should enable our test device to determine whether the vehicle is changing its certificates at the required interval.

We request comment on this test method and commenter's input on a potential test device that could be used to execute this proposed test schema. Would a test device that performs all of the functions outlined above sufficiently mimic real world conditions and also define those conditions sufficiently to achieve a repeatable test method? What other details should the agency explore and define? Are there other test methods that the agency should consider that can confirm that the transmitting vehicle signs the basic safety message properly with a less complex test?

The agency is also proposing to adopt a static test to evaluate the transmission range and other requirements (see Section III.E.1.a)). As testing experienced is gained, it may prove more efficient to combine the security credential, RF transmission, and possible other tests. The agency invites comment on the potential to combine and streamline test where possible.

(b) Signing the Message

Using the potential test method described in the previous section, we believe the agency would be able to verify that V2V devices are properly signing their basic safety messages, authenticating themselves as accurate sources of information. In essence, by using a test device that would be able to verify the digital signature using the ECDSA algorithm, the proposed test schema confirms that:

[157] As discussed later in this section, the timeframes for this test accommodate our current proposal for changing certificates.

- the sending device produced the correct hash of the message content/timestamp;
- the sending device appropriately sent its pseudonym certificate; and
- the public key could decode the signature created by the sender's private key.

By comparing the hash created by our test device to the hash decoded from the basic safety message we received from the device under test, our test procedure should be able to confirm the device under test is correctly signing the basic safety message. Further, we anticipate that the test device would also identify the root certificate authority and validate up to the root certificate authority.

(c) Certificates and Certificate Digests

The agency is considering including requirements to reduce the size of the basic safety message by requiring that vehicles not transmit parts of the basic safety message when they are not necessary. In theory, this could potentially conserve bandwidth in higher volume scenarios. The pseudonym certificate included in the basic safety message is an area under evaluation where message size could be reduced.

A receiving V2V device requires pseudonym certificates to decode the signature and confirm the identity of the sender. However, the agency does not anticipate that every message will need to carry the full certificate as the pseudonym certificate does not change for every message. This allows a period of time where the same certificate and potentially allowing for messages to only part of the entire pseudonym certificate. Therefore, the agency believes it would be appropriate, under certain circumstances, for devices to transmit a certificate digest which would be a hash of the full certificate.

A potential challenge to this approach is requiring a receiving device to support capture and storage of full certificates and certificate digests, as transmitting only a digest necessitates relating the digest to a full certificate. In addition to the capture and storage of certificates, the agency is also evaluating a potential requirement for the interval between the transmission of a full certificate and certificate digests. Current research suggests that the vehicle should transmit the full certificate twice per second and the digest the remaining times. However, if there is an event flag (e.g. hard braking event) in the BSM, the agency believes the full certificate should be transmitted at the next immediate opportunity. At this time our current proposed requirements do not cover this aspect of the device and but the agency requests comment concerning the need to employ certificate digests in place of the entire certificate.

We tentatively believe that a final rule on V2V would need to establish at least a minimum interval for transmitting the full certificate so that surrounding vehicles will know the maximum amount of time that they will need to wait in order to be able to confirm the identity of a transmitting vehicle. Without such a requirement, we question whether the standard would be able to ensure that vehicles transmitted their pseudonym certificate at a sufficient frequency to support the safety applications that other vehicles may use. However, we request comment on whether a minimum requirement for transmitting the full certificate is necessary. If so, what the

minimum time should be and whether a maximum time (or a specified interval such as 1 time per second) would be appropriate for this aspect of performance.

Thus, for this aspect of performance, our final performance requirements could specify minimum (and potentially maximum) times for transmitting the full certificate and requirements for what types of information need to be in the certificate digest. Thus, in addition to the testing method that we described above, our test device for that test method would also need to ensure that:

- the vehicle is transmitting the full certificate at the required interval;
- the vehicle is transmitting the certificate digest (which identifies the full certificate and when the full certificate was transmitted with all other messages that do not have the full certificate; and
- the certificate or digest transmitted along with a basic safety message is valid (i.e., it is a valid certificate issued by the SCMS/has the appropriate credentials from the root certificate authority).

(d) Changing Certificates and Privacy

As part of the process of signing a V2V message using the proposed SCMS approach, a vehicle could use a single certificate that is valid for a long period of time (e.g., years) to sign all basic safety messages that it transmits. This would help ensure that safety applications would be able to differentiate between authenticated sources of information and other less reliable sources of information when making judgements about their surroundings.

However, this approach could create additional privacy risk for consumers, as use of a single certificate could enable an observer collecting V2V transmissions to associate the basic safety messages coming from a single V2V device with a single sender. While associating a group of messages with a specific driver would need additional information outside of the V2V system, additional information would not be needed to know that all messages using the same certificate come from the same vehicle. To help mitigate this risk, we propose that vehicles frequently change or rotate certificates so that it will be more difficult to associate a large number of basic safety messages with the same V2V device or vehicle. Also, we are proposing that certificates not be valid for long periods of time to reduce the risk that they be collected and used to identify a specific vehicle at a future date and time.

(i) Current Research on Changing Certificates

Recent research evaluated several models for changing certificates. In the Safety Pilot Model Deployment, certificates had a validity period of 5 minutes and were completely discarded after use. Changing certificates on a more frequent basis helps to minimize potential privacy risk for individuals, it requires a large volume of certificates for a vehicle to manage, approximately 100,000 certificates for one year of operation. Model Deployment researchers determined that this approach would be inefficient as the majority of the time a vehicle is not in operation but certificates were still expiring even when the vehicle was not in operation. Based

on the experiences learned from this project, the researchers developed a more efficient design where a vehicle will have 20 valid certificates per week and changes certificates at least once every 5 minutes. Under this design, only 1,050 certificates would be needed per year. This is believed to strike a balance between privacy and efficiency by using certificates that rotate every five minutes and are valid only for one week. This alternative certificate usage model is currently under development and will be tested in the field as a part of the SCMS Proof-of-Concept projects.

(ii) Potential Performance Metric

We recognize that methods of changing certificate credentials exist on a spectrum between the competing interests of maximizing privacy protections and technological practicability. For example, it would afford the most privacy protection for consumers to use a different set of credentials with every basic safety message (i.e., change certificates 10 times per second). However, this would be impracticable because it is unreasonable to expect the SCMS to produce enough certificates to service all V2V devices when they use ten new certificates every second.[158] On the other hand, using the most technically simplistic method for authenticating the sender of the message would be to use one set of credentials for every message. However, as we described above, that would create significant privacy risk by associating all basic safety messages sent from a single source with each other.

In order to balance these competing interests, our tentative conclusion is that the current method for changing certificates used in the research would be a reasonable compromise that protects privacy in a technically feasible way. By rotating among 20 certificates every five minutes, we are ensuring that no group of basic safety messages will be linked to more than 5 minutes of other safety messages at a time. In other words, a person obtaining basic safety messages from a device may not be able to associate those messages with each other because their certificate is only used for 5 minutes out of every 100 minutes. Further, a device shutting off at one particular location would unlikely use the same certificate upon startup. Finally, in order to ensure that a person could not obtain all 20 certificates for a particular device, we are proposing for devices to completely discard their certificates each week and replace them with 20 new certificates.

We request comment from the public on our proposed method for changing certificatesand privacy concerns. Have we appropriately balanced the privacy interest with the interest in maintaining the technical feasibility of producing and storing certificates in vehicles? Is periodically rotating certificates the right approach to limiting the privacy impact of having signed messages? Have we established the appropriate thresholds for the method for changing

[158] A certificate is expected to be 117 bytes. The number of unique certs / year * size of one certificate. (103680 * 117 = 12.13MB for one vehicle for one year). *300 million vehicles = 3,639,168,000,000,000. Or 3.6 exabytes.

certificates (i.e., have we selected the correct duration for when devices need to rotate certificates and change the certificates to new ones altogether?). Further, should the agency establish requirements for rotating the 20 certificates (i.e., should the device rotating among 20 certificates every five minutes use the same order for rotating through the certificates or should the device use a different order the next time it cycles through the 20 certificates? What method should the agency choose for changing the cycling order of the 20 certificates?).

(iii) Test Method

As we discussed in Section III.E.3.b)(2)(a), our static test method for assessing whether a device is appropriately signing their basic safety messages can also assess whether a device is changing its security credentials as required if our test lasts for an appropriate amount of time. Based on our proposed requirements, we believe that it is appropriate to test the device for 100 minutes twice, separated by 7 days.

Testing the device for a 100 minute duration would sufficiently assess whether the device is rotating certificates every five minutes and using a different certificate every five minutes for the duration of 100 minutes (i.e., 20 certificates x 5 minutes per certificate). Finally, conducting this test twice (separated by 7 days) would allow the test to confirm whether the device is using 20 new certificates that are different from the certificates the device used in the first test.

(e) Preventing Message Transmission without Valid Certificates from a SCMS

The agency is also considering whether to require that devices stop transmitting basic safety messages if they lack valid security credentials, i.e. device transmission problems or being identified as a misbehaving device. The purpose would be for devices to avoid sending basic safety messages due to incorrect credentials. However, at this time, the agency does not have performance requirements or a test method for assessing this aspect of performance. In order to test this aspect of performance, the agency would need a method for exhausting the certificate supply of a vehicle and observing whether the vehicle would continue to transmit basic safety messages. We request comment on whether there is a practicable and repeatable way for producing these conditions in a vehicle under test. We also request comment as to whether this aspect of performance should be included in the final rule.

(3) Potential Regulatory Text for SCMS based message authentication

S.4 Definitions (additional)

Elliptical Curve Digital Signature Algorithm - The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). It was accepted in 1999 as an ANSI standard, and was accepted in 2000 as IEEE and NIST

standards. It was also accepted in 1998 as an ISO standard, and is under consideration for inclusion in some other ISO standards.[159]

Private Key - In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages.[160]

Public Key - In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures.[161]

Pseudonym Certificate Authority - issues short-term certificates to devices that are used with each BSM to ensure trust in the system.

Security Credential Management System - organization that oversees PKI verification process for vehicle communications by providing necessary signing credentials (i.e., digital certificates) and conducting related security functions, such as identifying and removing malfunctioning V2V devices from the system.

Validity period – pertains to the use of security certificates and tells the receiving device when the certificate being used by the transmitting vehicle is valid (i.e., do not accept these credentials if they are expired).

S5.4. Signing the BSM. A DSRC device must generate a signature for each BSM by creating a hash (using NIST formula SHA-2) of the message content and timestamp, and inputting the hashed contents through the Elliptical Curve Digital Signature Algorithm (ECDSA). This signature must be sent with each BSM, along with the pseudonym certificate (which includes the public key, the validity period, and the signature from the Pseudonym Certificate Authority). All digital certificates used must be obtained from the same DOT-identified authoritative root. When tested according to our test described in S7 below, the digital signature must match the output of our test device.

S5.4.1. Rotating certificates. A DSRC device must rotate among a specified number of valid certificates, initially a set of 20, during a specified seven day period changing certificates

every 5 minutes. At the end of each week, the DSRC device must completely discard all certificates used that week, and replace them with 20 new certificates.

c) Alternative Approach - Performance-based Message Authentication

(1) Overview

The agency is also bringing forth potential alternatives to the SCMS-based proposal for V2V message authentication. This first alternative takes a far less prescriptive approach to authentication and defines a performance-basedbased approach but not a specific architecture or technical requirement for message authentication. The basis of this alternative is to let V2V device implementers define their own approach for improving the integrity and authenticity of V2V messages.

The fundamental approach to this first alternative only requires that the receiver of a basic safety message be able to validate the contents of a message such that it can reasonably confirm that the message originated from a single valid V2V device, and the message was not altered during transmission. This alternative would broadly require that implementations utilize government-audited and approved cryptographic algorithms, parameters, and approaches.

(2) Illustrative Example

For illustrative purposes, consider the following example technical implementation. The sender of a BSM could use a security certificate issued by a certificate authority to digitally sign each BSM. The security certificate could be composed of the following elements:

- A date range describing the validity period for the certificate
- A Public key corresponding to a private key
- Digital signature from a certificate authority

(3) Potential Requirements under this Alternative

(a) Test Method and Test Device

This alternative's less prescriptive approach for message authentication results in a general testing requirement that would similar in context as the proposed PKI based authentication but leaves the extent of the proposed requirement undefined, or yet to be defined, static test procedures. This approach is inherently aligned with recognizing that potential future communication and their potential message authentication needs would be varied and, therefore, requires varied test methods for message signing and authentication.

NHTSA seeks comment on potential test methods and the test devices that could accommodate other, future, or yet-to-be-developed message signing and authentication schemas that could be applied to V2V communications. The agency is interested in details on how a test

device could fulfill the general requirement to sufficiently reflect real-world conditions and also define those conditions sufficiently to achieve a repeatable test method that ensure verified communications between V2V devices, using varied communication mediums? What other details should the agency explore and define? Are there other test methods that the agency should consider that can confirm that a transmitting V2V device signs the basic safety message properly?

d) Alternative Approach - No Message Authentication

This second potential alternative set out for comment does not specify any message authentication requirements for devices participating in a V2V communications. Under this second potential alternative, BSM messages would still need to be validated with a checksum or other integrity check and employ some form of through a misbehavior detection system to attempt to filter malicious or misconfigured messages. However, there would be no specific message authentication requirement. Implementers would be free to include such a feature as an optional function. The agency would not establish any performance requirements or test procedures under this potential alternative. The agency seeks comment on this no message authentication approach.

4. Misbehavior Reporting

a) Proposal - Misbehavior Reporting to a SCMS

NHTSA is proposing to establish practices and procedures for devices participating in V2V communications to recognize device misbehavior, both internally and by other devices. The fundamental purpose of misbehavior detection is to provide a means for V2V devices to identify and block messages from other misbehaving or malfunctioning V2V devices. V2V devices would be required to report device misbehavior to a central authority, namely the Security Credential Management System, once misbehavior is confirmed via a series of self-diagnosis or plausibility checks on incoming messages. This includes identifying methods for device self-diagnosis of both hardware and software to ensure that the device has not been altered or tampered with from intended behavior.

If an anomaly is detected and confirmed by a series of secondary plausibility checks, a "misbehavior event" would be identified, and a sample of BSM information such as geo-location, time-stamp, and a digitally signed (encrypted) certificate from the misbehaving device would be recorded as "evidence" of the event. The reporting device would then transmit its misbehavior report to the SCMS misbehavior authority (MBA) using a secondary communications channel.

The intent of the MBA is to gather misbehavior reports by all devices participating in the network. These reports would be analyzed in accordance with established and governed policies for global misbehavior detection determine if and when a particular vehicle should be placed onto a Certificate Revocation List (CRL). More accurately, is and when information related to a particular device's certificates should be placed onto the CRL such that other vehicles can use

the information to identify the misbehaving device, assume it cannot be a trusted device, and ignore its messages. The CRL would be updated periodically by the MBA and distributed to participating V2V devices.

The agency views misbehavior detection as a key feature of the proposed security architecture: that misbehaving devices are able to be efficiently detected, and their identity made available to other devices participating in the network. At the highest level, confidence in the V2V messaging could be eroded if misbehaving devices are not detected and reported to a centralized authority.

As indicated in Table II-5, additional research is being conducted to better understand the data, processing, and algorithm development necessary to implement misbehavior detection at both the local (device) level and global (SCMS) level. For misbehavior to be effective, techniques must be identified, developed, and implemented in both devices and at a central authority for the system to secure V2V messages. The proposed requirements concerning detection and reporting support misbehavior detection functionality, but do not include at this time the actual techniques to detect and identify misbehavior. Research is being conducted; however, the actual nature of misbehavior in the V2V ecosystem has yet to be defined given the lack of misbehavior data to support actual development of techniques and algorithms. Initial data will be available once the SCMS Proof-of-Concept (Section V.B.6.e) is operational and supporting the security of the Connected Vehicle Pilot activities. The agency seeks comment regarding the requirements to support misbehavior detection, the investigation of detection and identification techniques, and possible implementation issues including the need to evolve detection and identification algorithm capabilities over time.

(1) Reporting

The agency has worked extensively with its research partners to develop a comprehensive set of proposed reporting requirements for misbehavior detection. The reporting requirements attempt to strike a balance between frequency, the amount of data reported, and the need to effectively and efficiently identify misbehavior to mitigate any potential effects. As described previously, the purpose of the misbehavior reports is to:

- indicate potential misbehavior and misbehaving devices, and
- indicate suspicious activities around the reporting device

(a) Report content

The agency is proposing that a misbehavior report is a message signed by the reporting device and shall include at a minimum the following data:

- The reporter's certificate
- GNSS coordinates (latitude, longitude and elevation) at the location where the misbehavior was initially identified

- The GNSS coordinates where the misbehavior appears to have ended. This field is optional as it may not apply to all misbehavior. This could be useful for indicating where a DoS attack begins and where it ends.
- BSMs from both host device and remote threat device
- Warnings present at time of misbehavior detection, if any
- List of neighboring devices
- The Coordinated Universal Time (UTC) at which the misbehavior was detected
- Information identifying the detection method that triggered the report

The agency seeks comment on the proposed inclusion of the above data in a misbehavior report. Specifically, we would appreciate commenters providing any potential additional data that should be included. The agency also asks commenters to provide feedback on the potential for inclusion of any personally identifiable information (PII) related to misbehavior and the potential positives and negatives of such an inclusion.

Additionally, the agency is also seeking comment on the potential inclusion of the following items in the misbehavior report:

- The average Channel Busy Percentage observed if a Denial of Service is detected
- List of vehicles (device/certificate IDs) within communication range when misbehavior is detected
- Abstracted (non-V2V related) sensor information if such sensor information is available to the device
- Averaged speed of vehicles within communication range of the reporting vehicle

(b) Misbehavior Report Generation and Transmission

A misbehavior report shall be generated as follows:

- A misbehavior report shall be created at the time a misbehavior is detected
- Misbehavior reports shall be signed and transmitted with the same credentials as those of BSMs
- A misbehavior report shall be signed by the reporting device at the time of the report creation
- The misbehavior reports shall be encrypted with the public key of the misbehavior authority and transmitted to the central authority through a secured communication channel

(c) Misbehavior Report Storage

Misbehavior reports shall be stored as follows:

- The V2V device shall allocate sufficient persistent memory storage for 1600 KB of misbehavior event reports
- Misbehavior reports shall be stored persistently in non-volatile memory to avoid report erasure during vehicle shut-down and start-up cycles
- A misbehavior report shall be stored in persistent memory for at least 20 weeks
- If the allocated misbehavior report memory capacity is to be exceeded due to a new incoming misbehavior report, the oldest report or reports shall be overwritten to allow the storage of the newest report
- If misbehavior reports are to be stored in unencrypted storage medium, the content shall be encrypted

(2) CRL Processing

- If the credentials of a locally detected misbehaving device are already on the locally stored CRL it shall not be re-reported to the central authority

(3) SCMS Security

The agency recognizes the misbehavior mechanism identifies anomalies that could indicate malfunctions or malicious activities that could adversely impact proper operation of individual devices or the system; possibly causing unsafe or unreliable operation if trusted. Misbehavior operations and subsequent device requirements ensure that the device perpetrating the misbehavior can be rendered innocuous by revoking the device's security certificates effectively making them an untrusted source to properly functioning devices. The agency is therefore proposing the following the requirement is applied to a central authority, namely the SCMS, responsible for global misbehavior and management:

- The agency requires that a central authority employ protocols that establish a disposition based on reporting from various sources to mitigate the potential for misbehavior detection to become a gateway for an easy cybersecurity threat for denial of service.

(4) Request for Comment

The agency believes the proposed misbehavior reporting requirements could help reduce the number of misbehaving devices whose messages would be accepted by the V2V network and thus help reduce the chance of false safety warnings. The agency seeks comment on the misbehavior reporting approaches describe in this section along with potential other approaches the agency should consider.

More specifically, the agency appreciates thorough explanation of any suggested alternative approaches to misbehavior reporting, as well as sufficient description of why you believe that the proposed approach is, or is not appropriate. Additionally, the agency would appreciate suggestions on how to properly and reasonably test for misbehavior in a V2V system.

(5) Potential Regulatory Text for SCMS-based Misbehavior Detection and Reporting

S5.6. Detecting misbehavior. A DSRC device must detect and report misbehavior in the following ways:

S5.6.1. Internal self-diagnostics. A DSRC device must be able to perform the following self-diagnostic checks and report accordingly to the SCMS:

S5.6.1.1 If a DSRC device detects a malfunctioning sensor which may cause misbehavior, the device must:

a. Either transmit the BSM with the affected elements set to "Unavailable" if relevant DSRC standards allow the element to be set to "Unavailable"; or
b. Cease BSM transmission if relevant DSRC standards do not allow the element to be set to "Unavailable."

In the case of either (a) or (b) above, the DSRC device must report itself to the SCMS if it detects through self-diagnostics that one or more of its sensors is malfunctioning in a way that could cause misbehavior.

S5.6.1.2 If a DSRC device detects physical tampering with or manipulation of the DSRC radio, the DSRC device must report itself to the SCMS.

S5.6.2.3. If a BSM fails any plausibility check, the DSRC device shall flag the specific check failed and the source of the BSM and generate a misbehavior report that at a minimum includes the following data:

a) The reporter's certificate;
b) The Coordinated Universal Time (UTC) at which the misbehavior was detected;
c) GNSS coordinates (latitude, longitude, and elevation) at the location where the misbehavior was detected;
d) BSMs from both the host vehicle and remote threat vehicle associated with detection of the misbehavior;
e) Safety Application Warnings present at time of misbehavior detection, if any;
f) List of neighboring devices the misbehavior reporting device is receiving within 300m when the misbehavior is detected;
g) Information identifying the detection method that triggered the report.

The report may also include the 3-D GNSS coordinates at which the misbehavior appears to have ended, if applicable.

S5.6.2.4. A DSRC device must support the detection of other devices which are suspected of misbehaving, and at a minimum detect the following types of misbehavior:

a. False Warning Report: A misbehavior event is detected and sent to the SCMS when false warnings occur within the vehicle.
b. Proximity Plausibility: Instances are detected of two or more vehicles, either partially or wholly, occupying the same physical space based on the reported GPS positions.
c. Motion Validation: Attempts to validate the reported position of a transmitting vehicle based on the previously-reported velocity and heading values of the vehicle.
d. Content and Message Verification: Attempts to categorize BSMs as suspicious by checking the security credentials of and the data validity of the BSM.
e. DoS Detection: Attempts to determine instances and regions which are subject to potential DoS attacks.

S5.6.3. Creating and sending misbehavior reports.

S5.6.3.1. Misbehavior report content. A misbehavior report is a message signed by the reporting DSRC device and must include, at a minimum, the following data:

h) The reporter's certificate;
i) The Coordinated Universal Time (UTC) at which the misbehavior was detected;
j) GNSS coordinates (latitude, longitude, and elevation) at the location where the misbehavior was detected;
k) BSMs from both the host vehicle and remote threat vehicle associated with detection of the misbehavior;
l) Safety Application Warnings present at time of misbehavior detection, if any;
m) List of neighboring devices the misbehavior reporting device is receiving within 300m when the misbehavior is detected;
n) Information identifying the detection method that triggered the report.

The report may also include the 3-D GNSS coordinates at which the misbehavior appears to have ended, if applicable.

S5.6.3.2. Misbehavior report generation and transmission. A misbehavior report must be generated and transmitted as follows:

(a) A misbehavior report must be created within 2 seconds after the misbehavior is detected.
(b) Misbehavior reports must be signed and transmitted with the same credentials as those of BSMs.
(c) A misbehavior report must be signed by the reporting device at the time of the report creation.
(d) Misbehavior reports must be encrypted with the public key of the misbehavior authority and transmitted to the SCMS.

S5.6.3.3. Misbehavior report storage. Misbehavior reports must be stored as follows:

(a) The DSRC device must allocate sufficient persistent memory storage for 1,600 KB of misbehavior event reports.
(b) Misbehavior reports must be stored persistently in non-volatile memory[162] to avoid report erasure during vehicle shut-down and start-up cycles.
(c) A misbehavior report must be stored in persistent memory for at least 20 weeks.
(d) If the allocated misbehavior report memory capacity is to be exceeded due to a new incoming misbehavior report, the oldest report (or reports, if necessary) may be overwritten to allow the storage of the newest report.
(e) If misbehavior reports are stored in unencrypted storage medium, the content must be encrypted.

S5.6.3.4. CRL processing. If the credentials of a locally-detected misbehaving device are already on the locally-stored CRL, it need not be re-reported to the SCMS.

S5.8. Communicating with the SCMS. A DSRC device must be able to create an IP connection (to request new certs, to get new certs, to send CRL, to send misbehavior reports)to the SCMS using, for example, a wired network connection (Ethernet), cellular, DSRC connection through an RSE that has internet connectivity, or Wi-Fi. The connection must allow the SCMS to send information to the DSRC device and allow the DSRC device to send information to the SCMS.

S7.3.5 Misbehavior Detection (testing additional)

S7.3.5.1 Activate the SCMS to advertise connectivity using a WAVE Service Advertisement (WSA)

S7.3.5.5 Using the reference OBE device, transmit simulated misbehaving BSMs with a valid signature

S7.3.5.8 Verify if the misbehavior report (MBR) was uploaded to the SCMS

S7.4.6.10 Retrieve and process the log files to determine if a MBR was sent to the SCMS

S7.4.7 Misbehavior Detection: Signature failure

S7.4.7.1 Configure a remote test vehicle (RV1) to improperly sign BSMs

S7.4.7.2 Place RV1 on a two lane test track and position it in the right most lane

S7.4.7.3 Activate the test vehicle starting system to initiate BSM transmission

S7.4.7.4 Activate the DSRC packet capture device to log BSMs OTA

S7.4.7.5 Drive the test vehicle [30 mph +/- 1 mph] along the test track in the left lane and proceed past RV1

S7.4.7.6 Repeat S7.4.7.5 three (3)times

S7.4.7.7 Bring the test vehicle to a stop

S7.4.7.8 Retrieve and process the log files to determine compliance with S5.6

S7.4.7.9 Drive the test vehicle past the RSE at a constant [30 mph +/- 1 mph]

S7.4.8 Certificate Request

S7.4.8.1 Configure the RSE to send a WSA on the control channel every 100 msec, including channel information

S7.4.8.2 Activate the test vehicle starting system to initiate BSM transmission

S7.4.8.3 Activate the DSRC packet capture device to log BSMs OTA

S7.4.8.4 Drive the test vehicle [30 mph +/- 1 mph] along the test track and proceed past the RSE

S7.4.8.5 Bring the test vehicle to a stop

S7.4.8.6 Retrieve and process the log files to determine compliance with S5

S7.4.9 Certificate Delivery i (complete transaction)

S7.4.9.1 Configure the RSE to send a WSA on the control channel every 100 msec, including channel information

S7.4.9.2 Activate the test vehicle starting system to initiate BSM transmission

S7.4.9.3 Activate the DSRC packet capture device to log BSMs OTA

S7.4.9.4 Drive the test vehicle [30 mph +/- 1 mph] along the test track and approach the RSE

S7.4.9.5 Bring the test vehicle to a stop

S7.4.9.6 Retrieve and process the log files to determine compliance with S5

S7.4.10 Certificate Delivery ii (resumed transaction)

S7.4.10.1 Configure the RSE to send a WSA on the control channel every 100 msec, including channel information

S7.4.10.2 Activate the test vehicle starting system to initiate BSM transmission

S7.4.10.3 Activate the DSRC packet capture device to log BSMs OTA

S7.4.10.4 Drive the test vehicle [30 mph +/- 1 mph] along the test track and approach the RSE

S7.4.10.5 Drive the test vehicle away from RSE radio coverage before the complete certificate bundle has been delivered

S7.4.10.6 After 5 minutes, return the test vehicle to within RSE radio coverage

S7.4.10.5 Bring the test vehicle to a stop

S7.4.10.6 Retrieve and process the log files to determine compliance with S5

b) Alternative Approach - No Misbehavior Reporting

In contrast to the primary misbehavior detection proposal, the agency is seeking comment on an alternative approach to misbehavior detection where there are no requirements to report misbehavior or implement distribution of information to facilitate blocking based on misbehavior reports to an authority. Implementers would be free to include such features as reporting the detection of any misbehavior or a malfunction as optional functions. Independent of this alternative approach, the agency is proposing to require that implementers identify methods that would check the functionality, including hardware and software, of a V2V device ensuring that the device has not been altered or tampered with from intended behavior.

The agency appreciates commenter's views on this potential alternative approach including reasons why or why not this potential would be appropriate for identifying misbehaving or malicious devices participating in V2V communications. We also encourage commenters to provide any suggested alternative approaches to misbehavior reporting, as well as sufficient description of why you believe that the proposed approach is, or is not appropriate. Additionally, the agency would appreciate suggestions on how to properly and reasonably test for misbehavior in a V2V system.

5. Proposed Malfunction Indication Requirements

a) Overview

The agency is proposing to require that all V2V devices be equipped with a mechanism for notifying users that the device and/or its supporting equipment is not operating normally and some form of repair is necessary. The requirements proposed in this section are consistent across any potential technology employed in V2V communications. The agency is not specifying a

format for the notification mechanism, as elaborated below – it can be an illuminated telltale, a message in the message center, or something else – but it must be presented in the vehicle itself for OBE or on the device itself for non-integrated aftermarket products. This proposed requirement aligns with the proposed misbehavior requirements and cost estimates, in that misbehavior detection requires devices to perform self-diagnostics and report to users a failure condition. Likewise, the cost estimates for the proposal include costs for some type of malfunction indicator and reflect what we would consider to be a "minimalist" approach.

The agency has a long history of requiring both diagnostics and malfunction indicators. FMVSSs for electronic stability control (No. 126), tire pressure monitoring systems (No. 138), and air bags (No. 208), among others, include requirements for indicating when the system is in a failure condition. In these cases, the agency believed, and therefore required, that proper maintenance to ensure system operation is vitally important to driver and passenger safety. The agency has no reason to believe any differently for V2V devices, other than potentially strengthening those beliefs based on the cooperative nature of V2V and how the benefits are a "networked good;" where one device has the potential to benefitting many others.

b) Malfunction Indication Requirements

- Any device participating in the V2V system shall clearly indicate to their users a malfunction condition occurring in the device, its supporting equipment or the inputs used to form, transmit, and receive a basic safety message. Malfunction indication shall be provided in instances such as:
  - Device components not operating properly
  - Input sensor data not within appropriate tolerances
  - On Board memory failures
  - GPS receiver failures
  - Unable to transmit or receive basic safety messages
  - Any other failure that could prevent normal operation
- Malfunction indication shall be clearly presented to device users in the form of a lamp or message
- Owner's information shall clearly describe the malfunction indication, potential causes, and if needed, the need to have the device serviced
- The malfunction indication shall remain present until the V2V device is returned to normal operating state
- The malfunction indicator shall illuminate the malfunction indicator as part of power up initial system diagnostics to confirm the indicator is operating properly

The agency seeks comments on these proposed requirements. More specifically, the agency would like commenters to give their views on malfunction indication, the best ways to convey device malfunction to users, and why they believe this to be the case.

6. Software and Security Certificate Updates

The agency anticipates that, over time, V2V devices and the system overall will require periodic updates to address functionality, potential security, or potential privacy issues as they arise after a vehicle owner or operator takes possession of a vehicle. The agency is proposing that V2V devices allow for over-the-air (OTA) software and certificate updates and those device users be notified of any consent required for periodic device updates.[163] The agency believes that over-the-air devices updates will be viable and commonplace by the time a final rule to this proposal is finalized.[164],[165]

We anticipate this highest potential for periodic updates will come in two primary forms: device software updates and security credential updates. In either case, the agency believes user notification and consent would be required to execute the update. The approach of this proposal is provide the basic platform to enable V2V communications where the hardware needed is the most technologically basic enabler, essentially a radio transmitter and receiver. The device complexity, intellectual property and overall V2V operation is primarily rooted in the firmware and software loaded into a V2V device's hardware. The agency anticipates any updates to the device hardware would be manifested by a malfunction, device failure that would be subject a recall and/or warranty provisions if the device warranty is still valid.

Over the air updating will provide significant flexibility for updates, not only to V2V devices but many vehicle-resident components, to fundamental device operation but also, following suit of smartphone devices, enable "pushing out" new applications to automotive devices. The agency believes this approach can and will best exploit the V2V communications "platform" contained in this proposal.

As discussed throughout the proposal and more specifically, the legal authority section, Section V.C, the agency believes V2V device users will need to consent to both software and security certificate updates. Therefore, the agency is proposing to require that devices participating in the system provide users with indication, in the form of a descriptive telltale or text message displayed in a vehicle message center that is in clear view of the driver, that device software or security certificate updates are available and that users need to consent before the update can occur. The indication and consent mechanism must reside in the vehicle or device.

---

[163] See Section VI below for the agency's discussion of its legal authority. This proposed requirement is similar to many other existing requirements to warn drivers via telltales or messages about potential issues with required safety technologies, for example, the ESC or TPMS malfunction telltales. The difference in this case is simply that the agency expects a need to illuminate the telltale with some regularity, given that certificates will periodically run out and need to be replenished.

[164] "OTA updating brings benefits, challenges" SAE Automotive Engineering, August 16, 2016, http://articles.sae.org/14946/ (last accessed: Dec 7, 2016)

[165] "International Truck offers over-the-air programming for 2017 Cummins engines" SAE Automotive Engineering, May 19, 2016, http://articles.sae.org/14834/ (last accessed: Dec 7, 2016)

The agency seeks comment on this proposed requirement for software and certificate update. Do commenters agree with the proposed approach, why or why not? Do commenters have alternative suggestions for how V2V device users can seamlessly consent, without burden, to software and/or certificate updates? More specifically, how do commenters perceive potential mechanisms for receiving notification and consenting, or not, to any potential updates. What potential implications may result from the anticipated need for updates and consent? What real-world experience do commenters have performing over the air updates for devices? Please provide any supporting information that may help the agency explore and finalize an approach.

7. Cybersecurity

a) Cybersecurity Overview

Today's electronics, sensors, and computing power enable the deployment of vehicle safety technologies, such as forward-collision warning, automatic-emergency braking, and vehicle-to-vehicle technologies, which can keep drivers from crashing in the first place. NHTSA strongly believes in the need for cybersecurity, which is essential to the public acceptance of increasingly computerized vehicle systems, to the safety technology they govern, and to the realization of the safety-enhancement potential they offer.

Cybersecurity, within the context of road vehicles, is the protection of automotive electronic systems, communication networks and nodes that interface with vehicles, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation. The agency has been taking a holistic approach to vehicle cybersecurity, considering that all access points into the vehicle could potentially be compromised, and is focused on solutions to harden the vehicle's electronic architecture against potential attacks and to ensure vehicle systems take appropriate and safe actions, even when an attack may be successful.[166] A layered approach to vehicle cybersecurity within a risk-based framework reduces the probability of an attack's success and mitigates the ramifications of a potential unauthorized access.

NHTSA's vehicle cybersecurity approach is built upon the following principles:

- Based on the risk-based prioritized identification and protection of safety-critical vehicle control systems and personally identifiable information;
- Provides for timely detection and rapid response to vehicle cybersecurity incidents in the field;

[166] See "NHTSA and Vehicle Cybersecurity", http://www.nhtsa.gov/staticfiles/administration/pdf/presentations_speeches/2015/NHTSA-VehicleCybersecurity_07212015.pdf (last accessed Dec 12, 2016).

- Designs-in methods and measures to facilitate rapid recovery from incidents when they occur, and;
- Institutionalizes methods for accelerated adoption of lessons learned across the industry through effective information sharing, such as through participation in the Auto ISAC.

Our vehicle cybersecurity research program considers all access points into the vehicle, more broadly than, but also including V2V. This approach makes a distinction between

(1) how vehicle architectures should be designed that interface with the outer world such that risks to safety-critical system functionality could be effectively mitigated; and
(2) how each unique access point could be protected such that an appropriate relationship could be established for the messages exchanged over that medium.

b) Agency's Cybersecurity Approach to Hardening Vehicle architectures in General

Related to hardening the vehicle architectures to be cyber-resilient agnostic of the type of communications interface, NHTSA is pursuing a best-practices approach, which is based on the National Institute for Standards Technology's (NIST) proven cybersecurity framework that includes five principal functions: Identify, Protect, Detect, Respond, and Recover.

This approach suggests that all interfaces between the vehicle electrical architecture and the external world (personal or aftermarket devices, cars, infrastructure, cloud, etc.) need to be carefully considered for risks and appropriate mitigation strategies be implemented. These include not only protection methods, but also intrusion detection techniques, rapid remediation strategies and fast adoption of new lessons learned, because we assume that all entry points into the vehicle, such as Wi-Fi, infotainment, the OBD-II port, V2V, and other points of potential access to vehicle electronics, could be potentially be or become vulnerable over time. We suggest that the industry should make cybersecurity a priority by using a systematic and ongoing process to evaluate risks. And, this process should give explicit considerations to privacy and cybersecurity risks through the entire life-cycle of the vehicle. Further, safety of vehicle occupants and other road users should be an overriding consideration when assessing risks.

We continually monitor the industry as they move towards a more cyber-aware and cyber-resilient posture and will take necessary actions to ensure that there are no unreasonable safety-risks.

c) V2V-Specific Cybersecurity Considerations

NHTSA does not overlook the potential risks of interfacing the V2V vector with vehicle systems; however, we believe that the holistic approach we are taking in the broader sense as outlined above apply to the common characteristics of various different communications interfaces in the same manner.

In this section, we will primarily focus on the unique attributes of the V2V communications interface and present key steps that are being taken to mitigate the potential incremental risks they could pose.

Key attributes of V2V communications interface, as they relate to cybersecurity risks include the following:

(1) Security and privacy by design through a message authentication,
(2) Broadcast-listen protocol,
(3) Well-defined and fairly limited message structure,
(4) Communications range is limited to about 1000ft,

NHTSA's primary proposed message authentication alternative for V2V communications employs a PKI-based security. Each broadcast message is signed with cryptographic keys to facilitate a method for the receiving units to validate the authenticity and integrity of the transmitted message from its source.

Both the primary and performance-based alternatives for message authentication seek to ensure the integrity of messages between communicating units to help assert that the message has not been altered during transmission or been sent from a malicious sender. It is important to note that this approach does not necessarily validate the accuracy of the message content received.

We consider the cybersecurity risks associated with

(1) the PKI authentication method, and the infrastructure supporting it,
(2) the contents of the messages received, and
(3) the V2V communication interface as a potential channel to inject malware

(1) PKI-SCMS Cybersecurity requirements

In Section V, the primary message authentication proposal describes the SCMS. The system described is focused on the security functions and requirements necessary to help secure the V2V communications environment. Implementations of the performance-based alternative for message authentications may also need similar compensating approaches depending on the approach taken. While the proposed primary message authentication architecture provides well-recognized security protections, we further consider the potential cybersecurity vulnerabilities and discuss how they are expected to be mitigated.

(a) On-vehicle security materials (cryptographic information)

- The OBE will contain security materials that are critical to the operation of the V2V device, and the system as a whole. This includes long term enrollment

certificates, short term pseudonym certificates, public/private keys, SCMS security policies, and misbehavior reports. All of this data, if retrieved by unauthorized parties, could allow potential "bad actors" to transmit messages that may appear valid to the general ecosystem of devices because these messages are using actual credentials given to a trusted device.

- Attempts to retrieve valid security materials could involve targeting physical OBEs. In addition to having access to OBEs on personal vehicles, OBEs on vehicles that are at their End-of-Life (EOL) decommissioning phases (such as those that can be taken from vehicles in junkyards) could also create a pathway. In the event that a vehicle with a device has met with the end of its useful life, it is foreseen that the device could have up to three years' worth of valid security certificates, assuming that it has regular communication with the SCMS.

- One method that could mitigate the risk associated with retrieval of security information through physical access to the OBE would involve hardware security against tampering such as the use of FIPS[167] Level 3 hardware security module. This specification level is consistent with requiring the zeroisation of cryptographic information in the event that the device is tampered with. While this would protect against malicious attempts, it would likely result in managing the legitimate serviceability needs of the units, likely incurring additional costs for maintenance.

- The agency believes that the current environment regarding cybersecurity and protecting the public warrants a level of hardware security that goes beyond evidence of tampering to actually protecting cryptographic information in the event of a device breach with malicious intent. Therefore, the agency is proposing to require that V2V devices have a minimum of FIPS-140 Level 3 security protection. The agency also believes that at, a minimum, the following information shall be stored in FIPS-140 Level 3 storage:

---

[167] The FIPS families of standards contain a set of standards that pertain specifically to cryptographic storage models, FIPS-140 which the industry uses to store sensitive cryptographic information. The device long and short term certificates along with the devices public/private key pairs are generally regarded as cryptographic information. The FIPS-140 set of standards define various levels of security for cryptographic information storage ranging from 1 through 4, with increasing security measures as the levels get higher. Of particular interest to the OBE are levels 2 and levels 3. Amongst other differences, the agency is interested in the tamper capabilities of these levels. Level 2 is considered tamper evident storage. This can be achieved by placing seals on enclosures (like stickers on over the counter medication that say "do not use if seal is broken"), by using tamper evident screws and mounting hardware, and other such methodologies. Level 3 adds to this by requiring devices to be tamper resistant. There are many ways to achieve tamper resistance; however, one common method for protecting data is to have the device zero out cryptographic storage in the event that a device is tampered with.

- All individual pseudonym certificates
- RA, Intermediate CA, and PCA certificates
- the RA address
- system configuration files
- security policies
- Root CA certificate
- Device Enrollment certificate
- All system private keys
- The System CRL
- All unsent misbehavior reports

- The level of security requirements defined by FIPS-140 Level 3 is somewhat different than the historical regulatory authority approach exercised by NHTSA. NHTSA issues performance based requirements which can be found in the many safety standards issued and managed by the agency, although we can be specific in equipment requirements if it is necessary to meet a safety goal. Evaluating security protection ability does not necessarily conform to a performance requirement and compliance test paradigm followed by the agency. As such, NHTSA anticipates device compliance to be conducted by the agency through third party testing laboratories with expertise in confirming the appropriateness of device's hardware security.

- NHTSA seeks comments on this approach (FIPS-140 Level 3 requirement) and on what constitutes tampering, applicable triggers for zeroisation, and how the triggers could be implemented such that routine vehicle maintenance activities can be accomplished without undue burden on the V2V device. The agency seeks comment on the proposed FIPS-140 Level 3 device security requirements. In specific, the agency seeks comment on the FIPS and CCP security approaches briefly described in this section and the pros/cons of each, potential compliance approaches including verification schema for information that should be contained in a functioning, secure device, and views on the whether the proposed level of protection is sufficient for anticipate cybersecurity needs.

- Another approach that could address the more specific EOL OBE security exposure could be for the SCMS to establish a process and procedure by which responsible entities could notify the SCMS of end-of-life devices (entities that deal with old, junked, crashed or otherwise unusable vehicles that contain OBEs.) This would require the entity that determines the device is at its EOL be able to report to the security certificate information the SCMS would need to remove the device from the system by including the devices security credentials on the system "blacklist" rendering the security information useless. This approach could pose challenges in practical application where the vehicle or device may not

be operating properly. Secondly, enabling a method to obtain security information from a device could open up a potential security vulnerability that could be used by others to obtain security materials

We request comments on whether a process approach can succeed and whether there may be other means to secure the on-unit security information.

(2) Potential Regulatory Text for Physical Security for SCMS-based message authentication proposal

Following is potential regulatory text that could support the cybersecurity requirements discussed in the primary proposal for message authentication based on the SCMS.

S5.10.1. V2V devices must have a minimum security protection of FIPS-140 Level3. Additionally, all of the following information must be stored in FIPS-140 Level 3 storage:

1. All individual pseudonym certificates
2. RA, Intermediate CA, and PCA certificates
3. The RA address
4. System configuration files
5. Security policies
6. The Root CA certificate
7. The Device Enrollment Certificate
8. All system private keys
9. The system CRL

A V2V device connected to a vehicle data bus must incorporate isolation measures (firewalls) to prevent the V2V module from being a conduit allowing outside, malicious actors to gain access to the vehicle data bus and other vehicle modules connected to the data bus.

NHTSA seeks comments regarding the cybersecurity needs and requirements and how regulatory language needs to be crafted to appropriately express the requirements in terms industry can implement and performance can be objectively evaluated.

(3) Performance-based Physical Security Alternative

Following is potential regulatory text that could support the cybersecurity requirements discussed for a performance-based message authentication alternative.

S5.10.1. V2V devices must have a minimum security protection of FIPS-140 Level 3 for storage of cryptographic certificate, key, and other sensitive data. In addition, a V2V device connected to a vehicle data bus must incorporate isolation measures

(firewalls) to prevent the V2V module from being a conduit allowing outside, malicious actors to gain access to the vehicle data bus and other vehicle modules connected to the data bus.

(4) No Physical Security Alternative

Following is potential regulatory text that could support the cybersecurity requirements discussed for a no message authentication alternative.

S5.10.1. A V2V device connected to a vehicle data bus must incorporate isolation measures (firewalls) to prevent the V2V module from being a conduit allowing outside, malicious actors to gain access to the vehicle data bus and other vehicle modules connected to the data bus.

d) SCMS cybersecurity considerations

For the primary message authentication proposal, , the SCMS provides key services and security. Key functions of the SCMS include:

- communications with DSRC devices to transfer of security certificates,
- CRL maintenance and communications to the vehicles.

Section III.E.3.b) explained how security certificates are obtained, when and why certificates are changed, and how additional certificates would be requested and obtained. SCMS provides this service and uses encryption methods to facilitate secure communications to protect security information in transit.

CRL's are distributed to appropriate end-points in the same manner. The credentials and message encryption protect the communication between devices and the SCMS.

The security system of the SCMS is complex and intricate; due in parts to privacy protection, therefore the agency requests comments regarding the cybersecurity viability of V2V security and invites comments concerning the relationship of V2V security to the larger vehicle security universe.

e) Cybersecurity and V2V message content

While the security overlay of the V2V communications establishes confidence between authentic entities, the message content indicating the vehicle's behavior is obtained from sensors (such as GPS) and vehicle data buses. It would be possible to manipulate the sources of data to the OBE, which could send a BSM message with inaccurate message content to its surrounding. In cases, the message could be constructed intelligently that could make the messages sent from that vehicle not correspond to the sending vehicle's physical behavior.

Such manipulation could result in surrounding vehicles responding with warnings to the driver early on. The misbehavior detection mechanisms set out in this proposal are designed to detect the anomaly, however it is possible that specifically crafted messages could be delivered and accepted by safety applications.

In the case of the primary misbehavior detection proposal, the misbehaving sender would also hopefully be detected and the sender added to the CRL. However, it is important to examine what could happen if the message is not detected as misbehavior and the time period before the sending vehicle is added to CRL. OEMs treat V2V as a new sensor for the vehicle and applications designed using this message would assess the safety-risks associated with this sensing mechanism being wrong. Generally, warning systems imply less severity than active control. OEMs indicate that they would take safety-conscious approach, which would be different for different applications. They further indicate that for active control, they tend not to rely on any single sensor even in modern systems and expect that to be the same when V2V becomes available to get in the mix of their sensor suite. The impact of such malicious act would be limited vehicles within the communications range of the unit (~1,000 ft).

The broader impact on GPS or timing spoofing/jamming may have similar impacts, or result in limited denial of service. Misbehavior detection is projected to help in such cases and could also help identifying and enforcing rules against jammers.

Given there has been more reports of GPS jammers being used[168], we seek information and comment regarding how industry is addressing the GPS jamming issue. Are there techniques to identify when GPS jamming is occurring? If the GPS signal is being jammed or spoofed, does industry have plans to notify the driver, and what will be the context of the notification? During GPS jamming, will industry suspend operation of systems that rely on GPS information?

In addition, we solicit comment on whether our assessment of cybersecurity risks due to spoofed and potentially malicious BSM message data is reasonable. We also solicit input from OEMs and Suppliers on how they expect to handle potential single point failures associated with BSM signal contents. What risk-based criteria and process would be appropriate for V2V safety applications to help ensure the validity of the BSM message data received from other vehicles relative to vehicle-local sensor readings? If data from a vehicle's onboard sensors suggest a different outcome as compared to data from an incoming BSM message, how might V2V safety applications balance the trust on conflicting data? How should V2V safety applications handle a situation where incoming BSM message data is the only source of information available to make a safety decision? How does the nature of the systems' planned reaction (warning vs nature of

[168] See "GPS Under Attack as Crooks, Rogue Workers Wage Electronic War" at http://www.nbcnews.com/news/us-news/gps-under-attack-crooks-rogue-workers-wage-electronic-war-n618761 (last accessed Dec 7, 2016)

control) impact such a decision? What new vehicle sensors may be possible in the next 15-20 years that may significantly improve such sensor fusion and decision processes?

f) Cybersecurity and potential malware

One of the cybersecurity risks that needs considered is whether V2V communications could be used to insert malware to the OBE, unexpectedly change configuration, or result in unwanted behavior. Since the V2V channel will be mandated on all new cars, this medium would likely become one of the dominant wireless access points on the vehicle fleet in the field over time.

Further, it should be considered that, since the V2V protocol is based on broadcast and listen methodology, and does not establish networks between participating units the way a traditional network protocol does. Instead, communications takes place through a well-defined BSM message structure.

- It is well established that many software and hardware vulnerabilities occur at the communications interfaces of systems. Security of the interfaces must be the highest priority when developing a system. Therefore, we believe that implemented systems should provide adequate controls to prevent malformed, incomplete or erroneous messages that do not fit the specifications to pass to the OBE.

- The DARPA HACMS program has shown that formal verification can be used to mathematically prove the correctness of systems or interfaces. Formal verification uses mathematical techniques to formalize software as a mathematical proposition to be proved. While testing provides incomplete evidence of correctness, a proof guarantees correctness of the system. In an active project, we are pursuing the development of a formally verified reference parser for the V2V communication interfaces that could provide the industry guidance on one way to ensure that only expected range of BSM Part 1 and Part 2 would be accepted by the OBE. While we do not anticipate requiring the use of a formally verified parser, we expect that industry will pay attention and utilize such tools or other means to ensure that common communication interface vulnerabilities do not exist in implemented V2V units.

- NHTSA also anticipates pursuing fuzz-testing of production-level implementations of V2V hardware with and without the use of a formally verified parser. We also intend to develop a framework of test protocols and message sets that manufacturers could use to test their implementations.

- We reemphasize the importance of securing the V2V communication channel. If the V2V interface is not properly secured (whether by design or in implementation), we need to consider

the possibility of a "worm"[169] type malware where the malware could potentially self-replicate and propagate in an epidemic manner to other systems with the similar vulnerability (e.g. systems from the same manufacturer) that come into communications range. The potential imminent-safety impact of such malware would depend on many factors and most certainly depend of how the vehicle databus interfaces are designed. Even if the impact may not be safety-critical, this risk could potentially lead to large scale denial of service for the mandated V2V technology. The manufacturers should plan for detection and rapid remediation methods to address such issues. This need is similar for other wireless channels. For example, in the 2014 hacking of a Fiat-Chrysler vehicle[170], which led to eventual recall[171] of approximately 1.5 million vehicles, the researchers documented that they could have designed a vehicle worm for the cellular communication based vulnerability in that particular case.

We solicit input on whether the overall need for rapid remediation methodologies would imply different requirements for the V2V communication interfaces as opposed to others (such as cellular, Bluetooth, Wi-Fi). Further, we solicit comment that exploitation of a potential vulnerability in the V2V OBE does not immediately imply safety-critical system compromise.

The cybersecurity environment changes continually and at times rapidly. Capabilities designed into systems should take the whole lifecycle of the vehicle into account and provide for rapid response methods to potential incidents in the field. These methods could take various forms but should consider both the issue containment and practical remediation needs.

Generally, first important step is having a method to identify cybersecurity issues and share them with the broader community. We and the industry believe that the Automotive Information Sharing and Analysis Center (Auto ISAC) established in 2015 will have a major role in this respect. We anticipate that V2V related intelligence sharing through Auto-ISAC will accelerate the identification of issues and remediation actions. As part of this process, it should be foreseen that various aspects of the V2V design may need updates over the life of systems in the field, such as:

- Security certificates and protocols,
- Misbehavior detection algorithms and policies
- CRL contents and policies
- Device firmware

In the case of primary message authentication approach, the SCMS can update certificate and security protocols that are inputs to each device, but the actual software that performs the

---

[169] Worm refers to a standalone malware that replicates itself in order to spread to other systems.
[170] "Remote Exploitation of an Unaltered Passenger Vehicle", Charlie Miller and Chris Valasek. Page 48. Available at http://illmatics.com/Remote%20Car%20Hacking.pdf (last accessed Dec 7, 2016).
[171] NHTSA Recall Campaign Number: 15V461000.

security management for different devices can and will be implemented differently by different manufacturers. Each device supplier will need to manage handling of potentially required security updates. It is likely that there will need to be coordination among the SCMS and various devices suppliers to facilitate such updates. It may be the SCMS through the Misbehavior Authority that identifies the need for an update and communicates this to suppliers so that updates can be prepared.

There are many methods by which updates can be implemented. As seen with the different kind of devices that exist today, like tablets/iPads, there are various options and issues. Automated updates to computer systems can be implemented wired or wirelessly. Some of the updates; however, require consent; that screen that asks if you agree to the terms related to the update that may go on for pages. Some methods (personally updating device firmware) require technology savvy that many consumers do not possess. Others require owners bringing their cars to dealers, which are not often followed well.[172] The growing trend is towards building in capabilities for remote software updates.

According to a study released by IHS in September of 2015,[173] OEMs are going to begin implementing software updates over-the-air (OTA); similar to how smart phones are updated currently. In fact the study estimated that software-related repair might soon be able to be wirelessly installed on the vehicle without the owner ever leaving home.

Japanese OEMs pioneered navigation map updates in Japan via their telematics systems. BMW, VW, and Tesla have announced OTA procedures for updating navigation maps. In fact, both Tesla and BMW have already documented utilizing OTA updates to fix security issues onboard their vehicles.

With new vehicles having more connectivity with the internet and other wireless media, IIHS is predicting that upwards of 160 million cars will partake of OTA updates globally by 2022. In fact many of these may already be available to cars now. XM radios can potentially be utilized to download OTA updates to vehicles and in fact are pre-installed on upwards of 70 percent of all new light vehicles. 4G services, as well as onboard Wi-Fi units are penetrating further into the vehicle fleet as well.

Given that V2V operational and security software may need to be updated securely and widely while systems are in service, it may be unreasonable to expect that non-OTA software updates may have the desired impact and effectiveness (based on experiences in non-OTA domains for recalls). As such, NHTSA is soliciting feedback on whether it should consider requiring that V2V enabled vehicles have built-in OTA capability to have critical software

---

[172] According to online website Autotrader, the recall completion rate in 2015 was approximately 48 percent, down from 56 percent in 2014.

[173] "Over-the-air Software Updates to Create Boon for Automotive Market, IHS Says" at http://press.ihs.com/press-release/automotive/over-air-software-updates-create-boon-automotive-market-ihs-says (last accessed: Dec 7, 2016)

updates, and seeks comment on the practicability of requiring this in future vehicles. NHTSA also solicits feedback on whether vehicle owners should be given the option to decline critical security updates.

In addition, there will be situations when a security vulnerability may be known to NHTSA and manufacturers but not all V2V-equiped vehicles will have installed the patches or updates to mitigate the flaw. During this period, vehicles in the fleet may be vulnerable until the patch or update is installed. NHTSA is seeking comment on how this period of vulnerability should be managed, the time period over which updates or patches should be installed, how the number of patched and unpatched vehicles should be measured to determine patch adoption, and how to manage the situation when vehicles do not receive patches or user refuse to accept or agree to the update.

g) Enforcement Mechanisms

The National Highway Traffic Safety Administration (NHTSA), under the U.S. Department of Transportation, is the U.S. government agency that was established to carry out safety programs under the National Traffic and Motor Vehicle Safety Act of 1966, re-codified as Title 49 U.S.C. Chapter 301, Motor Vehicle Safety (the Vehicle Safety Act). Under that authority, NHTSA issues and enforces Federal motor vehicle safety standards (FMVSS) that apply to motor vehicles and to certain items of motor vehicle equipment. Associated regulations are found in Title 49 of the Code of Federal Regulations (CFR), Parts 500-599.

The Vehicle Safety Act requires that motor vehicles and regulated items of motor vehicle equipment as originally manufactured for sale in the United States be certified to comply with all applicable FMVSS. NHTSA does not play any part of the certification process. NHTSA does not approve any motor vehicles or motor vehicle equipment as complying with applicable FMVSS. Instead, under 49 U.S.C. 30115, each vehicle manufacturer and equipment manufacturer is ultimately responsible for certifying that its vehicles and equipment comply with all applicable FMVSS.

When establishing the FMVSS, NHTSA must ensure requirements are practicable, meet the need for motor vehicle safety, and are stated in objective terms. Each FMVSS specifies the minimum performance requirements and the objective test procedures needed by the agency to determine product compliance with those requirements.

The Office of Vehicle Safety Compliance (OVSC) is the office within NHTSA's Enforcement Division that is responsible for compliance verification testing. OVSC funds independent test laboratories throughout the United States to execute the verification tests. The verification tests are not certification tests since the vehicle manufacturers are ultimately responsible for vehicle certification, but are used to verify that tested motor vehicles appear to meet the requirements of the FMVSS. OVSC utilizes the test procedures specified in each FMVSS as the basis for developing a more detailed test procedure that includes test conditions, set-ups, test equipment, step-by-step test execution, and data tables. Each funded test laboratory

is required to utilize the OVSC test procedure to establish even more detailed test procedures with step-by-step approaches documented including check-off lists and data tables.

In most cases, when OVSC and a contracted test laboratory perform FMVSS tests, the test vehicle appears to meet the requirements of the applicable standard; however, in some instances, test failures are identified. When an apparent test failure is identified, the following steps will be followed by OVSC to resolve the possible noncompliance.

- The contracted test laboratory notifies OVSC of any potential test failure.
- The test laboratory verifies that the test procedure was executed exactly as required and that all laboratory test equipment utilized has up-to-date calibration information attached.
- The test laboratory provides detailed test results to OVSC for evaluation.
- The laboratory may be directed to recalibrate any critical test equipment to ensure proper operation.
- The vehicle manufacturer is notified of the test failure and the test data is shared.
- OVSC requests the manufacturer provide documentation and its basis for certification.
- The vehicle manufacturer may choose to conduct additional internal testing to gather additional data for evaluation.
- Meetings will be held as required with test laboratory and vehicle manufacturer personnel to identify test execution related problem or possible vehicle noncompliance.
- Additional verification tests on same vehicle or identical vehicle may be executed to validate test results.
- If noncompliance is identified and confirmed by vehicle manufacturer, the manufacturer is required to submit a 49 CFR Part 573 report of noncompliance report within five working days after a noncompliance has been determined.
- The manufacturer will work with NHTSA to ensure a fix has been developed to correct the identified noncompliance.
- Follow-up tests may be executed to verify the fix does in fact correct the problem.
- The vehicle manufacturer will work with NHTSA to ensure no new noncomplying vehicles are sold and that the vehicles on the road are recalled to fix the confirmed noncompliance.

The above steps are not necessarily in the exact order they may occur based upon the type of test failure and because many of the steps are occurring simultaneously. Furthermore, the actual steps required to resolve any potential test failure will be predicated on the technical attributes of the failure and the difficulties associated with the ultimate resolution of the problem.

h) Compliance Test Procedures

To ensure that light vehicles equipped with a V2V communications system, On Board Equipment (OBE), is interoperable and compliant with the minimum performance requirements,

the regulatory text of this proposal, Section XI, proposes static, dynamic, and simulated performance tests. These tests have the potential for evaluating the performance of the V2V Radios and verifying the accuracy of the Basic Safety Message (BSM) safety message, Part I.

NOTE: The performance metrics mentioned in this document are placeholders to illustrate what aspect of performance we could evaluate at each step of the test. The performance metrics themselves will be updated pursuant to any decision to propose x or y as a requirement.

Overall, we anticipate devices under test will be instrumented with independent measurement sensors, devices, and a data acquisition system (DAS) in order to collect V2V system data. The independent measurement equipment will collect Differential Global Positioning System (DGPS) information, vehicle speed, vehicle 3-axis accelerations, vehicle yaw rate, vehicle systems status information, and radio performance data.

IV. Public Acceptance, Privacy and Security

A. Importance of public acceptance to establishing the V2V system

In the Readiness Report, NHTSA extensively discussed the importance of consumer acceptance to the success of V2V, given that as a cooperative system that benefits from network effects, V2V depends on drivers' willingness to participate. V2V needs vehicles to be equipped in order to broadcast messages that other vehicles can "hear," but in order for equipped vehicles to join the roads, consumers must be willing to recognize the benefits of a V2V system and support its adoption by the U.S. vehicle fleet via the purchase of the new, equipped vehicles, or by adding V2V capability to their existing vehicles through aftermarket devices. Thus, consumers must *want* V2V in order for V2V to reach its full potential. If consumers avoid the technology for some reason, it will take longer to achieve the network effect, and safety benefits will be slower to accrue.

Additionally, the courts have determined that public acceptance of a mandated technology is necessary to ensure that the mandate fulfills the requirements of the Safety Act. As discussed further in Section V.C below, if the public rejects a technology that the agency has required for new vehicles, the courts have found that the standard may neither be practicable nor meet the need for safety in the absence of public acceptance. If vehicle manufacturers literally cannot sell V2V-equipped vehicles because consumers *en masse* refuse to buy them, then it is possible that a court would conclude that the standard was not consistent with the Safety Act.

NHTSA must therefore consider the potential elements of a V2V requirement that may affect public acceptance, and do what we can to address them, both through carefully considering how we develop the mandate, and through consumer education to improve understanding of what the technology does and does not do. Additionally, we expect, simultaneously, that vehicle manufacturers subject to the eventual mandate will likewise work to improve public understanding of the benefits of V2V, boosting consumer acceptance overall. We also seek

comment on the extent to which an if-equipped approach potentially may alleviate some consumer acceptance concerns.

B. Elements that can affect public acceptance in the V2V context

Based on our review of the research conducted so far and the responses to the ANPRM and Readiness Report, NHTSA believes that the several elements of the V2V system discussed below may affect public acceptance.

1. False positives

A "false positive" occurs when a warning is issued to a driver and the warning is unnecessary (or when the driver believes the warning is unnecessary), because there is no immediate safety risk that the driver has not already accounted for. False positives can startle and, if there are too many, annoy a driver, causing drivers to possibly lose confidence in the system's ability to warn them properly of danger and desire to have the warning disabled; reducing overall system benefits. If the driver does not notice immediately that a false positive is in fact false, the driver might carry out an unnecessary evasive maneuver, potentially increasing the risk of an accident.

In the SPMD, we initially saw fairly high numbers of false positive warnings for some V2V applications.[174] Further analysis indicated this was due largely to the fact that the safety applications under evaluation were still prototypes. Part of the goal of the SPMD was to provide vehicle manufacturers with the opportunity to gain real-world experience with V2V safety applications; providing the opportunity to improve their "tuning" to maximize safety while minimizing false positives. Driver complaints, particularly regarding IMA warnings triggered by cloverleaf highway on-ramps and elevated roads that crossed over other roadways, led manufacturers to adjust the safety applications to accommodate the these originally-unexpected "warning" conditions. The SPMD experience proved that these adjustments significantly reduced false positive warnings for this application.

At this time, NHTSA cannot account preemptively for the possibility of future false positive warnings. Given that we are only proposing today to mandate V2V transmission capability and are not yet requiring specific safety applications, we are not developing requirements for how safety applications must perform, and we recognize that doing so would be a significant undertaking. We do expect, however, that manufacturers will voluntarily develop and install safety applications once V2V communications capability is required available. As with existing advanced crash avoidance systems and as in the SPMD, we expect manufacturers

[174] See, e.g., Nodine et al., "Independent Evaluation of Light-Vehicle Safety Applications Based on Vehicle-to-Vehicle Communications Used in the 2012-2013 Safety Pilot Model Deployment," USDOT Volpe Center, DOT HS 812 222, December 2015, Section 5.1. Available at Docket NHTSA-2016-0126.

to address false positive issues that arise in use in order to improve customer satisfaction. Because false positive issues with V2V-based safety applications are typically a software issue rather than a hardware issue Manufacturers may even be able to solve by deploying solutions to such problems through over-the-air software updates, rather than requiring vehicles to be brought in for adjustment. Data from the SPMD suggests that it is possible to reduce false positives in production safety applications and thus we believe it should not pose a significant public acceptance issue for V2V. Additionally, if NHTSA determines in the future that false positives in the field create an unreasonable risk to safety, NHTSA could pursue remedies for them through its enforcement authority.

2. Privacy

If consumers fear that V2V communications will allow their movements to be "tracked," either for government or private purposes, and that such information could be used to their detriment, they may avoid buying new cars with V2V systems installed, or attempt to disable the V2V systems in their own vehicles. Concerns about privacy directly implicate consumer acceptance. For this reason, in addition to NHTSA's obligation under federal privacy law to identify the privacy impacts stemming from its regulatory activities,[175] the Agency also must consider consumer privacy carefully in our development of V2V requirements. For example, as discussed above, SAE J2735 BSM specification contains a series of optional data elements, such as vehicle identification number (VIN), intended to be broadcast as part of the V2V transmission that enables safety applications. Because the Agency has determined that transmission of VIN and other information that directly identifies a specific vehicle or its driver or owner could create significant privacy risks for private consumers, this proposal contains performance requirements that exclude from the BSM such explicitly identifying data. The Agency also is concerned that other data elements in the BSM potentially could be used to identify specific individuals when combined over time and with data sources outside of the V2V system. For this reason, we have proposed a more general exclusion of "reasonably linkable" data elements from the BSM to minimize consumer privacy risk that could result from associating BSMs with specific individuals. We discuss our privacy risk analysis in more in detail in Sections IV.C and IV.D, and in the draft PIA published concurrent with this NPRM.

NHTSA expects manufacturers to pursue a privacy positive approach to implementing the proposed V2V requirements. In furtherance of the Fair Information Practice Principles (FIPPs), especially those of transparency and notice, we have developed a draft privacy statement that we will require manufacturers to provide to consumers, included in the regulatory text below. In order to ensure effective notice, we intend for manufacturers to provide this statement to consumers in understandable, accessible formats and at multiple easily identifiable locations and times, including but not limited to the time of sale. We seek comment from the public on the most effective time and means of providing such multi-layered notice to

[175] Section 522 of the Consolidated Appropriations Act, 2005, Pub. L. 108-447

individuals purchasing new and used vehicles with V2V systems. We note that the industry has developed a set of voluntary privacy principles for vehicle technologies and services, which have been accepted by members of both the Alliance and Global Automakers, covering the significant majority of motor vehicle manufacturers.[176] We also seek comment from the public on how these principles would apply to V2V communications, as detailed in this NPRM, and the extent to which application of these voluntary minimum principles in the V2V context would provide adequate notice and transparency to consumers.

To date, vehicle technologies that have raised privacy concerns for consumers have been "opt-in," meaning that either consumers expressly agree to the use of these technologies in their vehicles (and thereby provide explicit consent) or consumer purchase vehicles containing technologies not mandated by NHTSA (and thereby, arguably, provide implicit consent). V2V presents a somewhat different situation, as we are proposing that at least 50 percent of new vehicles will be required to have V2V devices starting in model year 2021. Since this would be a mandated technology, consumer choice will be limited to the decision of whether or not to purchase a new car (all of which eventually would contain V2V technology, if mandated). From a privacy perspective, such implicit consent is not an optimal implementation of the FIPPs principle of consumer choice. However, as discussed below in Section VI.C., the agency has determined that there are no viable alternatives to a mandate of V2V technology. In the agency's view, the absence of consumer choice is required to achieve safety in the V2V context, increasing the significance of ensuring that industry deploys V2V technology in a privacy positive, transparent manner and provides consumers with effective, multi-layered privacy notice. Consumers who are privacy-sensitive tend to feel more strongly when the government is mandating something that creates potential privacy risks to individuals, as compared to when they voluntarily choose whether to purchase and use such technology. NHTSA and vehicle manufacturers will continue to work to ensure that V2V does not create the type of privacy impacts frequently raised in comments, and will need to educate consumers about the potential privacy impacts and privacy-enhancing controls designed into the V2V system. That said, NHTSA seeks comment on the extent to which an if-equipped approach potentially may provide consumers with more of a choice to "opt in" to V2V technology – or whether, if mandated, consumers should be provided an "opt out" option for privacy reasons.

3. Hacking (cybersecurity)

If consumers fear that V2V will allow wrongdoers to break into their vehicle's computerized systems and take control of vehicle operation, then, as with privacy concerns, they may avoid purchasing new vehicles equipped with V2V or attempt to remove already-installed V2V in their own vehicles. This fear is really a two-part concern: (1) that V2V equipment can be "hacked," and (2) that *if* V2V equipment can be hacked, the consumer's safety may be at risk.

---

[176] "PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES" available at http://www.autoalliance.org/?objectid=865F3AC0-68FD-11E4-866D000C296BA163 (last accessed dec 7, 2016).

Regarding the concern that V2V equipment can be hacked, as discussed in much more detail in Section III.E.7 above, counter measures have been identified using a risk-based approach to determine the types of threats and risks to the equipment that may occur. We are proposing to require additional hardening of the on-board V2V equipment beyond normal automotive-grade specifications to help reduce the chance of physical compromise of V2V. In addition we have included alternatives for message authentication and misbehavior reporting to solicit comment regarding to further reduction of cybersecurity risk in V2V message exchange. We seek comment on what additional requirements, if any, we might consider adding to the standard to mitigate infiltration risk yet further. If commenters believe additional steps are needed, we ask that they describe the protection mechanism and/or approach as fully as possible, and also provide cost information to accomplish them – or whether, if mandated, consumers should be provided anoption to disable V2V for cybersecurity reasons.

Regarding the concern that V2V equipment, if hacked, can create a safety risk, NHTSA expects manufacturers to ensure that vehicle systems take appropriate safe steps to the maximum extent possible, even when an attack may be successful.[177] These can include protective/preventive measures and techniques like isolation of safety-critical control systems networks or encryption and other hardware and software solutions that lower the likelihood of a successful hack and diminish the potential impact of a successful hack; real-time intrusion detection measures that continually monitor signatures of potential intrusions in the electronic system architecture; real-time response methods that mitigate the potential adverse effects of a successful hack, preserving to the extent possible the driver's ability to control the vehicle; and information sharing and analysis of successful hacks by affected parties, development of a fix, and dissemination of the fix to all relevant stakeholders. In July 2015, in response to NHTSA's challenge, the auto industry created an Information Sharing and Analysis Center ("ISAC") to help the industry proactively and uniformly address cybersecurity threats, and we would expect that such a body could be a useful forum for addressing V2V-related security risks, if any. A number of auto manufacturers are also rapidly ramping up internal teams to identity and address cybersecurity risks associated with new technologies.[178]

In March 2014, researchers from Galois, Inc. issued a white paper with specific recommendations for reducing security risk associated with V2V communications, which they

[177] Additional information about NHTSA's approach to automotive cybersecurity is available at http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity (last accessed Sept. 23, 2015).

[178] See, e.g., King, Rachel, "GM Grapples with Big Data, Cybersecurity in Vehicle Broadband Connections," Wall Street Journal, Feb. 10, 2015. Available at http://blogs.wsj.com/cio/2015/02/10/gm-grapples-with-big-data-cybersecurity-in-vehicle-broadband-connections/ (last accessed Dec 7, 2016).

stated would "automatically rule out a whole class of security vulnerabilities" at low cost with known technologies.[179] The recommendations were as follows:

- All legal inputs shall be specified precisely using a grammar. Inputs shall only represent data, not computation, and all data types shall be unambiguous (i.e., not machine-dependent). Maximum sizes shall be specified to help reduce denial-of-service and overflow attacks.
- Every input shall be checked to confirm that it conforms to the input specification. Interface messages shall be traceable to mission-critical functionality. Non-required messages should be rejected.
- Parsers and serializers shall be generated, not hand-written, to ensure they do not themselves introduce any security vulnerabilities. Evidence should be provided that
    - *parse(serialize(m)) = m*, for all messages *m*, and
    - parse(i) = REJECT, for all non-valid inputs i.
- Fuzz testing shall be used to demonstrate that implementations are resilient to malicious inputs.
- A standardized crypto solution such as AES-GCM shall be used to ensure confidentiality, integrity, and the impossibility of reply attacks.

DARPA staff, in discussing V2V cybersecurity issues with DOT researchers, recommended these techniques be included in any V2V requirements going. NHTSA seeks comment on whether these specific techniques should be incorporated into the proposed FMVSS requirements, and if so, how; alternatively, NHTSA seeks comment on whether these techniques should be incorporated prior to vehicle manufacturer certification with the FMVSS, and if so, how, and how NHTSA would verify their incorporation.

4. Health

As discussed in more detail below in Section IV.E, a number of individual citizens commented to the ANPRM and Readiness Report that they were concerned about what they believed to be potentially negative health effects that could result from a DSRC mandate. As discussed in Section IV.E below, NHTSA has considered this issue carefully, and whether there are ways to mitigate these concerns without obviating the very real safety benefits that a V2V mandate will enable. We believe that consumer education, undertaken both by the Federal government and by vehicle manufacturers, may help to alleviate some of these concerns.

---

[179] See Launchbury, John, Dylan McNamee, and Lee Pike, Galois Inc., "A Technique for Secure Vehicle-to-Vehicle Communication," Mar. 9, 2014. Available at http://galois.com/wp-content/uploads/2014/07/whitepaper_SecureInterfaces.pdf (last accessed Dec 7, 2016).

5. Research conducted on consumer acceptance issues

Working with Booz Allen Hamilton, NHTSA has conducted additional research on consumer acceptance issues since the ANPRM and Readiness Report. The objective of the research was to conduct both qualitative and quantitative research to broaden our understanding of consumers' acceptance of V2V technology and to inform future outreach and communication efforts to the public. The qualitative phase included focus groups held in Spring of 2015. Focus group participants were shown a brief video on what V2V communications are, how they work, and how they contribute to vehicle safety, and then asked to discuss a series of questions about the technology, their understanding of it and interest in it, and benefits and drawbacks. Overall, on a scale of 1 to 10, the majority of focus group participants rated their interest in V2V as a 5 or higher for the next car. However, participants also expressed concern that the technology would not be effective if it were not universally adopted, and that over-reliance on or distraction by V2V warnings could cause drivers to become less attentive and increase risk. Although most focus group participants believed that V2V would allow drivers to be tracked, few were concerned with the privacy implications of tracking.[180]

Following the conclusion of the focus groups and analysis of their findings, a survey was developed for online quantitative testing to examine these issues further. The survey was conducted by Ipsos, under contract to BAH. The survey sought to evaluate several objectives:

- What is the degree of public acceptance of V2V?
- What proportion of people are concerned about each barrier? How much importance is attached to that concern?
- What proportion of people agree with the potential benefits of V2V? How much importance is attached to that benefit?
- How does the population differ on the above viewpoints (age, gender, urbanicity, etc.)?
- What are predictors of acceptance of V2V technology (age, gender, urbanicity, etc.)?

Over 1,500 people responded to the survey, and the sample was matched to the target population on age, gender, ethnicity, income, and region. Respondents viewed a brief informational video about V2V, and then answered 35 questions. Approximately half of respondents were interested in having V2V in their next car, with "accepters" tending to be male, older, urban, and more educated. All responses had a margin of error of +/- 2.5 percent

[180] "Vehicle to Vehicle Crash Avoidance Safety Technology: Public Acceptance Final Report" December, 2015. Available at Docket No. NHTSA-2016-0126

In terms of barriers or concerns, 69 percent of respondents believed that V2V would encourage other drivers to be too reliant and less attentive to the driving task, and over 50 percent expressed concern about cybersecurity and the need for enough vehicles to be equipped for the benefits to accrue. Between 30 and 40 percent expressed concern about tracking by the government or law enforcement and about the risk that they themselves could become too reliant and inattentive to driving. Only 20 percent expressed concern about health risk from electromagnetic activity. Of those concerns, however, some were deemed more important than others (that is, simply because respondents identified a risk, did not necessarily mean that they considered it an important risk). Respondents viewed law enforcement and government tracking as less important, but cybersecurity, other drivers' inattentiveness, and health risks as more important, when they were concerned about them.

In terms of benefits of V2V, 55 percent of respondents believed that V2V would reduce the number and severity of vehicle crashes, 53 percent believed that it would make driving more convenient and efficient, and 50 percent believed that V2V could lower insurance rates. As for barriers, respondents tended to believe that benefits for others would be somewhat greater than the benefits that they themselves would experience. Importance did not vary as much for benefits as it did for barriers.

In terms of how opinions about benefits and barriers correspond to whether a respondent wanted V2V in their next car, the survey results found that, on balance, all respondents were concerned about barriers, but "accepters" of V2V rated the benefits more highly. When asked how much they would be willing to pay for V2V, 78 percent of respondents were willing to pay less than $200.

Based on the research conducted thus far and assuming that the survey respondents are, as intended, reasonably representative of the nation as a whole, it appears that while there may be work yet for the agency and manufacturers to do in order to reassure consumers of V2V's benefits, there may not be a sufficient public acceptance problem that an FMVSS requiring V2V communications in new vehicles would face clear legal risk on that issue. NHTSA intends to continue researching approaches to consumer outreach on V2V and will work with industry and other relevant stakeholders in doing so. We seek comment on what the agency should consider in developing those approaches to best ensure the success of a future V2V system.

6. User flexibilities for participation in system

In the ANPRM, we sought comment on whether there were any issues relating to consumer acceptance that the agency had *not* yet considered, and asked how the agency should consider them for the NPRM. In response, a number of individual commenters expressed concern that they experience extreme sensitivity to electromagnetic radiation, and that therefore DSRC should not be mandated, or that if it was mandated, that the agency should allow drivers to disable it. Health issues raised in comments are covered below in Section IV.E, but the question of whether the agency should require or permit an "off switch" for V2V communications arose when commenters suggested it as a way to mitigate concerns over health effects. A handful of other individual commenters stated that the agency should allow drivers to

turn off DSRC for privacy or security reasons, out of concern that DSRC transmissions could allow their movements to be tracked, or that the device could be hacked by malicious third parties to obtain personal information about the driver. A number of individual commenters raising these concerns about health or tracking suggested that they would attempt to disable V2V in their vehicles, or only purchase older vehicles without V2V.

While NHTSA had asked in the ANPRM whether commenters had thoughts regarding whether V2V-based *warnings* should be permitted to be modified or disabled,[181] in the interest of maximizing safety benefits, NHTSA had not considered allowing manufacturers to provide consumers with a mechanism to disable V2V itself, whether temporarily or permanently.

Generally, if NHTSA concludes that a vehicle system or technology provides sufficient safety benefits that it should be required as an FMVSS, NHTSA has not permitted it to be disabled. In fact, Congress expressly prohibits manufacturers, distributors, dealers, and motor vehicle repair businesses from knowingly making inoperative any part of a device or element of design installed on or in a motor vehicle in compliance with an applicable motor vehicle safety standard prescribed by NHTSA.[182] In some cases, however, NHTSA has established FMVSSs that permit system disablement or alteration when there is a clearly-defined safety need for doing so.

For example, FMVSS No. 126 for electronic stability control (ESC) allows manufacturers to include an "ESC Off" control that puts the system in a state where ESC does not meet the FMVSS performance requirements, as long as the system defaults to full ESC capability at the start of the next ignition cycle and illuminates a telltale in the meantime to warn the driver that ESC is not available.[183] NHTSA allowed the ESC Off control because we were aware that in certain driving situations, ESC activation could actually make driving *less* safe rather than *more* safe – if a driver is stuck in deep snow or sand and is trying to free their vehicle, quickly spinning wheels could cause ESC to activate when it should not. Additionally, the agency was concerned that drivers who did not have the option of disabling ESC when absolutely necessary might find their own, permanent way to disable ESC completely. Having an off switch that reverted to full functionality at the next ignition cycle at least allowed ESC to continue providing safety benefits the rest of the time. NHTSA concluded that allowing temporary disablement was better than risking the permanent loss of safety benefits.[184]

---

[181] *See* 79 Fed. Reg. 49270, at 49272 (Aug. 20, 2014) (Question 13 in the ANPRM asks whether commenters believe that V2V-based warnings should be permitted to be modified or disabled)
[182] *See* 49 U.S.C. 30122(b).
[183] *See* 49 CFR part 126, S5.4. We note that despite the overarching requirement to return to full functionality at the new ignition cycle, S5.4 does not require ESC to return to full functionality if the vehicle is in a mode for "low-speed, off-road driving," or if the front and rear axles are locked because the vehicle is in some sort of 4WD mode.
[184] 72 Fed. Reg. at 17279-80 (Apr. 6, 2007).

As another example, FMVSS No. 208 for occupant crash protection allowed manufacturers to include a device up until September 1, 2012, that deactivated the right front passenger seat air bag, but only in vehicles without a second row of seating, or in vehicles where the second row of seating is smaller than a specified size.[185] Like the ESC Off function, the "passenger air bag off" function also requires a telltale to illuminate to warn the driver that the air bag is disabled; unlike the ESC Off function, the passenger air bag off function, if present, remains deactivated until it is reactivated by means of the deactivation device (i.e., the driver presses the button again, rather than the air bag simply reactivating at the start of the next ignition cycle).[186] In establishing this option, the agency noted public acceptance issues with advanced air bags, and stated that allowing on-off switches for some period after all vehicles were equipped with advanced air bags would help parents feel more confident about the system's reliability based on real-world experience.[187]

Thus, in prior instances when NHTSA has allowed drivers the option of changing or disabling the functionality of a required safety system, it has been in the interest of providing *more* safety. Similarly, were V2V to impose substantial new safety risks, there could be a safety reason to disable transmission and reception of messages. To the extent that consumers may wish that the agency allow a way for them to disable V2V because of concerns about privacy or cybersecurity, we reiterate our position as discussed in Sections IV.B and IV.C on privacy and Section V on security we have worked to design requirements that reduce the possibility of such threats. To the extent that consumers wish a mechanism to disable V2V devices out of concern over potential health effects, we note simply that disabling your own V2V unit would not help you avoid V2V transmissions, because other light vehicles will also be equipped with the technology, and if you have your own vehicle it is presumably for the purpose of traveling to places where other vehicles also go. Turning V2V off for this reason would forfeit the safety benefit of being "seen" by other vehicles" and "seeing" other vehicles, without providing any other benefit.

Moreover, unlike for most of the prior technologies in which NHTSA allowed drivers the option of changing or disabling the functionality of a required safety system, allowing V2V communications to be disabled would affect the safety of more drivers than just the driver who turned off their own V2V device. A cooperative system like V2V protects you by making you more "visible" to other drivers and by letting you know when they pose imminent risks to you. A driver who disables V2V on their vehicle makes their vehicle less visible to other drivers,

---

[185] *See* 49 CFR part 208, S4.5.4.

[186] *Id*.

[187] Deactivation of the "advanced" right front passenger air bag was primarily intended to address the possibility that, in vehicles with no (or very small) back seats, a child seat might have to be placed in the front passenger seat rather than in the back. The primary mechanism to mitigate the risk of the front passenger air bag deploying when a child seat is present is a suppression system, but the agency allowed vehicle manufacturers to include an off switch for several years to improve parents' confidence that the suppression systems were working successfully in the field. *See* 65 FR at 30723 (May 12, 2000).

potentially affecting their own relative safety risk and the safety risk to those around them. The safety benefits from a cooperative system could be undermined by allowing drivers to opt out. If there is no safety benefit from opting out, and doing so would undermine safety benefits both for the driver who opts out and for drivers around them, opting out may not be justified.

However, V2V is a novel technology concept in the transportation context, which differs in some ways from other technologies covered by the FMVSS. NHTSA recognizes that, as discussed elsewhere in this notice, any technology that is required to transmit and receive information on a persistent basis creates potential privacy and cybersecurity risks. NHTSA is making every effort to reduce these risks while setting requirements that would provide life-saving benefits. That said, we acknowledge that there may be circumstances when there could be a need to deactivate the V2V device on a vehicle. These may include individuals or groups with specific privacy needs, the emergence of unanticipated cybersecurity threats, or other reasons. To address these cases, NHTSA is requesting comment on possible approaches to deactivating V2V related hardware and software as and when appropriate, as well as the costs and benefits of such approaches. These could include deactivations initiated by drivers, manufacturers, or the government; with different scopes, such as vehicle-specific or broader deactivations; with different lengths, such as for a single key start or more long-lasting; and with different levels of ease, such as an accessible consumer-friendly method or one that would require mechanical expertise.

C. Consumer Privacy

NHTSA takes consumer privacy very seriously. Although collection of data by on-board systems such as Event Data Recorders and On-Board Diagnostic systems is nothing new, the connectivity proposed by the Agency will expand the data transmitted and received by cars. V2V systems will create and transmit data about driver behavior and the surrounding environment not currently available from most on-board systems. For this reason, V2V and future vehicle to infrastructure and pedestrian (V2X) technologies raise important privacy questions.

The agency is committed to regulating V2V communications in a manner that both protects individuals and promotes this important safety technology. NHTSA has worked closely with experts and our industry research partners (CAMP and the VIIC) to design and deploy a V2V system that helps protect consumer privacy. As conceived, the system will contain multiple technical, physical, and organizational controls to reduce privacy risks – including those related to vehicle tracking by individuals and government or commercial entities. As proposed, V2V messages will not contain information directly identifying a vehicle (as through VIN, license plate or registration information) or its driver or owner (as through name, address or driver's license number), or data "linkable, as practical matter," or "reasonably linkable" to an individual. NHTSA intends for these terms to have the same meaning, specifically: capable of being used to identify a specific person on a persistent basis without unreasonable cost or effort, either in real time or retrospectively, given available data sources. Our research to date suggests that using V2V transmissions to track the path and activities of identified drivers or owners, while possible,

could be a complex undertaking and may require significant resources and effort.[188] The Agency has concluded that excluding "reasonably linkable" data elements from the BSM will help protect consumer privacy appropriately and meaningfully while still providing V2V systems in vehicles with sufficient information to enable crash-avoidance safety applications.

We request comment on the proposed mandate that the BSM exclude data elements "reasonably linkable" to an individual (as that term is defined above) and whether this appropriately balances consumer privacy with safety. Additionally, will exclusion from the BSM of "reasonably linkable" data elements undermine the need for a standard BSM data set in furtherance of interoperability or exclude data required for safety applications?

NHTSA, with the support of the DOT Privacy Officer and NHTSA's Office of the Chief Information Officer, conducted an interim privacy risk assessment of the V2V system prior to issuance of the Readiness Report and ANPRM. The interim assessment was intended to provide the structure and serve as a starting point for NHTSA's planned PIA, which is a more in-depth assessment of potential privacy impacts to consumer privacy that might stem from a V2V regulatory action, and of the system controls that mitigate those risks. On the basis of then available information and stated assumptions, NHTSA's interim privacy assessment identified the system's business needs, relevant system functions, areas of potential risks, and existing/other risk-mitigating technical and policy controls.

NHTSA received a significant number of comments on the issue of privacy in response to the ANPRM and Readiness Report. Generally, the privacy comments related to consumer acceptance and reflected consumer and industry concerns that the V2V system would be used by government and commercial entities to track the route or activities of individuals, or would be perceived by individuals to have that capability. A vast majority of the privacy comments addressed one or more of the following areas:

1. NHTSA's privacy impact assessment;
2. "privacy by design" and data privacy protections;
3. data access and privacy;
4. consumer education; and
5. Congressional or other government action related to V2V data.

Since receiving these comments, NHTSA has worked closely with privacy experts to identify and prioritize for further analysis specific areas of potential privacy impact in the V2V system. Additional privacy research, such as dynamic modeling related to location tracking and

---

[188] See Reports: FHWA-JPO-15-237 – "Final Design Analysis Report"September 18, 2015, FHWA-JPO-15-236 – "Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework (Final-Rev A)" February 24,2016, FHWA-JPO-15-235– "Final Requirements Report" September 11, 2015, and "Technical Memorandum: Modeling and simulation of Areas of Potential V2V Privacy Risk"March 8, 2016 located in Docket No. NHTSA-2016-0126

analysis of PKI best practices, is underway that will refine NHTSA's approach to mitigating potential privacy impacts stemming from the V2V system. On the basis of the PIA, comments received on the NPRM and PIA, and ongoing privacy research, agency decision-makers will be in an informed position to determine whether any residual risk (i.e., risk in the system that cannot reasonably be mitigated) is acceptable – and, in the alternative, whether functionality should be sacrificed in order to achieve an acceptable level of residual risk, and if so, what functionality.

1. NHTSA's PIA

Over a dozen organizations requested that NHTSA conduct a privacy impact assessment (PIA) of the V2V system as proposed in the NPRM. Many of these commenters noted additionally that a PIA will be critical to consumer acceptance of V2V. Several organizations requested that NHTSA take steps (in addition to conducting a PIA) to help enhance and speed consumer acceptance of V2V technologies. Comments relating to the scope of NHTSA's PIA included a request that NHTSA broaden the scope of its privacy analysis to include privacy impacts associated with vehicle to infrastructure (V2I) and vehicle to "other" (such as pedestrians) (V2X) applications, and also that NHTSA release privacy research underlying its PIA.

The Alliance of Automobile Manufacturers (Alliance) suggested that NHTSA hold public workshops with the Federal Trade Commission (FTC) to thoroughly investigate privacy issues related to the V2V system. It also recommended that NHTSA expand the scope of the PIA so that it "considers all possible uses of the envisioned transportation communications network including all potential internal and external abuses, and other challenges not solely those concerned with safety, mobility and the environment." The Automotive Safety Council recommended that an independent third party review the PIA. Finally, the Electronic Frontier Foundation (EFF) and Privacy Rights Clearinghouse requested that NHTSA release all initial risk assessments and research on which its initial risk assessment and PIA are based, including those related to location tracking and identification capabilities. Additionally, the Alliance took the position that PIA should analyze the privacy concerns relating to the broader V2X communications infrastructure, which includes commercial venture, law enforcement, and taxation issues. The FTC requested that NHTSA take into account the Fair Information Practice Principles (FIPPs) framework in regulating the V2V system.

NHTSA agrees with commenters emphasizing the critical importance of issuing a PIA detailing the agency's analysis of the potential privacy impacts of the V2V system as proposed in the NPRM. Not only is NHTSA required by law[189] to do so, but the FIPPs-based privacy-risk analysis documented in the PIA has informed NHTSA's proposal significantly, and helped to refine the privacy controls that NHTSA and its research partners designed into the V2V system to mitigate potential privacy impacts, including that related to vehicle tracking. NHTSA intends

[189] Section 522 of the Consolidated Appropriations Act, 2005, Pub. L. 108-447

to work closely with the FTC, which is the primary federal agency with authority over consumer privacy and data security, on consumer privacy issues related to theV2V system. Such intra-governmental collaboration is likely to include coordination on the PIA and ongoing privacy research. It may also include conducting joint public meetings or workshops with stakeholders following issuance of the NPRM and PIA, which has undergone intra-governmental review. For a variety of reasons, NHTSA did not (and could not) have it reviewed by non-governmental third parties prior to publication. However, NHTSA looks forward to receiving comments on the privacy issues discussed in the NPRM and PIA from a broad range of stakeholders and other interested entities.

With regard to the scope of NHTSA's PIA, the agency wishes to emphasize that, to the extent possible in the context of a still evolving V2V ecosystem, our PIA intentionally is scoped to take into account potential internal and external threat actors and potential abuses of the V2V system -- not solely those directly related to safety, mobility or environmental applications. As discussed in the PIA Summary section below, NHTSA's PIA focusses not on specific V2V system components or applications. Rather, it focuses on data transactions system-wide that could have privacy impacts, and the controls that mitigate those potential impacts. To the extent that specific V2V data transactions might be vulnerable to privacy impacts, our risk-analysis broadly considers potential threats posed by a wide range of internal and external actors, including foreign governments, commercial non-government entities, other non-governmental entities (such as research/academic actors and malicious individuals or groups). Additionally, our analysis takes into account potential privacy impacts posed by internal V2V system actors.

2. Privacy by Design and Data Privacy Protections

Many commenters requested that NHTSA deploy the V2V system in a way that ensures drivers' privacy and the security of the system. Some sought specific privacy protections, such as "total anonymity" if drivers cannot opt out of the V2V system, the protection of any PII associated with the system, and avoidance of using any PII at all. Commenters also sought end-to-end encryption of any PII, no local or remote V2V data storage, and limitations on V2V data collection, as well as technical and administrative safeguards on any V2V data collected.

Mercedes-Benz commented that the security entity envisioned to secure the V2V system, called the Security Credential Management Server (SCMS), must have security and privacy controls to protect against external threats and internal abuses. Fiat Chrysler Automobiles (FCA) expressed concern about the potential privacy impacts of the security system's design, called the certificate revocation list (CRL). The National Motorists Association emphasized safeguarding V2V messages sent via mandated V2V devices. Infineon Technologies pointed out that the unique cellular subscriber number would defeat the privacy and tracking requirement in the system, as proposed, to the extent that cellular is used as a V2V communications media. American Trucking Association requested that NHTSA protect the confidentiality of proprietary information, such as lane density, vehicle specifications, and trip origin and destination. The Association of Global Automakers (Global) and GM stated that V2V, as envisioned, does not pose significant risks to the privacy of individuals. By contrast, EFF stated the exact opposite,

noting its concern that the V2V system as discussed in the ANPRM and Readiness Report does not protect the privacy of drivers adequately.

Based on our exploration of privacy impacts and analysis of the V2V system design to date, we respectfully disagree with the position espoused by EFF that the V2V system fails to protect driver privacy. The system contains multiple technical and organizational controls to help mitigate unreasonable privacy risks posed by external actors including those posed by SCMS insiders. V2V transmissions would exclude data directly identifying a private motor vehicle or its driver or owner and reasonably linkable to an individual via data sources outside of the V2V system or over time. V2V devices would transmit safety information in only a limited geographical range. Neither the V2V system, nor its components (including OBEs) would collect or store the contents of messages sent or received, except for a limited time to maintain awareness of nearby vehicles for safety purposes or case of device malfunction. Additionally, the system described in our proposal would be protected by a complex PKI security infrastructure designed specifically to help mitigate privacy impacts and create a secure V2V environment in which motorists who do not know one another can participate in the system without personally identifying themselves or their vehicles.

As discussed in the PIA and demonstrated by the data flows detailed in that document, the CRL discussed in the misbehavior reporting section of our primary proposal also would be designed to mitigate privacy impacts to individuals. It would contain specific information sufficient to permit V2V devices to use certificate information to recognize safety messages that should be ignored, if received. However, the CRL would not contain identifying information about specific vehicles or specific certificate numbers – nor would the information on the CRL permit third parties or SCMS insiders to identify specific vehicles or their owners or drivers.

The Agency understands that concern about whether the V2V system can or will be used by government and commercial entities to track the route or activities of individuals is critical to consumer acceptance and the viability of NHTSA's proposal. DOT is continuing to work with privacy experts to identify additional controls that might further mitigate any privacy risks (including that of tracking) in the V2V system, no matter how remote. The planned implementation by DOT of a proof of concept (PoC) security entity (discussed in Section V.B.6.e)) and related policy research will provide an operational environment in which to continue to explore the viability of additional privacy controls applicable to the V2V system, as currently envisioned and designed.

That said, as we noted in the Readiness Report, it is important to emphasize that residual risk stemming from the V2V system will never be zero due in part to the inherent complexity of the V2V system design and the diversity/large number of interacting components/entities, both technological and human. Additionally, technology changes at a rapid pace and may adversely impact system controls designed to help protect privacy in unforeseen ways. For these reasons, as is standard practice in both the public and private sectors, NHTSA has performed a PIA to identify potential areas of residual risk and resulting privacy consequences/harms that might result from its proposal. The current status of NHTSA's PIA is summarized below. The technical framework for the V2V system has gone through many iterations and adjustments

during the conduct of the V2V research program, as the system has evolved to meet revised or additional needs and to incorporate the results of research. For this reason, while the current technical framework is sufficient for purposes of NHTSA's rulemaking proposal, DOT's assessment of the potential privacy impacts that could result from the V2V proposal necessarily will be an ongoing process that takes into account future adjustments to the technology and security system required to support the technology, as well as ongoing privacy research. After reviewing comments on the NPRM and PIA and working closely with the FTC and stakeholders to address privacy concerns, NHTSA will issue an updated PIA concurrent with its issuance of a V2V final rule.

3. Data Access, Data Use and Privacy

The issue of data ownership arose in the comments of Ford, Auto Care Association, and others. All of these commenters requested clarification of who owns the data generated by the V2V system. Many commenters asserted that vehicle owners should own V2V and other data generated by motor vehicles, generally. Systems Research Associates requested a specific regulation vesting ownership in vehicle owners, not manufacturers. Another commenter expressed concern about ownership of data inherent in the context of car sharing and rentals arrangements.

The inherently related concept of consumer consent also appeared in many privacy comments. Civil liberties organizations suggested that NHTSA mandate that consumers provide "active consent" in the form of express written consent before manufacturers may collect data containing personally identifiable information (PII). Manufacturers requested that NHTSA ensure transparency by requiring that consumers authorize collection of PII through either consent or contract, and that manufacturers inform vehicle owners of what information will be collected and how this information will be used. This approach to transparency is consistent with industry privacy principles adopted in 2014 by members of the Alliance and the Association of Global Automakers, entitled "Consumer Privacy Protection Principles for Vehicle Technologies and Services" (OEM Privacy Principles or Principles), discussed in prior sections. Several manufacturers and civil liberties organizations, including EPIC and EFF, suggested that these voluntary industry principles should serve as a baseline for data privacy protections in the V2V context. EPIC also suggested that NHTSA follow the White House's Consumer Privacy Bill of Rights.

NHTSA feels strongly that in the context a V2V system based on broadcast messages, the critical consumer privacy issue is not that of data ownership, but that of data access and use – ensuring that the consumer has clear, understandable and transparent notice of the makeup of the V2V message broadcast by mandated V2V equipment, who may access V2V messages emanating from a consumer's motor vehicle, and how the data in V2V messages may be collected and used. For this reason, NHTSA proposes that motor vehicle manufacturers, at a minimum, include the following standard V2V Privacy Statement (set forth below) in all owner's manuals (regardless of media) and on a publicly-accessible web location that current and future owners may search by make/model/year to obtain the data access and privacy policies applicable to their motor vehicle, including those specifically addressing V2V data and functions. We also

seek the public's assistance in identifying additional formats and methods for providing this privacy statement to consumers that with the goal of achieving the timely and effective notice desired – notice that has increased significance in the context of a V2V mandate that effectively (and by design to achieve safety ends) limits consumer choice and consent.

4. V2V Privacy Statement

a) V2V Messages

The National Highway Traffic Safety Administration (NHTSA) requires that your vehicle be equipped with a Vehicle-to-Vehicle (V2V) safety system. The V2V system is designed to give your vehicle a 360 degree awareness of the driving environment and warn you in the event of a pending crash, allowing you to take actions to avoid or mitigate the crash, if the manufacturer of your vehicle has installed V2V safety applications.

Your V2V system periodically broadcasts and receives from all nearby vehicles a V2V message that contains important safety information, including vehicle position, speed, and direction. V2V messages are broadcast ten times per second in only the limited geographical range (approximately 300 meters) necessary to enable V2V safety application to warn drivers of pending crash events.

To help protect driver privacy, V2V messages do not directly identify you or your vehicle (as through vehicle identification number or State motor vehicle registration), or contain data that is reasonably or, as a practical matter, linkable to you. For purposes of this statement, V2V data is "reasonably" or "as a practical matter" linkable to you if it can be used to trace V2V messages back to you personally for more than a temporary period of time (in other words, on a persistent basis) without unreasonable expense or effort, in real time or after the fact, given available data sources. Excluding reasonably linkable data from V2V messages helps protect consumer privacy, while still providing your V2V system with sufficient information to enable crash-avoidance safety applications.

b) Collection, Storage and Use of V2V Information

Your V2V system does not collect or store V2V messages except for a limited time needed to maintain awareness of nearby vehicles for safety purposes or in case of equipment malfunction. In the event of malfunction, the V2V system collects only those messages required, and keeps that information only for long enough to assess a V2V device's misbehavior and, if a product defect seems likely, to provide defect information to your vehicle's manufacturer.

NHTSA does not regulate the collection or use of V2V communications or data beyond the specific use by motor vehicles and motor vehicle equipment for safety-related applications. That means that other individuals and entities may use specialized equipment to collect and aggregate (group together) V2V transmissions and use them for any purpose including applications such as motor vehicle and highway safety, mobility, environmental, governmental and commercial purposes. For example, States and localities may deploy roadside equipment

that enables connectivity between your vehicle, roadways and non-vehicle roadway users (such as cyclists or pedestrians). These technologies may provide direct benefits such as use of V2V data to further increase your vehicle's awareness of its surroundings, work zones, first responders, accidents, cyclists and pedestrians. State and local entities (such as traffic control centers or transportation authorities) may use aggregate V2V safety messages for traffic monitoring, road maintenance, transportation research, transportation planning, truck inspection, emergency and first responder, ride-sharing, and transit maintenance purposes. Commercial entities also may use aggregate V2V messages to provide valuable services to customers, such as traffic flow management and location-based analytics, and for other purposes (some of which might impact consumer privacy in unanticipated ways). NHTSA does not regulate the collection or use of V2V data by commercial entities or other third parties.

While V2V messages do not directly identify vehicles or their drivers, or contain data reasonably linkable to you on a persistent basis, the collection, storage and use of V2V data may have residual privacy impacts on private motor vehicle owners or drivers. Consumers who want additional information about privacy in the V2V system may review NHTSA's V2V Privacy Impact Assessment, published by The U.S. Department of Transportation at http://www.transportation.gov/privacy.

If you have concerns or questions about the privacy practices of vehicle manufacturers or third party service providers or applications, please contact the Federal Trade Commission. https://www.ftc.gov.

5. Consumer Education

Many commenters emphasized the need to educate consumers about the V2V system to enhance public acceptance through a coordinated and wide-spread information campaign utilizing traditional print and television outlets and the web, including the AAA, Global, Arizona Department of Transportation, Cohda Wireless, GM, Infineon Technologies, National Motorists Association, Pennsylvania Department of Transportation, Toyota, TRW Automotive, Automotive Safety Council, and Delphi Automotive.

Comments from the Automotive Safety Council, TRW Automotive, and Delphi Automotive suggested that such education should focus on the V2V safety message, what it contains, and how any information in the BSM will be used. The National Motorists Association recommended that NHTSA educate motorists on the system's privacy protection assurances. AAA recommended educating the public on how the V2V system will benefit them, and on the privacy and security protections built into the system. Toyota suggested that NHTSA educate the public about the fact that the V2V system will not transmit or store PII. The Privacy Rights Clearinghouse suggested that NHTSA educate the public on how the V2V system works. Honda focused more on educating the public on the security designed into the V2V system.

NHTSA agrees with commenters that educating the public about this important new safety technology, and the security and privacy protections designed into the V2V system, will be critical to consumer acceptance. For this reason, as suggested by many commenters, the

agency plans to work closely with the FTC, motor vehicle manufacturers, privacy advocates and other stakeholders to design a comprehensive public education strategy on the topic of privacy in the V2V system for consumers. Any claims regarding security or privacy made as part of NHTSA's public outreach will necessarily be justified by evidence based on the best scientific knowledge regarding security and privacy. Development of a consumer education strategy will likely be among the privacy-specific topics addressed in public meetings and/or workshops held by the agency after issuance of the NPRM and PIA.

6. Congressional/Other Government Action

NHTSA received comments from civil liberties groups and manufacturers that included calls on Congress to take action to protect consumer privacy in the V2V system. EFF and Privacy Rights Clearinghouse took the position that Federal legislation is imperative to protect driver privacy. The Alliance called on Congress to coordinate the relevant Federal agencies "to articulate a framework for privacy and security before further rulemaking proceeds" because, in its view, NHTSA alone does not have the authority to address V2V privacy and security issues. Honda and EPIC emphasized the need for ensuring that data is legally protected from third party access, and that unauthorized access is legally punishable. EPIC's comment focused on legal protections from OEM access, while Honda's comment focused on legal protections from government access.

NHTSA understands why legislation making it illegal for third parties or government agencies to collect V2V messages, or limiting those parties' retention or use of V2V messages, would be attractive to stakeholders – and the Alliance is correct in its assertion that such government action is outside the scope of the agency's regulatory authority over manufacturers of motor vehicles and motor vehicle equipment. As noted above, the introduction of V2V technology creates new privacy risks that cannot be fully mitigated. That said, in the agency's view, the V2V system is protected by sufficient security and privacy measures to mitigate unreasonable privacy risks. NHTSA seeks comment on these tentative conclusions -- and on whether new legislation may be required to protect consumer privacy appropriately.

D. Summary of PIA

1. What is a PIA?

Section 522 of the Consolidated Appropriations Act, 2005 (Pub. L. 108-447) requires that Federal agencies conduct privacy impact assessments (PIAs) of proposed regulatory activities involving collections or system of information with the potential to impact individual privacy. A PIA documents the flow of information and information requirements within a system by detailing how and why information is transmitted, collected, stored and shared to: (1) ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of the proposed data transactions; and (3) examine and evaluate protections and alternative processes for handling data to mitigate potential privacy impacts. It is a practical method of providing the public with documented assurance that the agency has identified and appropriately addressed potential privacy issues resulting from its activities. A

PIA also facilitates informed regulatory policy decisions by enhancing an agency's understanding of privacy impacts, and of options available for mitigating those potential impacts.

After reviewing a PIA, members of the public should have a broad understanding of any potential privacy impacts associated with a proposed regulatory action, and the technical and policy approaches taken by an agency to mitigate the resulting privacy impacts.

2. PIA Scope

The V2V system is complex and involves many different components, entities, communications networks, and data flows (within and among system components). For this reason, NHTSA opted not to analyze the potential privacy impacts in the V2V system on a component-specific basis. Rather, NHTSA focused its PIA on discrete data flows within the system, as an organic whole. NHTSA worked with privacy experts to zero in on discrete aspects of the V2V system most relevant to individual privacy for impact assessment purposes, identify and prioritize potential privacy impacts requiring further analysis (such as dynamic modeling), and validate the privacy-related requirements in NHTSA's regulatory proposal.

The V2V NPRM PIA identifies those V2V transactions involving data most relevant to individual privacy and the multiple technical, physical and policy controls designed into the V2V system to help mitigate potential privacy impacts.

To place our discussion of potential V2V privacy issues in context, NHTSA's PIA first briefly discusses several non-V2V methods of tracking a motor vehicle that currently exist.

3. Non-V2V Methods of Tracking

For comparative purposes, it is useful to consider the potential privacy impacts of the V2V system in the context of tracking mechanisms that do not involve any aspect of the V2V system (non-V2V tracking methods). These non-V2V methods of tracking inform the Agency's risk analysis because, to the extent that they may be cheaper, easier, and require less skill or access to a motor vehicle, they are relevant to our assessment of the likelihood of an individual or entity attempting to use V2V as a method of tracking. Examples of mechanisms that currently may be used to track a motor vehicle target include physical surveillance (i.e., following a car by visual observation), placement of a specialized GPS device on a motor vehicle, physical access to Onboard GPS logs, electronic toll transactions, cell phone history, vehicle-specific cell connections (e.g., OnStar), traffic surveillance cameras, electronic toll transponder tracking, and databases fed by automated license plate scanners. As compared to the potential approaches to V2V tracking discussed below, many of these non-V2V tracking methods appear may be cheaper, easier, require less (and/or no skill) under certain scenarios.

4. V2V Data Flows/Transactions with Privacy Relevance

As a starting point for the analysis that underlies this PIA, NHTSA identified and examined all data flows within the V2V system to determine which included data fields that may

have privacy impacts, either alone or in combination. We identified three data flows relevant for privacy impact purposes:

- Broadcast and receipt of V2V messages (also called Basic Safety Messages (BSMs)
- Broadcast and receipt of Misbehavior Reports
- Distribution of Certificate Revocation List (CRL)

Below, we describe these three data flows and detail the technical, policy and physical controls designed into the system to mitigate potential privacy impacts in connection with each flow. We then discuss the potential privacy impacts that remain, notwithstanding existing privacy controls. These constitute potential areas of residual risk for consideration by decision-makers.

a) Broadcast and Receipt of the Basic Safety Message (BSM)

BSMs are one of the primary building blocks for V2V communications. They provide situational awareness information to individual vehicles regarding traffic and safety. BSMs are broadcast ten times per second by a vehicle to all neighboring vehicles and are designed to warn the drivers of those vehicles of crash imminent situations.

Under NHTSA's proposal and any future adaptation of the technology, BSMs would contain information regarding a vehicle's GPS position, speed, path history, path trajectory, breaking status and other data, as detailed above in Section III.E. As discussed below, some data transactions necessitated by the security system may result in additional potential privacy impacts, some of which may be residual.

b) Broadcast and Receipt of Misbehavior Messages

Under NHTSA's proposal, when a vehicle receives a BSM from a neighboring vehicle, its V2V system validates the received message and then performs a cross check to evaluate the accuracy of data in the message. For example, it might compare the message content with other received messages or with equivalent information from onboard vehicle sensors. As a result of that cross check, the vehicle's V2V system may identify certain messages as faulty or "misbehaving." NHTSA's primary proposal for misbehavior reporting proposes that the V2V system then prepares a misbehavior report and sends it to the V2V security entity. The security entity evaluates the misbehavior report and may identify a defective V2V device. If it does, the V2V security entity will update the Certificate Revocation List (CRL) with information about the certificates assigned to the defective V2V device. The CRL is accessed by all V2V system components and vehicles on a periodic basis and contains information that warns V2V system participants not to rely on messages that come from the defective device. The security entity also might blacklist the device, in which case it will be unable to obtain additional security credentials from the security entity.

Also under our proposal, organizational and/or legal separation of information and functions within the security entity are important privacy impact-mitigating controls that are designed to prevent a single component or insider from having sufficient information to identify certificates assigned to a specific vehicle or owner. NHTSA plans to work closely with stakeholders to develop policies and procedures to institutionalize appropriate separation of data and functions within the National SCMS.

Under the second alternative for misbehavior reporting, the no misbehavior reporting proposal would not involve any additional broadcast or transmission of reports to V2V security entities. This means that no additional privacy risk would be imposed under the no misbehavior reporting alternative.

c) Misbehavior Reports

As described above, NHTSA's primary proposal for misbehavior reporting proposes that the V2V equipment in vehicles send misbehavior reports to the V2V security entity. Such reports will include the received BSM (which appears to be faulty) and other information, such as:

- Reporter's pseudonym certificate
- Reporter's signature
- Time at which misbehavior was identified
- 3D GPS coordinates at which misbehavior was identified
- List of vehicles (device/pseudonym certificate IDs) within range at the time
- Average speed of vehicles within range at the time
- Suspicion type (warning reports, proximity plausibility, motion validation, content and message verification, denial of service)
- Supporting evidence
    - Triggering BSM(s)
    - Host vehicle BSM(s)
    - Neighboring vehicle BSM(s)
    - Warnings
    - Neighboring devices
    - Suspected attacker

d) Distribution of Certificate Revocation List

As explained above, by evaluating misbehavior reports, the security entity envisioned may identify misbehaving V2V devices in vehicles and place information about those devices on the CRL. The security entity then would make updated CRLs available to V2V system participants and other system parts on a periodic basis to alert OBEs to ignore BSMs coming from the defective V2V equipment. There is only one type of CRL. Current system design

plans do not include placing individual security certificates on the CRL. Rather, each CRL would contain information (specifically, linkseed1, linkseed2, time period index, and LA Identifiers 1 and 2) that OBEs could use to calculate the values of the certificates in messages that should be ignored.

5. Privacy-Mitigating Controls

From the inception of the research program that would result in V2V technology over a decade ago, NHTSA has worked with its research partners, CAMP and the VIIC, to purse an integrated, privacy positive approach to the V2V system. For this reason, the V2V system described in our proposal would contain multiple layers of technical, policy and physical controls to help mitigate potential privacy impacts system-wide. Below, we discuss the privacy impact-mitigating controls that would apply to each of the three privacy-relevant data flows discussed above. In the course of this discussion, we detail some of the key privacy controls that we expect to see in a National SCMS (based on the current SCMS technical design, see Section V.B.2).

a) Privacy Controls Applicable to the Broadcast and Receipt of the Basic Safety Message (BSM)

(1) No directly identifying or "reasonably linkable" data in V2V transmissions

Under our proposals, the BSM would not contain information that directly identifies a private motor vehicle (as through VIN, license plate or registration information) or its owner or driver. BSM transmissions also would exclude data "reasonably linkable" or "as a practical matter" linkable to a specific individual.

(2) Rotating Security Credentials

Another critical control would help mitigate privacy risks created by signing messages. At the time of manufacture, a vehicle's V2V equipment would receive 3 years' worth of security certificates. Once the device is initialized into the V2V security system, the security system would send to the device keys on a weekly basis that will unlock 20 certificates at a time. During the course of the week, a vehicle's V2V equipment would use the certificates on a random basis, shuffling certificates at five minute intervals. These certificates would enable a vehicle's V2V system to verify the authenticity and integrity of a received BSM or, in the alternative, identify V2V messages that should be ignored (i.e., those that the security entity has identified as coming from misbehaving V2V equipment and placed on the CRL). The shuffling and random use of certificates every five minutes also will help minimize the risk of vehicle tracking by preventing a security certificate from becoming a de facto vehicle identifier (also referred to as a "quasi-identifier").

(3) Limited Transmission Radius

V2V equipment in vehicles would transmit safety information in a very limited geographical range, typically only to motor vehicles within a 300 meter radius of a V2V device. This limited broadcast is sufficient to enable V2V crash avoidance applications in neighboring vehicles, while limiting access by more geographically distant vehicles that cannot benefit from the safety information.

(4) No BSM Data Collection or Storage within the V2V system

Neither V2V devices in motor vehicles, nor the V2V system as a whole would collect or store the contents of V2V messages sent or received, except for the short time period necessary for a vehicle to use messages for safety applications or in the limited case of device malfunction. These technical controls would help prevent in-vehicle V2V equipment or the V2V system, as a whole, from after-the-fact tracking of a vehicle's location by accessing and analyzing a vehicle's BSMs. Although specialized roadside and mobile equipment would be able to access and collect BSMs, the V2V data collected would contain no information directly identifying or reasonably linkable to a specific private vehicle or its driver or owner, because the transmission of such information would not be allowed by the V2V rule. Research is ongoing on the methods, cost and effort required to use collected BSMs in combination with other available information or over time to track a specific, targeted vehicle or driver. The Agency believes that such linkage between collected BSMs and a specific vehicle or driver is plausible, but has not yet determined whether it is practical or reasonable, given the resources or effort required. This additional research will help to ensure that our proposed V2V FMVSS incorporates all available, appropriate controls to mitigate unreasonable privacy risk related to collection of BSM transmissions by roadside or mobile sensors. We acknowledge that introduction of this technology will result in residual privacy risk that cannot be mitigated. We seek comment on these tentative conclusions.

(5) FIPS-140 Level 3 HSM

NHTSA has proposed performance requirements that include use of FIPS-140 Level 3 hardware security module (HSM) in all V2V equipment in motor vehicles. This physical computing device would safeguard and manage a vehicle's security certificates and guard against equipment tampering and bus probing. This type of secure hardware provides evidence of tampering, such as logging and alerting of tampering, and tamper resistance such as deleting keys upon tamper detection.

(6) Consumer Notice

NHTSA would require that motor vehicle manufacturers, at a minimum, include a standard V2V Privacy Statement in all owner's manuals (regardless of media) and on a publicly accessible web location that current and future owners may search by make/model/year to obtain

the data access and privacy policies applicable to their motor vehicle, including those specifically addressing V2V data and functions, asdetailed in Section IV.C. As discussed above, NHTSA also considering the possibility of requiring additional methods for communicating the V2V Privacy Statement to consumers and seeks comment on the most effective methods for providing such notice.

b) Privacy Controls Applicable to Broadcast and Receipt of Misbehavior Messages

When a V2V device in a motor vehicle appears to malfunction, the V2V system would collect and store only BSMs relevant to assessing the device's performance, consistent with the need to address the root cause of the malfunction if it is, or appears to be, widespread.

(1) Encryption of Misbehavior Report

Like all security materials exchanged between V2V equipment in vehicles and a security authority, misbehavior reports would be encrypted. This would help limit but not prevent potential privacy risks that could stem from unintended or unauthorized access to data in misbehavior messages. Specifically, this would reduce the possibility that BSMs contained in misbehavior reports may provide information about the past location of a reporting vehicle (and thereby of the vehicle owner's activities and relationship between the two vehicles), or of vehicles located nearby the reporting vehicle.

(2) Functional/data separation across SCMS components

A key privacy-mitigating control applicable to this data stream is the technical design for the security entity proposed by NHTSA, which provides for functional and data separation across different organizationally and/or legally separate SCMS components. This technical control is designed to prevent individual SCMS entities or insiders from using information, including from misbehavior messages, for unauthorized purposes. The technical separation of information and functions within the security entity could be overcome only by a specific entity within the security organization (called the Misbehavior Authority or MA) after determining, based on misbehavior messages, that a vehicle's V2V equipment is malfunctioning and needs to be blacklisted (i.e., prevented from obtaining any additional security certificates). In order to do so, the MA would need to gather information from the various independent, separate parts of the security entity to identify the device to be blacklisted.

(3) Misbehavior Reports Are Stripped of Geographic Location Information

An example of information separation serving as a privacy control is evident in one particular component of the security organization – the Location Obscurer Proxy (LOP). Misbehavior messages (like other communications between a vehicle's V2V equipment and the security entity) travel through the LOP entity to get to other parts of the security organization.

The LOP would strip out information from the misbehavior message that otherwise would permit other parts of the security organization (like the MA) to associate a vehicle's V2V messages with its geographic location. This technical separation of geographic information from messages transmitted between vehicle's V2V systems and the security entity is designed to prevent individual security entities or V2V security organization insiders from colluding to use BSM information inappropriately or to track individual vehicles.

(4) Separation of Security Organization Governance

The design for the V2V security entity (or SCMS) calls for the separation of some critical functions into legally distinct and independent entities that, together, make up the SCMS. This legal separation of security entity governance is designed to prevent individual entities or V2V security organization insiders from colluding to use information for unauthorized purposes such as tracking individual vehicles.

c) Privacy Controls Applicable to Distribution of the CRL List

(1) Misbehaving V2V equipment in a vehicle stops broadcasting

It is possible that information regarding a vehicle's revoked security certificates could enable all revoked certificates to be associated with the same vehicle. This might be used to persistently identify a vehicle during the vehicles' activities. In order to mitigate this potential privacy risk, once a vehicle's V2V system determines that information about it is on the CRL and that the security organization has revoked its security certificates, it would stop broadcasting the BSM.

6. Potential Privacy Issues by Transaction Type

Based on our analysis of the privacy relevant data flows and controls discussed above, we identified five potential privacy scenarios for further research and/or consideration by the Agency. Table IV-1 below summarizes the scenarios and corresponding system transactions identified for further analysis.

Table IV-1 Transactions Identified for Further Analysis

Transaction Type	Description
BSM Broadcast Transaction	1. Can data elements, such as location, in the BSM be combined to form a temporary or persistent vehicle identifier
BSM Broadcast Transaction	2. Can data elements in the BSM be combined to identify vehicles temporarily so that different security certificates can be associated with the same vehicle during the vehicle's activities
BSM Broadcast Transaction	3. Do the physical characteristics of the carrier wave (i.e., the wave's fingerprint) associated with a vehicle's BSM serve as a vehicle identifier

Broadcast and Receipt of a Misbehavior Message	4. Do BSMs in misbehavior reporting provide sufficient information about the past location of the reporting or other vehicles to retrospectively track the vehicle's path?
Certificate Revocation List (CRL) Distribution Transaction	5. Does information regarding blacklisted vehicles' security certificates enable all vehicle security certificates to be associated with one another and thus, with the same specific vehicle?

As noted above, based on our exploration of privacy impacts and analysis of the V2V system design to date, it is NHTSA's expectation that the multiple technical, policy and physical controls incorporated into the design of the V2V system detailed will help to mitigate privacy risks to consumers. Methods of tracking vehicles, such as surveillance and use of specialized GPS devices already exist and may be easier, less expensive, and require less skill and access than would vehicle tracking using V2V messages or other information in the V2V system in certain conditions. Nevertheless, DOT is continuing to work with privacy experts to perform dynamic modeling and explore the viability of additional controls that might further mitigate any potential impacts demonstrated in the privacy-relevant transactions identified above for further analysis. The planned implementation by DOT of a PoC security entity (SCMS) and related PKI policy research will provide an operational environment in which to continue to explore the viability of additional privacy-mitigating controls applicable to the V2V System, as currently envisioned and designed. We seek comment on whether there are other potential privacy risks stemming from the V2V systems proposed that the agency should investigate and, if so, what specific risks.

E. Health effects

NHTSA received numerous comments from individuals in response to the ANPRM concerning the potential for V2V technology to contribute to electromagnetic hypersensitivity ("EHS"). Overall, the comments focused on how a national V2V deployment could potentially disadvantage persons that may be electro-sensitive.[190] In response, NHTSA engaged the DOT Volpe Center to review available literature and government agency actions regarding EHS in support of this NPRM. More specifically, NHTSA needed to learn more about the potential conditions causing EHS, actions taken by other federal agencies that have been involved in similar technology deployments or whose mission is primarily human health-focused, and any qualifying actions granted by the Americans with Disabilities Act (ADA) related to EHS among other potential externalities that may affect a potential V2V technology deployment.

[190] "Electromagnetic Hypersensitivity Comment Review and Analysis", NHTSA V2V Support – Task 3, dated March 13, 2015, Noblis.

1. Overview

According to the World Health Organization (WHO), EHS is characterized by a variety of non-specific symptoms that are attributed to exposure to electro-magnetic frequencies ("EMF") by those reporting symptoms. The symptoms most commonly experienced include dermatological symptoms (redness, tingling, and burning sensations) as well as neurasthenic and vegetative symptoms (fatigue, tiredness, difficulty concentrating, dizziness, nausea, heart palpitation, and digestive disturbances). The collection of symptoms is not part of any recognized syndrome. Reports have indicated that EHS can be a disabling problem for the affected individual; however, EHS has no clear diagnostic criteria and it appears there is no scientific basis to link EHS symptoms to EMF exposure. Further, EHS is not a medical diagnosis, nor is it clear that it represents a single medical problem.[191]

2. Wireless Devices and Health and Safety Concerns

The Federal Communications Commission (FCC), federal health and safety agencies such as the Environmental Protection Agency (EPA), the Food and Drug Administration (FDA), the National Institute for Occupational Safety and Health (NIOSH) and the Occupational Safety and Health Administration (OSHA) have been actively involved in monitoring and investigating issues related to radio frequency ("RF") exposure. Federal, state, and local government agencies and other organizations have generally relied on RF exposure standards developed by expert, non-government organizations such as the Institute of Electrical and Electronics Engineers (IEEE) and the National Council on Radiation Protection and Measurements (NCRP).

Several U.S. government agencies and international organizations are working cooperatively to monitor research on the health effects of RF exposure. The World Health Organization's (WHO) International Electromagnetic Fields Project (IEFP) provides information on health risks, establishes research needs, and supports efforts to harmonize RF exposure standards. Some health and safety interest groups have interpreted certain reports to suggest that wireless device use may be linked to cancer and other illnesses, posing potentially greater risks for children than adults. While these assertions have gained increased public attention, currently no scientific evidence establishes a causal link between wireless device use and cancer or other illnesses.[192]

---

[191] "Electromagnetic fields and public health: Backgrounder", The World Health Organization (WHO), December 2005. Available at http://www.who.int/peh-emf/publications/facts/fs296/en/ (last accessed Sept. 28, 2015).

[192] "Wireless Devices and Health Concerns", Federal Communications Commission (FCC), Consumer and Governmental Affairs Bureau, updated March 12, 2014. Available at http://www.fcc.gov/guides/wireless-devices-and-health-concerns (last accessed Dec 12, 2016).

3. Exposure Limits

In the U.S, IEEE has developed limits for human exposure to RF energy, and these limits have been widely influential around the world and require periodic updates. Internationally, the exposure limits for RF energy vary widely in different countries. A few countries have chosen lower limits, in part due to differences in philosophy in setting limits. IEEE and most other Western exposure limits are designed on the basis of identified thresholds for hazards of RF and thus are science-based. Switzerland, Italy, and a few other countries have adopted "precautionary" exposure limits for RF energy. These are not based on identified hazards, but reflect the desire to set exposure limits as low as economically and technically practical, to guard against the possibility of an as-yet unidentified hazard of RF exposure at low levels.[193]

4. U.S. Department of Energy (DOE) Smart Grid Implementation

Many comments to the ANPRM were related to the implementation and expansion of "smart grid" or "smart meter" technology being deployed in the United States. The "smart grid" generally refers to a class of technology used to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. These systems are made possible by two-way communication technology and computer processing that has been used for decades in other industries.[194]

Federal legislation was enacted in both 2005 (Energy Policy Act, or "EPAct") and 2007 (Energy Independence and Security Act, or "EISA") that contained major provisions on demand response, smart metering, and smart grids.[195] The primary purpose of using smart meters and grids is to improve energy efficiency – very precise electricity usage information can be transmitted back to the utility in real-time, enabling the utility to better direct how much electricity is transmitted, and when, which in turn can improve power generation efficiency by not producing more power than necessary at a given time. According to a report prepared by the Federal Energy Regulatory Commission (FERC) in December 2014, approximately 15.3 million advanced meters were installed and operational through the Department of Energy (DOE) Smart Grid Investment Grant (SGIG) program. Ultimately, 15.5 million advanced meters are expected

---

[193] "COMAR Technical Information Statement the IEEE exposure limits for radiofrequency and microwave energy", Marvin C. Ziskin, IEEE Engineering in Medicine and Biology Magazine, March/April, 2005. Available at http://ewh.ieee.org/soc/embs/comar/standardsTIS.pdf (last accessed Dec. 12, 2016).

[194] Department of Energy "Smart Grid" website. Available at http://energy.gov/oe/services/technology-development/smart-grid (last accessed Dec 12, 2016).

[195] "Demand Response & Smart Metering Policy Actions Since the Energy Policy Act of 2005 – A Summary for State Officials", Prepared by U.S. Demand Response Coordinating Committee for The National Council on Electricity Policy, 2008. http://energy.gov/oe/downloads/demand-response-and-smart-metering-policy-actions-energy-policy-act-2005-summary-state (last accessed: Dec 12, 2016)

to be installed and operational under SGIG. All SGIG projects are expected to reach completion in 2014, with continued reporting requirements through 2016.[196]

In the last several years, some consumers have objected to deployment of the "smart" utility meters needed for DOE's Smart Grid implementation. Smart meters transmit information via wireless technology using electromagnetic frequencies (EMF). Smart utility meters operate in the 902-928 MHz frequency band and the 2.4 GHz range, which is where the human body absorbs energy less efficiently and the Maximum Permissible Exposure (MPE) limits for RF exposure are less restrictive.[197]

Smart utility meters in households or businesses will generally transmit data to an access point (usually on utility poles) once every four hours for about 50 milliseconds at a time. Once the smart grid is fully active, it is expected that smart utility meters will transmit more frequently than once every four hours, resulting in a higher duty cycle.[198] A 2011 report from the California Council on Science and Technology (CCST) showed minimum and maximum exposure levels for various sources, including a smart meter that is always on at two distances from the body. The CCST concluded that RF exposure levels for smart meters in either scenario would be less than microwave ovens and considerably less than cell phones, but more than Wi-Fi routers or FM radio/TV broadcasts.[199] It should also be noted that a 2011 report from the Electric Power Research Institute (EPRI) assessed exposures in front of and behind smart utility meters. It determined that the average exposure levels from smart utility meters, measured from a single meter and from an array of meters, were at levels similar to those from other devices that produce RF in the home and surrounding environment.[200]

A typical "smart" utility meter device uses a low power one watt wireless radio to send customer energy-usage information wirelessly.[201] The V2V DSRC devices used for NHTSA

---

[196] "Assessment of Demand Response and Advanced Metering", Federal Energy Regulatory Commission (FERC) Report, December 2014. Available at https://www.ferc.gov/industries/electric/indus-act/demand-response/dem-res-adv-metering.asp (last accessed Dec 12, 2016).
[197] Federal Communications Commission, (FCC), 2011. Radio frequency safety, available at https://www.fcc.gov/encyclopedia/radio-frequency-safety (last accessed Dec 12, 2016).
[198] "Review of Health Issues Related to Smart Meters", Monterey County Health Department, Public Health Bureau, Epidemiology and Evaluation, March, 2011. Available at https://www.nema.org/Technical/Documents/Smart%20Meter%20Safety%20-%20Marin%20Co%20CA%20whitepaper.pdf (last accessed Dec 12, 2016).
[199] "Health Impacts of RF Exposure from Smart Meters", California Council on Science and Technology, April 2011. Available at https://ccst.us/publications/2011/2011smart-final.pdf (last accessed Dec 12, 2016).
[200] "RF Exposure Levels from Smart Meters: A Case Study of One Model", Electric Power Research Institute (EPRI), February 2011. Available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001022270 (last accessed Dec 12, 2016).
[201] Radio Frequency FAQ, http://www.pge.com/en/safety/systemworks/rf/faq/index.page (last accessed Jun. 5, 2015).

research in the Safety Pilot activities are allowed to transmit at up to 33 dBm[202] (approximately 2.0 watts of power output)., as defined by FCC specifications.[203] The "normal" operating transmission output range for these devices is 20 dBm (or approximately 100mW) for devices operating in the allocated DSRC frequency range. For additional comparison purposes, the typical cellular phone operates at higher power output levels of 27 dBm (approximately 500 mW). Cellular phones are capped at the same maximum transmission power output of 33 dBm.

The public objections to these deployments have been based on concerns over potential health effects. Specifically, some consumers are concerned about exposure to wireless RF emissions emanating from smart meters in their homes, which has led to legal challenges for smart meter programs. Due to these objections, several state commissions authorized an "opt-out" provision for individual consumers who do not wish to have smart meters installed in their homes. In response to public perception of the technology, the Department of Energy pursued development of outreach materials citing current scientific and industry evidence that radio frequency from smart grid devices in the home is not detrimental to health. The materials are being provided to state commissions, utilities in the DOE Smart Grid Program, and other community-based organizations in effort to convey these messages to the end-user community.[204]

5. Federal Agency Oversight & Responsibilities

Many consumer and industrial products use or produce some form of electromagnetic energy. Various agencies within the Federal Government have been involved in monitoring, researching, or regulating issues related to human exposure to radio frequency radiation. A summary of the federal Government's role is provided below:[205]

- **Federal Communications Commission (FCC):** The FCC authorizes and licenses most RF telecommunications services, facilities, and devices used by the public, industry, and state and local governmental agencies. The FCC's exposure guidelines that V2V devices

---

[202] dBm or decibel-milliwatt is an electrical power unit in decibels (dB), referenced to 1 milliwatt (mW). The power in decibel-milliwatts (P(dBm)) is equal to 10 times base 10 logarithm of the power in milliwatts (P(mW)).
[203] "Table I.5a—Maximum STA transmit power classification for the 5.85–5.925 GHz band in the United States", IEEE specification 802.11P -2010, Page 31. Available at https://www.ietf.org/mail-archive/web/its/current/pdfqf992dHy9x.pdf (last accessed Dec 12, 2016).
[204] Recommendations on Consumer Acceptance of Smart Grid, Electricity Advisory Committee, Richard Cowart, Chair to Honorable Patricia Hoffman, Assistant Secretary for Electricity Delivery and Energy Reliability, U. S. Department of Energy, June 6, 2013. http://energy.gov/sites/prod/files/2013/06/f1/EAC_SGConsumerRecs.pdf (last accessed Dec 12, 2016).
[205] "Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields", OET Bulletin 56, Fourth Edition, August 1999, Federal Communications Commission, Office of Engineering and Technology. Available at https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet56/oet56e4.pdf (last accessed Dec 12, 2016).

are anticipated to follow, and the ANSI/IEEE and NCRP guidelines upon which they are based, specify limits for human exposure to RF emission from hand-held RF devices in terms of specific absorption rate (SAR). Additionally, under the National Environmental Policy Act of 1969 (NEPA), the FCC has certain responsibilities to consider whether its actions will "significantly affect the quality of the human environment." To meet its NEPA obligations, the Commission has adopted requirements for evaluating the impact of its actions (47 CFR 1.1301, et. seq.). One of several environmental factors addressed by these requirements is human exposure to RF energy emitted by FCC-regulated transmitters and facilities. The FCC's rules provide a list of various Commission actions that may have a significant effect on the environment. If FCC approval to construct or operate a facility would likely result in a significant environmental effect, the applicant must submit an Environmental Assessment (EA). The EA is reviewed by FCC staff to determine whether an Environmental Impact Statement (EIS) is necessary.[206]

- **National Telecommunications and Information Administration:** NTIA is an agency of the U.S. Department of Commerce and is responsible for authorizing Federal Government use of the RF electromagnetic spectrum. Like the FCC, NTIA also has NEPA responsibilities and has enacted similar guidelines and processes to those of FCC to ensure compliance.
- **Food and Drug Administration (FDA):** by authority of the Radiation Control for Health and Safety Act of 1968, the FDA's Center for Devices and Radiological Health (CDRH) develops performance standards for the emission of radiation from electronic products including: X-ray equipment, other medical devices, television sets and microwave ovens, laser products, and sunlamps. The CDRH has not adopted performance standards for other RF-emitting products. The FDA is the leading federal health agency in monitoring the latest research developments and advising other agencies with respect to the safety of RF-emitting products used by the public, such as cellular and mobile devices.
- **Environmental Protection Agency (EPA):** EPA activities pertaining to RF safety and health are presently limited to advisory functions. EPA has chaired an Interagency Radiofrequency Working Group, which coordinates RF health-related activities among federal agencies who have regulatory responsibilities in this area.
- **Occupational Safety and Health Administration (OSHA):** OSHA is responsible for protecting workers from exposure to hazardous chemical and physical agents. In 1971, OSHA issued a protection guide, which V2V devices are anticipated to operate within, for exposure of workers to radiation (29 CFR 1910.97). The guide covers frequencies

[206] "Evaluating Compliance with FCC Guidelines for Human Exposure to Radio frequency Electromagnetic Fields", Federal Communications Commission, Office of Engineering & Technology, OET Bulletin 65 (Edition 97-01), August 1997. Available at https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet65/oet65b.pdf (last accessed Dec 12, 2016).

from 10 MHz to 100GHz. The guide was later ruled to be only advisory and not mandatory.[207]

- **National Institute for Occupational Safety and Health (NIOSH):** NIOSH is part of the U.S. Department of Health and Human Services, Centers for Disease Control and Prevention (CDC) and conducts research and investigations into issues related to occupational exposure to chemical and physical agents. NIOSH research is focused on radio frequencies, extremely low frequencies (ELF) and static magnetic fields. CDC/NIOSH provides various guidance documents related to the focused research areas.[208]
- **The Architectural and Transportation Barriers Compliance Board (Access Board):** The Access Board is the federal agency devoted to the accessibility for people with disabilities. In November 1999, the Access Board issued a proposed rule to revise and update their accessibility guidelines. During the public comment period on the proposed rule, the Access Board received approximately 600 comments from individuals with multiple chemical and electromagnetic sensitivities. The Board issued a statement recognizing that people with these sensitivities may be considered disabled under the ADA if conditions perceived to be caused by these sensitivities "so severely impair the neurological, respiratory, or other functions of an individual that it substantially limits one or more of the individual's major life activities." The Board contracted with the National Institute of Building Sciences (NIBS) to establish the Indoor Environmental Quality (IEQ) Project. The overall objectives of the IEQ project were to establish a collaborative process among a range of stakeholders to recommend practical, implementable actions to both improve access to buildings for people with EMS while also improving indoor environmental quality to create healthier buildings for the entire population. The NIBS IEQ Final Report was issued in July 2005 and provides recommendations for accommodations for people with chemical and/or electromagnetic sensitivities. The agency is unaware of any further actions by the Access Board on this issue.[209]
- **Department of Defense (DOD):** The DOD conducts research on the biological effects of RF energy.

---

[207] OET Bulletin #56, Federal Communications Commission, FCC, available at https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet56/oet56e3.pdf (last accessed Dec 12, 2016).

[208] "EMF (ELECTRIC AND MAGNETIC FIELDS)," available at http://www.cdc.gov/niosh/topics/emf/ (last accessed Dec 12, 2016).

[209] "IEQ Indoor Quality Final Report, National Institute for Building Services, July 14, 2005. http://apps.fcc.gov/ecfs/document/view?id=7520945309 (last accessed: Dec 12, 2016)

6. EHS in the US and abroad

a) Americans with Disabilities Act

The Americans with Disabilities Act ("ADA") does not contain a lengthy list of medical conditions that constitute disabilities. Instead, the ADA provides a general definition for "disability", which requires a showing of a having a physical or mental impairment that substantially limits one or more major life activities, a history or record of such an impairment, or being perceived by others as having such an impairment. Several states have enacted even more liberal policies on disability rights that afford greater potential protections than the ADA as it relates to EHS.

To date, the agency is unaware of any finding that EHS constitutes a disability. As mentioned above, the NIBS IEQ provided some recommendations, but did not conclude the EHS was in fact a disability. The agency is unaware of any further actions, either by the Access Board or some other entity, which recognized EHS as a disability or any science that would prove this.

b) Global recognition

Globally, some nations have heightened awareness of EHS by requiring provisions to accommodate those claiming its effects. In Sweden, for example, these provisions could include unique lighting fixtures and/or computer monitors for places of employment. The Canadian Government, The Canadian Human Rights Commission (CHRC) has also recognized EMS, describing environmental sensitivities as follows: "The term "environmental sensitivities" describes a variety of reactions to chemicals, electromagnetic radiation, and other environmental factors at exposure levels commonly tolerated by many people."[210] The CHRC published a series of recommendations for building environments in effort to reduce potential EMS conditions.[211] In 2009, the European Parliament urged member states to follow Sweden's example to provide people with ES protection and equal opportunities.

7. Conclusion

The agency appreciates the ANPRM comments bringing attention to V2V technology and a potential relationship to EHS. The agency takes these concerns very seriously. The literature review conducted by the agency highlighted long, and still ongoing, activities to better understand the relationship to electromagnetic radiation and the symptoms of individuals

---

[210] "What You Should Know About Electromagnetic Sensitivity (EMS)", Christiane Tourtet. B.A, International MCS/EMS Awareness, available at http://www.nettally.com/prusty/CTEMS.pdf (last accessed Dec. 8, 2016).

[211] Sears, Margaret E., "The Medical Perspective on Environmental Sensitivities," May 2007. Available at http://www.chrc-ccdp.ca/sites/default/files/envsensitivity_en_1.pdf. (last accessed Dec. 8, 2016).

reporting electromagnetic hypersensitivity. As a Federal government agency focused on automotive safety, NHTSA acknowledges the expertise of our sister agencies such as the Federal Communications Commission and the Food and Drug Administration, among others, which have been involved with electromagnetic fields, in parallel with the pervasiveness of cellular phone deployment in the United States and globally.

The FDA currently states in response to the question, "Is there a connection between certain health problems and exposure to radiofrequency fields via cell phone use?" that "The results of most studies conducted to date indicate that there is not. In addition, attempts to replicate and confirm the few studies that did show a connection have failed."[212] However, NHTSA acknowledges that research is still ongoing and, as technology evolves; wireless communications will most likely continue to increase. The agency believes the continued efforts of the Radiofrequency Interagency Work Group (RFIAWG)[213] may yield any potential future guidance for wireless device deployment and usage.

V2V devices are currently certified for use in the 5.9 GHz frequency allocation by the FCC, and the agency additionally anticipates any future certifications by the FCC will ensure that V2V devices will comply with all criteria related to RF emissions.

Currently, the FCC publishes a very helpful guide on "Wireless Devices and Health Concerns,"[214] in which the Commission states, "While there is no federally developed national standard for safe levels of exposure to radiofrequency (RF) energy, many federal agencies have addressed this important issue." The Commission acknowledges the efforts the interagency working group, its members, and their ongoing monitoring and investigating issues related to RF exposure.

V2V devices would operate at distances to humans significantly further that the distance relationship of a portable cellular phone to its operator, where the device is generally carried on a person or pressed directly to the ear. V2V devices used in the Safety Pilot operated at similar power levels to handheld cellular phones and the agency expects power levels for production deployment to remain consistent with the levels used in the Safety Pilot activities. Based on these two conditions, we believe it is reasonable to anticipate that any new guidance issued by the RFIAWG and its participating federal agencies on future cellular phone or wireless device usage could potentially be relevant to V2V devices, albeit in a somewhat diminished magnitude based on the distances the devices will operate in relation to persons.

---

[212] Radiation-Emitting Products, "Current Research Results," available at http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/HomeBusinessandEntertainment/CellPhones/ucm116335.htm (last accessed Dec. 8, 2016).
[213] Group members can be found at http://www.emrpolicy.org/litigation/case_law/docs/workgroupmemberslist.pdf (last accessed: Dec 8, 2016)
[214] See "Wireless Devices and Health Concerns" https://www.fcc.gov/guides/wireless-devices-and-health-concerns (last accessed Dec. 8, 2016).

V. Device Authorization

A. Approaches to security credentialing

As part of exploring different methods of authenticating V2V messages, the agency has examined in addition to the primary message authentication proposal's PKI base SCMS (single-root approach), two potential approaches to ensuring V2V messages are secure. These include a vehicle based approach, and an approach where multiple roots of confidence would be utilized. Each approach is described in the following sections.

B. Federated Security Credential Management (SCMS)

1. Overview[215]

For V2V communications to work effectively and as intended to facilitate crash avoidance safety applications, it is critical that users of the network have confidence in the validity of basic safety messages received from other system users – indistinct users whom they have never met and do not know personally. For this reason, DOT and its research partners have developed a sophisticated security system that allows for the creation and management of digital security credentials (referred to as "certificates") that enable users to have confidence in one another, and the system as a whole. In fact, the security system designed to create confidence in the V2V environment is a more complex and sophisticated version of the same public key infrastructure (PKI) system that consumers and merchants use every day to verify credit card transactions at the supermarket or make on-line purchases (any time you see the "https," for example). PKI systems also have long been used by the Federal government and corporate America, successfully and securely, to verify the identity of their employees for access and security purposes.

In the V2V context, system participants use digital certificates to validate the integrity of safety messages exchanged 10 times per second by V2V devices in motor vehicles. The body of each safety message is unencrypted; the sender signs the message with a digital certificate and the receiver checks to ensure that the signature is valid before relying on the message content. This PKI verification process requires an organization referred to as a Security Credential Management System (SCMS) to provide those necessary signing credentials (i.e., digital certificates) and conduct related security functions, such as identifying and removing

[215] The SCMS overview and governance discussions in this notice are based in significant part on a report DOT entitled, "Organizational and Operational Models for the Security Credentials Management System (SCMS); Industry Governance Models, Privacy Analysis, and Cost Updates," dated October 23, 2013, prepared by Booz Allen Hamilton under contract to DOT, non-deliberative portions of which may be viewed in Docket: NHTSA-2014-0022.

malfunctioning V2V devices from the system. The V2V Readiness Report details the SCMS component of the V2V system.[216]

When NHTSA issued its V2V Readiness Report, for a variety of reasons discussed therein, the agency envisioned that the SCMS would be established, funded, and governed primarily by one or more private entities – possibly a consortium of automobile and V2V device manufacturers -- with limited Federal involvement. Through comments to the ANPRM, the SCMS RFI process, collaborative research with the VIIC, and additional DOT policy research, NHTSA now has developed several different potential processes by which a V2V SCMS might be stood up, owned, operated, and governed. DOT is committed to playing a central pre-deployment role in developing the organizational framework of a viable and sustainable V2V SCMS, as well as the policies and procedures required to support the SCMS - depending on comments received in response to this NPRM. In order to do so, DOT has expanded the scope of its pre-deployment policy research significantly to include several additional critical activities. DOT intends to work closely with experienced PKI and organizational management consultants and stakeholders to:

- Deploy a Proof-of-Concept SCMS based on the current design to support additional privacy and security research, as well as the certificate needs of CV Pilots funded by DOT and early industry adopters of V2V;
- Develop policies and procedures (based on industry best practices, standards, comparable privacy-sensitive PKIs, and individual input from SCMS and V2V stakeholders) that could be used to govern the organization, accreditation, and operation of a V2V SCMS and its components, including drafts of an SCMS Certificate Policy (CP), Certification Practice Statement (CPS), and Privacy Policy;
- Develop a model for, and then prototype a private, multi-stakeholder governance entity (on the basis of existing multi-stakeholder models) that could support deployment of an operational SCMS.
- Develop one or more public-private governance models (on the basis of existing comparable organizations) that could support deployment of an operational SCMS, given appropriate funding.

We are hopeful that this critical technical and policy research will provide government and private stakeholders with a detailed blueprint of several viable options for standing up an SCMS. One promising path that DOT actively will continue to explore is that of working with a private sector, multi-stakeholder entity that could serve as an SCMS Manager to deploy, govern, and coordinate operation of a fully-operational V2V SCMS, in which DOT would play an ongoing advisory role. However, DOT's planned research also encompasses robust exploration

[216] See Section IX.B of the V2V Readiness Report.

of other paths that could support the deployment of a sustainable, operational V2V SCMS, given appropriate public and/or private funding.

We begin this discussion with a description of the technical and organizational design of the SCMS that will support V2V, V2I, and V2X communications. We then summarize and address comments on the technical design received by NHTSA in connection with the ANPRM, V2V Readiness Report, and RFI process. As the foundation to a discussion of SCMS governance, we identify the diverse group of public and private entities and stakeholders with interests in deployment of a V2V SCMS (together described in this document as members of a "SCMS ecosystem" or "SCMS industry" requiring governance for successful deployment of V2V communications). We summarize and address governance comments received in response to the ANPRM, V2V Readiness Report, and during the RFI process. We detail DOT's planned deployment of the proof-of-concept (POC) SCMS. We then detail planned work with experts and SCMS "industry" participants to develop policies and procedures for the National SCMS, and to flesh out one or more a viable model for organization, ownership, and governance of the National SCMS. Following is a discussion of ICANN as a comparative industry example of successful, private sector multi-stakeholder governance, the evolution of which is instructive to government and private sector stakeholders in the SCMS ecosystem. Finally, we outline NHTSA's plan to issue, on the basis of this additional PKI and organizational research, a policy statement on SCMS governance on which we will seek comment from stakeholders representing all aspects of the SCMS ecosystem.

2. Technical Design

The technical design for a SCMS reflects the processes associated with certificate production, distribution, and revocation, and illustrates how these SCMS functions interact with each other and with OBE. Several functions work together in a PKI system. The V2V SCMS is based on a standard PKI design to which additional functions have been added specifically to address the identified security and privacy needs of V2V, V2I, and V2X technologies. The term "pseudonym functions" is used to refer to those functions responsible for creating the short-term certificates used by the OBE in V2V messaging. The term "pseudonym" is used to indicate that short-term certificates contain no unique or personally-identifying information about users or their vehicles, but still allow users to participate in the system, in essence allowing use of a pseudonym. The pseudonym functions differ from those functions that take part in the "bootstrap" process, described later in this section. Pseudonym functions create, manage, distribute, monitor, and revoke short-term certificates for vehicles.

These functions are listed below in alphabetical order:

- Intermediate Certificate Authority (Intermediate CA)
- Linkage Authority (LA)
- Location Obscurer Proxy (LOP)
- Misbehavior Authority (MA)
- Pseudonym Certificate Authority (PCA)

- Registration Authority (RA)
- Request Coordination
- Root Certificate Authority (Root CA)
- SCMS Manager

Distinct from the pseudonym functions that execute the short-term certificate processes are the functions that carry out the "bootstrap" process (the initialization of the device into the system). The bootstrap process establishes the initial connection between OBE and the SCMS. This process is characterized by its chief component, the Enrollment Certificate Authority (ECA), which is responsible for assigning an enrollment certificate to each OBE. The bootstrap functions remain separate from the pseudonym functions because of the potential connection to individual identifying information (like a VIN) during bootstrap.

The functions within the bootstrap process are listed below in alphabetical order:

- Certification Lab
- Device Configuration Manager (DCM)
- Enrollment Certificate Authority (ECA)

A brief description of each SCMS function is provided in Table V-1.

Table V-1 SCMS Components and Description

Abbreviation	Function Name	Activities
Certification Lab	Certification Lab	Tests OBE and informs ECA that units of a particular type are eligible for enrollment certificates
DCM	Device Configuration Manager	Coordinates initial distribution with OBE and enables OBE to request certificates from RA
ECA	Enrollment Certificate Authority	Activates OBE and credentials users
Intermediate CA	Intermediate Certificate Authority	Shields Root CA from system and provides more flexibility for trust management
LA	Linkage Authority	Each pair of LAs communicates with the RA to provide linkage values necessary for certificate production, and assists the MA in misbehavior processes
LOP	Location Obscurer Proxy	Obscures the locations of requesting devices (e.g., OBE requesting certificates) from other functions, such as the RA
MA	Misbehavior Authority	Collects misbehavior reports from OBE and analyzes system-wide misbehavior. Coordinates with PCA and RA to produce CRL. Other activities include CRL generation, broadcast, and store; internal blacklist manager (IBLM); and global detection.
PCA	Pseudonym Certificate Authority	Generates and signs short-lived certificates

RA	Registration Authority	Coordinates certificate production with other functions; sends certificates to OBE (during full deployment)
Request Coordination	Request Coordination	Coordinates certificate requests from OBE to RA
Root CA	Root Certificate Authority	Provides system-wide confidence through CME certificates issued to all CMEs; represents the basis of confidence in the system
SCMS Manager	Security Credentials Management System Manager	Defines and oversees standards and practices for the SCMS, related to both technical and policy issues

The technical design of the SCMS is focused on communications and activities of the various PKI functions. Among other fundamental principles, the technical design for the system incorporates a "privacy by design" approach that separates information and organizational functions in order to mitigate potential risks to consumer privacy. The model depicted in Figure V-1 below illustrates one way these functions could be grouped into legal/administrative organizations within the larger SCMS "industry," while still protecting consumer privacy appropriately and ensuring secure, efficient communications.

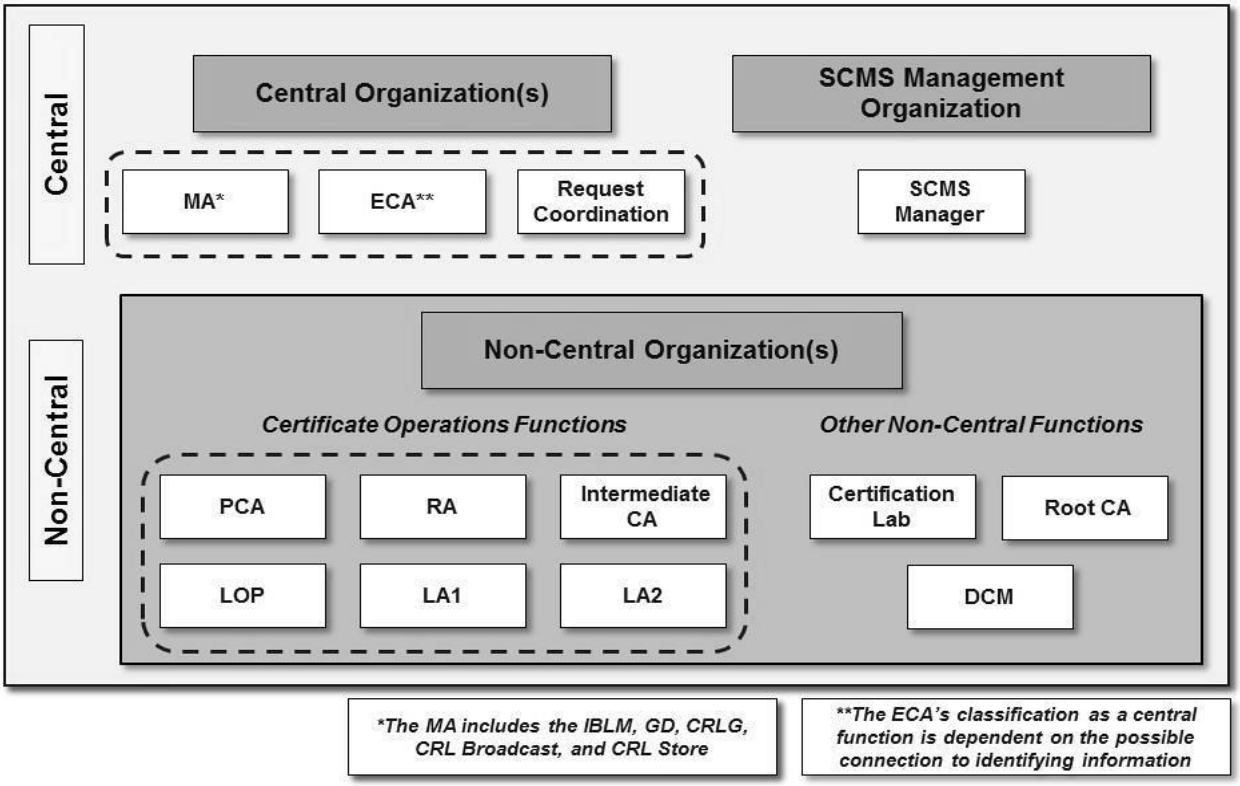

Figure V-1 SCMS Industry Model

Blue boxes in the diagram represent Certificate Management Entities (CMEs), or groupings of SCMS functions. Functions carried out within the CMEs are represented by the white boxes. For purposes of this illustrative model, these groupings clarify those functions that may be owned by multiple organizations, versus those that may be best handled in a more centralized manner. However, as noted in the V2V Readiness Report, ultimately, the decision as to which SCMS functions may be perform by a single entity and whether central and non-central functions may be combined are matters of governance defined by the system's Certificate Policy. For this reason, if this PKI technical design for the SCMS is implemented, the final decision on which organizations can be owners/operators and how scope and responsibility will be divided among the CMEs will likely be a central policy issue determined jointly by NHTSA and the entity that takes the lead in governing and coordinating operation of the V2V SCMS.

3. Independent Evaluation of SCMS Technical Design

The design of the Security Credential Management System has gone through many iterations and adjustments throughout V2V research program as the system has evolved to meet revised or additional needs. Additionally, evolutionary changes have occurred as a result of implementation and operation in support of the USDOT's Safety Pilot Model Deployment.

To better understand maturity and robustness of the SCMS, the USDOT retained the MITRE Corporation to conduct an independent evaluation and risk assessment of both security and privacy design features of the SCMS. This work was used to inform continuing refinements and provide USDOT with a basis for future policy and technical decisions related to deployment.

MITRE was directed to conduct: (1) an independent and comprehensive evaluation and risk assessment of the July 2013 SCMS design for a V2V connected vehicle environment; and (2) a technical analysis of the potential privacy risks of the entire V2V system that includes security but also focuses on the operation of V2V communications in support of crash avoidance safety applications.

The independent evaluation by MITRE identified security requirements needed to support secure V2V communications, and revisited threats and risks in relation to the design and how the identified requirements addressed the potential risks. The results of the SCMS design evaluation are detailed in Final Requirements Report, September 11, 2015, Report Number: FHWA-JPO-15-235, and Final Design Analysis Report, September 18, 2015, Report No: FHWA-JPO-15-237.

The MITRE evaluation was based on the previous 6 years of research that investigated core issues related to: securing DSRC communications; privacy implications; achieving interoperability; governance and organizational structure; and identifying and addressing communication threats and risks. The Government provided reports associated with these studies to the MITRE Corporation as a basis to conduct their evaluation and identify the

minimum requirements of the SCMS that would support the three primary components of the system that are:

1. V2V devices that support DSRC messages broadcast to and received from other devices; and the ability to send/receive messages to/from the Security Certificate Management System for digital security credentials that provide the means of message authentication;
2. A Security Certificate Management System (SCMS) which is the security organization that issues, distributes, and revokes digital security credentials. The SCMS is comprised of a number of entities and functions. It is also designed to detect and remove misbehaving devices; and
3. A communications network that facilitates two-way encrypted communications between an SCMS and a DSRC device (to include both vehicles and roadside units).

The MITRE evaluation focused on a revised SCMS technical design that benefited and evolved from knowledge gained during operation of a technical prototype implemented as part of the Safety Pilot Model Deployment. This prototype implementation exercised initial technical functionality needed to produce and manage security certificate material for the deployed devices, and, there was a rudimentary technical organization and management structure. This early SCMS prototype provided technical data related to PKI architecture and functions, and there were new insights gained regarding the over-the-air transmission of security materials and use of alternate communication media that include DSRC and cellular.

Prior to the MITRE evaluation were years of research conducted to understand and develop the SCMS design. The first forma research was conducted in 2010. CAMP commissioned 5 leading communication/internet security entities to assess the security needs and identify a security approach for DSRC communications. Security Innovations, Escrypt, Telcordia Technologies Carnegie Mellon University, University of Illinois at Urbana-Champaign, and General Motors India Science Lab investigated aspects of the system and collaborated on recommendations. Security Innovations and Escrypt conducted a risk analysis and identified initial risks related to broadcast communications among vehicles and devices. These risks included denial of service attacks, Sybil attacks, altered messages, replay of messages, and compromised nodes. The risks were rated and mitigation techniques identified. The risk analysis was combined with investigations by: Telcordia Technologies (design and analysis of applicable and scalable PKI systems); Carnegie Mellon and University of Illinois at Urbana-Champaign (adaptations to address privacy); and General Motors India Lab (misbehavior detection solutions). The overall recommendation was a PKI based system with frequently changing certificates.

Two years later after preliminary work was done on the SCMS design, USDOT and CAMP conducted a risk assessment based on the NIST 800-30 publication, Guide for Conducting Risk Assessments. Using the NIST framework, attackers and attack scenarios were identified. Identified attackers included, for example, a clever outsider and a well-funded foreign hostile organization. Attack scenarios included local and widespread Sybil attacks, Root

Compromise, Intermediate Certificate Authority Compromise, Registration Authority Compromise, False Misbehavior Report, False Certificate Requests, and Trust Management Compromise. For various attack scenarios risk was estimated based on likelihood and impact. The estimates were based on a modified NIST risk matrix given the NIST matrix did not rate any scenario as "high". The risk assessment identified Root Compromise, Intermediate Certificate Authority Compromise, Registration Authority Compromise, and Trust Management Compromise to have high risk even after possible mitigation techniques were considered. This work informed the next stage of SCMS design refinement which included (among other refinements) an objective of finding new innovative techniques to move high risks to medium risks, and medium risks to low risks.

An updated high level SCMS design was completed July 2014 and documented via 4 separate but connected reports that included: (1) Study 1, Security Credential Management System, Final Report, July 2014; (2) Vehicle Safety Communications Security Studies Final Report, July 2014; (3) Study 3 Final Report, Definition of Communication Protocols Between SCMS Components, July 2014; and, (4) Phase 2 Final Report Volume 3: Security Research for Misbehavior Detection, Nov 2014.

These reports formed the base of the information available to MITRE regarding the latest design of the SCMS.

Other reports provided to MITRE included past research findings concerning interoperability, initial communications security needs, and SCMS organizational analysis.

MITRE also had access the standards referenced in the reports that included SAEJ2735, IEEE 1609, and the latest input to SAEJ2945 that was being developed during the MITRE evaluation.

MITRE used the information described above to identify the minimum or essential requirements needed for a SCMS design to support the three primary components identified above (Final Requirements Report —September 11, 2015, Report Number: FHWA-JPO-15-235), and an assessment of how the latest SCMS design aligns with these minimum requirements (Final Design Analysis Report — September 18, 2015, Report No: FHWA-JPO-15-237). The Requirements Report also includes a risk assessment where MITRE reviewed past risk assessments and identified threats, threat actors, attacks, vulnerability, consequence, likelihood, impact severity, and risk in relation to the minimum requirements and latest design information base on the NIST 800-30, Guide for Conducting Risk Assessments.

The risk assessment assessed a number of possible threats to the system, some described by the CAMP reports, others identified by the MITRE team. Of the twenty-one threats identified, MITRE concluded that fourteen may be mitigated by a system design that conforms to

the minimum requirements, but for seven of the threats, no system design requirements seemed to apply[217]. In some cases, threats may be mitigated by additional system design features that perform to the minimum requirements. For other threats, no system requirements are listed. These include threats that involve compromises of or unauthorized access to SCMS or OEM system components or databases. For these, mitigation will depend not on system technical design but rather on implementation of security policies and operational practices that would be part of the SCMS operational governance function. Further, MITRE noted that such Governance functions and policies may be captured in documents such as a Certificate Policy and the Certificate Practice Statement. These documents and other governance policies and protocols will be developed as part of the SCMS PoC operations project that will support V2X deployment projects as discussed in Section V.B.6.e).

The MITRE Final Design Analysis report evaluates the SCMS design (as documented in the above listed Reports from CAMP) against a list of derived minimum requirements from the Final Requirements Report.

MITRE noted that the design of the SCMS has several innovative elements that deserve further development and analysis in future design revisions and system operational implementations. The list below identifies areas recommended by MITRE for further development:

- Required cyber-resiliency capabilities, such as designs for continuous monitoring for proper operation, anomaly detection functions, and systematic software reset of installed software components.
- Misbehavior Authority (MA) design. The MA constitutes a critical single point of failure as conceived. Additionally, it presents enticing points for adversary compromise against key system objectives surrounding trustworthiness, misbehavior handling, and acceptance.
- Design of capabilities that would enable secure updating of on board equipment (OBE), Security Credential Management System (SCMS), and other component software, especially given the complexity and lifetime of the system and its components.
- Completion and clarification of the specifications of the operation and reporting functions around misbehavior, blacklist, revocation, and of the data elements maintained.
- Evaluation of the reduction of risks in privacy protection with the pseudonym certificate (PC) design instead of other, less complex, yet suitable privacy sensitive designs.

[217] The threats list from the MITRE report is not a comprehensive list of threats or risks to overall V2V system success, but are focused on threats to the objectives of providing secure V2V communication, protecting the privacy of vehicle operators, and enabling the identification and removal of bad actors from system participation

The above areas will be addressed by USDOT and its industry partners as the SCMS design continues to be refined, and as part of the implementation and operation of the first-ever fully representative SCMS proof of concept (PoC).

Further, even though it is not yet clear whether the SCMS should be designated as a "critical national infrastructure", once the SCMS Proof-of-Concept becomes operational, USDOT intends to apply the NIST Framework for Improving Critical Infrastructure Cybersecurity, (currently, Version 1.0, February 12, 2014). Much of the guidance provided in The Framework for Improving Critical Infrastructure Cybersecurity is directed at organizational practices to identify cybersecurity risks; protect against threats and detect cybersecurity events; and respond to and recover from cybersecurity breaches. As the SCMS PoC organizational design and governance policies mature and are actually being implemented, then USDOT will be able to apply the NIST Framework to help identify and mitigate residual risks.

In should be noted that USDOT (and MITRE) were precluded from applying the NIST Framework for Improving Critical Infrastructure Cybersecurity because the design of the SCMS was only conceptual (not yet implemented) and detailed organizational designs, governance structures, and operational policies and procedures remained to be completed and implemented. However, the risk assessment performed by MITRE did follow the basic process of identifying the state of the current system and developing a target state of cybersecurity to obtain through refinement and additions to technical, operational and governance aspects of the system. Examples include the MITRE risk assessment, the investigation regarding the role, functions, and governance responsibilities of an SCMS manager, and the analysis and evaluation of cybersecurity protection needs that moved the protection requirement from FIPS-140 Level 2 to Level 3. The SCMS design continues to mature to address risks such as Root Compromise[218] and software updates. Continued refinement is also evident through the "SCMS Proof-of-Concept End-Entity Requirements and Specifications Supporting SCMS, Software Release Version 1.1, being used by Connected Vehicle Pilots as they prepare to connect to the SCMS PoC for security.[219]

Further, it should be understood that the SCMS PoC is being implemented at this time by USDOT to serve USDOT sponsored demonstrations and early deployments—and to allow for a better understanding both technically and operationally of how the SCMS may be deployed at a national level. To this extent, the designs, methods, policies and procedures implemented to ensure secure communications, manage privacy risks, and address cybersecurity threats will need to be accepted and implemented by the private entities that choose to establish and operate a National SCMS.

---

[218] See Root Elector System Design at http://www.mycreativeregistry.net/IPCOM/000245336 (last accessed Dec 4, 2016)

[219] The EE Requirements and Specifications can be found via the following link: http://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf (last accessed Dec 7, 2016)

We welcome comment concerning: the cybersecurity risks associated with the SCMS; the analysis methods used to date to assess risk; and what framework/assessment methods should be used during SCMS PoC implementation and operation; and any other information regarding possible threats and risk that have not yet be identified.

4. SCMS RFI Comments and Agency Responses

As discussed in Section II.F, NHTSA issued a Request for Information (RFI)[220] regarding a potential Security Credential Management System (SCMS) that could support the National deployment of a secure V2V communication system.

The purposes of the RFI were to help the agency: (1) Become aware of private entities that may have an interest in exploring the possibility of developing and/or operating components of a V2V SCMS; (2) Receive responses to the questions posed about the establishment of an SCMS provided in the last section of the RFI; and (3) Obtain feedback, expressions of interest, and comments from all interested public, private, and academic entities on any aspect of the SCMS.

NHTSA received twenty-one responses to the RFI with approximately eleven of the responses indicating an interest in running aspects of, or the entire, SCMS. The respondents included vehicle manufacturers, software component developers and suppliers, cryptography experts, certificate management entities, satellite and cellular service providers, and academia.

Deployment of a V2V communications system, and of an SCMS to support confidence in V2V communications, are unprecedented activities. For this reason, the agency believed it was appropriate to meet with a subset of respondents, the eleven expressing interest in operating aspects of the SCMS or the SCMS as a whole, to ensure there was a shared understanding of respondents' comments, potential role in an SCMS, and the agency's position on a possible SCMS creation and implementation. The agency was able to meet with ten of the eleven respondents that had indicated interest in operating aspects of a potential SCMS. One respondent, Verizon, was not able to meet with the agency. The meetings took place between January and March of 2015 at DOT headquarters either in person or via teleconference.

Overall, the meeting discussions were very informative and the agency greatly appreciated the time and effort the respondents expended following-up their RFI responses. In general, based on the RFI comments and the discussions with respondents, the team identified the following key themes concerning various aspects of the SCMS.

- Government must play a significate role in the establishment and management of the SCMS.

---

[220] 79 FR 61927 (Oct 15, 2014).

- Business opportunities are seen at the CME and Security services levels.
- Security system entities understand the relationship of the design to privacy, with some indicating they may be able to find some efficiency as they develop their systems.
- One respondent indicated that the design sets a new paradigm that other regions may adopt in the future.
- An SCMS Board of Directors needs to be initialized by the Federal Government – specifically citing the existing ICANN Model,[221] charged with managing the world-wide-web domain and server naming allocation and standard, as an example framework that could transcend to V2V.
- Establishment of the SCMS Manager would require capital/initial funding.
- One entity discussed being the SCMS Manager.
- One entity indicated they would build and operate the entire SCMS system but would need another entity to be the SCMS Manager.
- Little information provided about potential financial models.
- Possible revenue sources included: CME license fees, certificate subscription fees, yearly service fees.
- To move forward with development/deployment, all indicated they need more information regarding the Government role, the SCMS Manager, and details about the security design.
- Liability was a major concern, with a strong interest from all participants in some form of Federal indemnification.

a) SCMS RFI Comments

(1) UMTRI

The University of Michigan's Transportation Research Institute (UMTRI) met with representatives from the NHTSA V2V NRPM Team to discuss their SCMS RFI response. UMTRI's response provided views regarding privacy, governance, potential SCMS component separation and linkage. UMTRI's RFI response indicated other parties may be better suited to respond on specific governance organizational aspects but supported a public-private partnership model for overall governance, a potential model discussed in the V2V Readiness Report. UMTRI went one step further by offering the suggestion of an additional "public-private-academic" model that could potentially benefit from an academic partner's fundamentally neutral stance, little commercial interests and direct access to significant research resources. More specifically, UMTRI expressed interest in participating in the SCMS Manager and potentially being "a proper candidate" for operating the two Linkage Authorities identified in the current system design. UMTRI indicated their regular work on classified projects, existing

[221] See, e.g., https://www.icann.org/resources/pages/chart-2012-02-11-en (last accessed Dec. 7, 2016).

infrastructure, and their experience "running highly privacy sensitive computer systems such as the University of Michigan Health System support their interest in operating the Linkage Authorities."

UMTRI indicated other parties may be better suited to provide a response regarding financial sustainability. In our meeting, however, UMTRI indicated they could possibly pose the SCMS financial sustainability proposition to their MBA students as a potential project.

When discussing potential SCMS operational and policy standards, UMTRI indicated support for NHTSA's approach that SCMS components like the CME should be legally distinct. Support for keeping SCMS components legally separate is rooted in the need to ensure privacy and based on the key notions that firewalls within a single legal entity might not be sufficient to ensure privacy, different legal organizations will most likely protect a data center with a differing technologies, and that distinct legal organizations inhibit the possibility of a single point of entry into multiple systems.

UMTRI suggested two types of operational policies, Type 1 for applications that are under governance of SCMS Manager (e.g., V2V safety applications) and Type 2 for applications that are not under the governance of SCMS Manager but are part of the V2X application portfolio (e.g., mobility applications provided by third party providers).

(2) Certified Security Solutions, Inc.

Certified Security Solutions, Inc. (CSS) represented the exposure to new potential stakeholders, suppliers, and services V2V is bringing to NHTSA. CSS supplies security solutions such as security certificate management systems and managed public-key infrastructures (PKI). CSS also provides digital security consulting services related to PKI and identity and access management. Historically, the agency has not interacted with suppliers such as CSS in the course of regulating vehicle manufacturers and, similarly, CSS has been involved with industries far removed from the auto industry, such as supporting digital certificates for surgical devices like heart pacemakers.

CSS indicated interest in three areas of the SCMS: 1) participation in an advisory board regarding the policy, specifications, and requirements of the SCMS, V2V initiative, and its components, 2) creating components and solutions, such as the Registration Authority or Device Configuration Manager, and 3) creating software and/or managed service offerings for operations and oversight such as "dashboards" used for monitoring system performance.

CSS's response to the RFI centered on the first question related to governance. CSS foresees a large and diverse array of participants involved in the operation of a National SCMS deployment. As such, CSS indicated examples of "self-governance" advisory boards that have, "proven to be relatively effective in improving the interoperability and overall security of their respective areas." In their view, CSS suggested that this sort of overall model "makes the most sense when considering the magnitude and importance of an initiative such as the SCMS." These examples included:

- The certification authorities (CA)/Browser forum (https://cabforum.org), comprised of CA and web browser vendors with a focus on defining a coordinated set of guidelines to improve browser and SSL security.
- The Internet Engineering Task Force (IETF) (www.ietf.org) and its collection of specific Working Groups.
- The Industrial Internet Consortium (www.iiconsortium.org), an industry-driven working group aimed at solving the challenges posed by large-scale machine-to-machine (M2M) communication.

The agency's meeting with CSS yielded additional details on their written response along with ideas for potential approaches to a National SCMS deployment. At the highest level, CSS indicated a potential SCMS advisory board would be responsible to define the appropriate certificate policy standards to ensure consistent and successful implementations that will be required for the anticipated multiple CAs deployed across multiple systems.

CSS indicated that utilizing multiple root CAs may benefit from redundancy versus a single root CA, and also brought forth the notion of "bridged" root CAs that could be cross-signed to allow different vehicle or device manufacturers to "trust" each other while maintaining their own "root of trust," enhancing confidence in message exchanges.

SCMS financial sustainability discussions were limited to existing approaches for certificate management services, where per certificate fees could potentially be avoidable.

(3) Trustpoint Innovation Technologies, Ltd.

Representatives from Trustpoint Innovation Technologies met with the V2V NPRM Team to discuss their submission to the RFI response. Trustpoint was founded in 2012 by Dr. Scott Vanstone and Sherry Shannon. Mr. Vanstone was also a co-founder of Certicom, whom also provided a response the SCMS RFI, which was acquired by BlackBerry in 2009.

Trustpoint has been involved with the SCMS and security design research conducted with the agency's research partner, CAMP. Trustpoint's response to the RFI focused on their interest in helping to develop deployment-ready SCMS components such as the Pseudonym CA, Registration Authority, Linkage Authority, Enrollment CA, Intermediate CA, and Root CA.

Trustpoint indicated that significant investment and development in software and testing will be necessary to deploy a National SCMS. This is based on their belief the PKI approach used for SCMS research will need to be extended and extensively proven for a production system, based on the need for a new software stack[222] built around new cryptography and

[222] A software stack is a set of programs that work together to produce a result; typically an operating system and its applications. For example, a smartphone software stack comprises the operating system along with the phone app,

protocols. Trustpoint is interested in being part of a consortium to deploy production SCMS components.

When meeting with the agency, Trustpoint expanded on their views of a National SCMS deployment. The key discussion points included cryptography approaches, attack vectors, participation in a consortium, and thoughts on production deployment that includes clear policies and procedures, and thoughts on device level security. In addition, Trustpoint reviewed the cost model the agency provided with the ANPRM and V2V Readiness Report.

Trustpoint discussed how Elliptic Curve Cryptography (ECC) is, in their opinion, the only feasible security solution for resource-constrained environments where processing power, power consumption, storage space, and bandwidth are limited. In comparison to RSA,[223] an early wide-spread remote device security mechanism, ECC is much more compact yet provides a higher level of security. Trustpoint indicated that 500 bits of ECC information is equivalent to nearly 1500 bits of RSA cryptographic information.

Trustpoint supported the development of a "test bed" for components that could operate in a National, deployed system. Successful deployment and verified operation in the test bed could be considered "certified for deployment." Components certified in the test bed would support an "off-the-shelf" software component approach that, for example, would yield Registration Authorities for each manufacturer. Trustpoint stressed the need to have standardized components for consistent system interaction while allowing each OEM to manage their vehicle fleets individually versus a central management approach. The SCMS Proof of Concept project currently under development by the agency and CAMP, to support connected vehicle test beds that will be deployed regionally along with expansion of the Safety Pilot Model Deployment environment more broadly throughout southeastern Michigan, could potentially serve as a test bed for broader, National system deployment. Trustpoint suggested, however, that additional definition and implementation will be needed in the areas of operation, management, and auditing for a successful National SCMS deployment.

Trustpoint suggested the cost model provided by the agency and used in the V2V Readiness Report cost calculations needed some adjustment in the areas of bandwidth, hardware security module, and software development costs. More specifically, Trustpoint indicated replication for hardware security would be needed for redundancy and continuous, uninterrupted system operation. Trustpoint estimates the annual issuance of 36 million certificates will have additional bandwidth needs beyond that estimated in the cost model. Finally, Trustpoint believed the software development cost used in the cost model was substantially underestimated.

Web browser and other basic applications. See http://www.pcmag.com/encyclopedia/term/51702/software-stack (last accessed Dec. 8, 2016).

[223] RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet. See http://searchsecurity.techtarget.com/definition/RSA (last accessed Dec. 8, 2016).

(4) DURA Automotive Systems, LLC

Dura Automotive Systems, LLC is a Tier 1 supplier to the automotive industry supplying structural body systems, mechatronic control systems, and exterior systems including window systems and exterior trim. Dura responded to the SCMS RFI with a vision of how the SCMS Manager could be formed, implemented and sustained. Dura indicated they would like to fulfill the role of developing and implementing the SCMS governance board and participating as a member. Dura was the only respondent indicating interest in taking the role of developing functions at the SCMS Manager level and above.

Dura favored a private model governance approach for the SCMS, excluding some identified issues. In their response, DURA identified two successful examples of both private and public models currently in place that address requirements similar to those identified in the RFI. A private model example is the Internet Corporation for Assigned Names and Numbers ("ICANN"),[224] a private, not-for-profit corporation established in 1998. The public model cited by Dura is the operating arrangement for the Federal Aviation Administration (FAA) and the national air traffic control system.[225]

DURA specifically suggested, "a policy statement from the Department of Transportation advising the public that the U.S. government is prepared to enter into an agreement with a new, not-for-profit corporation formed by private sector transportation multi-stakeholders to administer the Security Credential Management System" and suggested the corporation be referred to as, "the Inter-Connected Automotive Safety Network ("ICASN"). Additionally, Dura suggested that its incorporation, governance and operation mirror as much as possible to that of ICANN."

Dura suggested a subscription-based approach for ongoing SCMS sustainability and further recommended "aligning the subscription period with vehicle licensing / annual license plate renewal." Dura also commented on how liability for system operation could influence costs; more specifically, from an insurance cost perspective.

(5) Bosch – ESCRYPT

Robert Bosch LLC affiliate ESCRYPT provided a response to the SCMS RFI with comments on potential governance strategies and expressed interest in implementing the Pseudonym Certificate Authority (PCA) and Linkage Authority (LA) components.

---

[224] For more information on the ICANN private model, see https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en (last accessed Dec. 8, 2016).

[225] For more information on the public FAA model, see http://www.faa.gov/about/office_org/headquarters_offices/agc/pol_adjudication/agc400/litigation/ (last accessed Dec. 8, 2016).

Bosch-ESCRYPT supported a private-public collaboration versus a self-governance model and commented that SCMS ownership should take a multi-layered approach, with high level policies residing within the USDOT and lower level implementation responsibility given to private organizations. ESCRYPT supported having the SCMS spread amongst differing, distinct organizations to help maintain privacy, and recommended a governance board to fulfill the SCMS Manager function, with membership defined by NHTSA but to include representatives from government, vehicle manufacturers, private organizations, and privacy groups.

ESCRYPT expressed interest implementing a production SCMS PCA and LA based on their support of the Safety Pilot Model Deployment. In their SCMS RFI response, ESCRYPT proposed an architecture that utilizes two types of certificates to ensure privacy. The first is short term pseudonyms, lasting from seconds to hours and being switched frequently. The second is long-term certificates along with three Certification Authorities: Long-Term; Pseudonym; and a Resolution Authority, the latter of which strips anonymity from pseudonym certificates that are believed to be a potential threat.

When meeting with the agency, Bosch-ESCRYPT expressed the importance of regional policy harmonization and stable standards, indicating that, once implemented, these important pieces will be not be changed easily or quickly.

The agency asked ESCRYPT for their experience on device management and how ESCRYPT has handled conditions such as managing and closing security breaches, device "end of life" management, and hardware security to help inform potential approaches for this NPRM. ESCRYPT indicated that over-the-air (OTA) software update is the best approach to closing potential security breaches and in support of NHTSA's vital recall efforts. When discussing device "end of life" scenarios, ESCRYPT suggested the approach of revoking existing certificates for an identified device and preventing future certificate updates allowing, in theory, the device to "fade away" from the system. Finally, when discussing potential hardware security needs, Bosch indicated they have experience with hardware security modules ("HSM") and secure hardware extensions ("SHE") successfully deployed in Europe and that, in terms of V2V, a lower-security implementation limits potential use cases of a system. The agency interprets this discussion, overall, that proposing a hardened device could extend a device's capability and contribute to overall system confidence.

(6) Certicom/Blackberry Technology Solutions

Certicom, a wholly owned subsidiary of Blackberry Ltd., provided a response to the SCMS RFI and also met with the agency to follow-up their response. Certicom provides "applied cryptography and security solutions for the embedded market" including engagement with governments and vehicle OEMs. Certicom has experience implementing Elliptic Curve Cryptography (ECC), "which provides the most security per bit of any known public key cryptosystem." Certicom's parent company, BlackBerry, builds devices used by government and enterprise organizations, and operates a global secure network and mobile messaging platform. BlackBerry Technology Solutions also operates BlackBerry's QNX group which has presence in automotive telematics implementations.

Certicom supported a private consortium to manage a V2V SCMS, indicating that this approach could help "accelerate the deployments of V2X systems" serving both infrastructure and aftermarket devices. They stated that a possible "concern could arise if regulation unnecessarily limits the opportunity for participants to drive commercial innovation." Certicom expressed interest in the SCMS operational roles of the Certificate Management Entity (CME) such as operating a Certification Authority (CA) and/or a Registration Authority (RA). However, Certicom indicated revenue models and costs would need to be better understood before committing definitively to any portion of the system operation.

Certicom commented that long-term viability of the SCMS is highly dependent on public acceptance. As such, participants in the system need a strong public identification (brand) and experience with successful security, safe, reliable and privacy implementations.

During the agency's meeting with Certicom, the discussion focused on clarifying the RFI responses but also in key areas of revenue generation, security approaches, and certificate and device management approaches used for Blackberry devices and other implementations that Certicom has supported, which includes public utility installed residential "smart meters."

Certicom indicated there could be many reasons that entities would want to participate in a National SCMS and there could be potential opportunities presented such as the support of the security needs for manufacturing and system operations. In addition, expanded future roadside equipment could lead to yet-unknown revenue generation opportunities. Overall, V2V and a supporting SCMS could, in theory, "create a whole new market." Certicom also suggested participants in the SCMS could generate on-going revenue by royalties from device manufacturers.

In terms of approaches to device security, Certicom indicated there are at least three security key-scenarios for devices. The following table provides an overview of these approaches and a corresponding, relative level of security provided by each.

Table V-2 Overview of Security Approaches

Security Method	PKI	Keys/Certificates sent to device at time of manufacture	In device chipset ("silicon")
Example	Thermostat	Telematics	Blackberry
Relative Security	Sufficient	Better	Best

When discussing device and certificate management, Certicom provided an overview of three certificate distribution and management systems: Blackberry PKI, the ZigBee Smart Energy public utility residential meter system, and Certicom's approach to certificate and asset management for device original equipment manufacturers (OEMs).

The certificate service for Blackberry devices is designed for scalability, and secures devices from "birth" where a registration "seed" is embedded in the a device's onboard

microchip ("silicon") at the time of device manufacturer. The registration seed could be viewed like a V2V enrollment certificate, all of which is linked to the "root of trust" for the Blackberry ecosystem.

Certicom's overview of the ZigBee public utility smart meter certificate system varies from Blackberry devices, in that devices participating in that system are supplied from various manufacturers – similar to how V2V device implementation is envisioned, but the ecosystem itself could be viewed as localized.

In this implementation, ZigBee "Smart Energy" device certificates utilize an EQCV format issued in batches of one million. Certicom indicated they are able to issue approximately one million certificates in approximately one and half hours of processing. Each device participating in the system is identified by unique vendor identification, and verification is performed to confirm that each device's media access control (MAC)[226] address is unique. Key pairs for each device are then bound to the device MAC address and vendor ID through the certificate. Figure V-2 shows a graphic representation of the ZigBee certificate management system.

[226] Media Access Control address refers to the unique 48-bit serial number in the network circuitry of Ethernet and Wi-Fi devices that identifies that machine from every other globally. See http://www.pcmag.com/encyclopedia/term/46422/mac-address (last accessed Jul. 14, 2015).

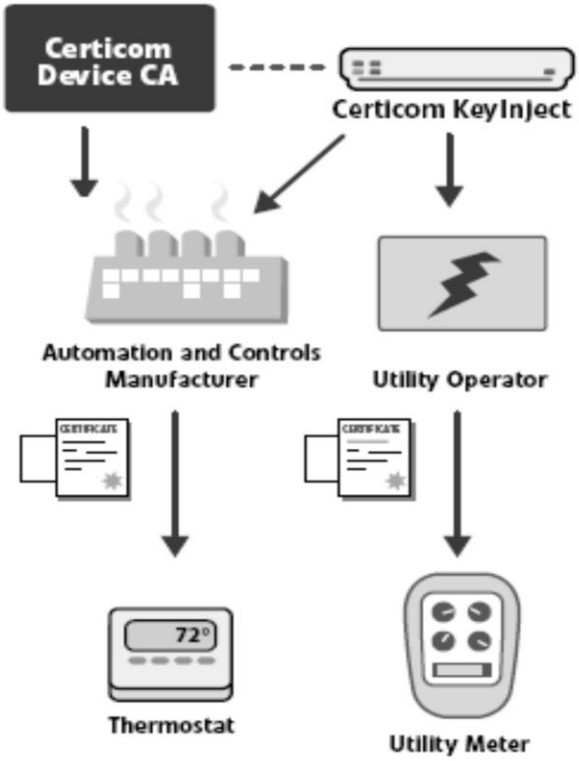

Figure V-2 ZigBee Smart Energy Certificate System

Finally, Certicom provided an overview of a certificate authority and asset management system that they are able to supply for device original equipment manufacturers. The system is designed to enable OEMs and silicon vendors to remotely secure devices that are assembled at geographically-dispersed locations, similar to how vehicles are assembled. The system described provides operational visibility and control of secure key injection into a device at time of manufacture or initialization, secure device serialization and tracking, and support for anti-cloning and anti–counterfeiting. Figure V-3 provides a representation of this system and shows the remote management across various locations. The "tester" would be the point of security key injection into a device.

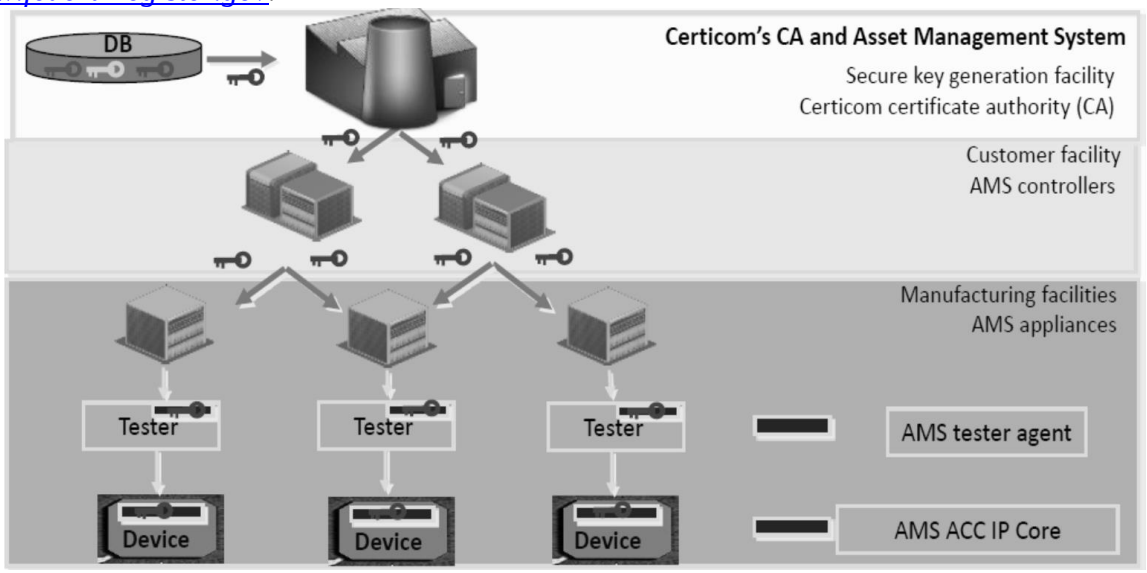

Figure V-3 Certicom Certificate Authority and Asset Management System

Certicom indicated that this system enables OEMs to manage and distribute the sensitive security keying material, along with potentially other sensitive information, to an untrusted contract manufacturing environment supplying components for their end product. Figure V-4 shows the process flow for loading security information to a device in an untrusted manufacturing environment.

NOTE: This document has been signed and we are submitting it for publication in the Federal Register. While we have taken steps to ensure the accuracy of this Internet version of the document, it is not the official version. Please refer to the official version in a forthcoming Federal Register publication or on GPO's Web Site. You can access the Federal Register at: www.federalregister.gov.

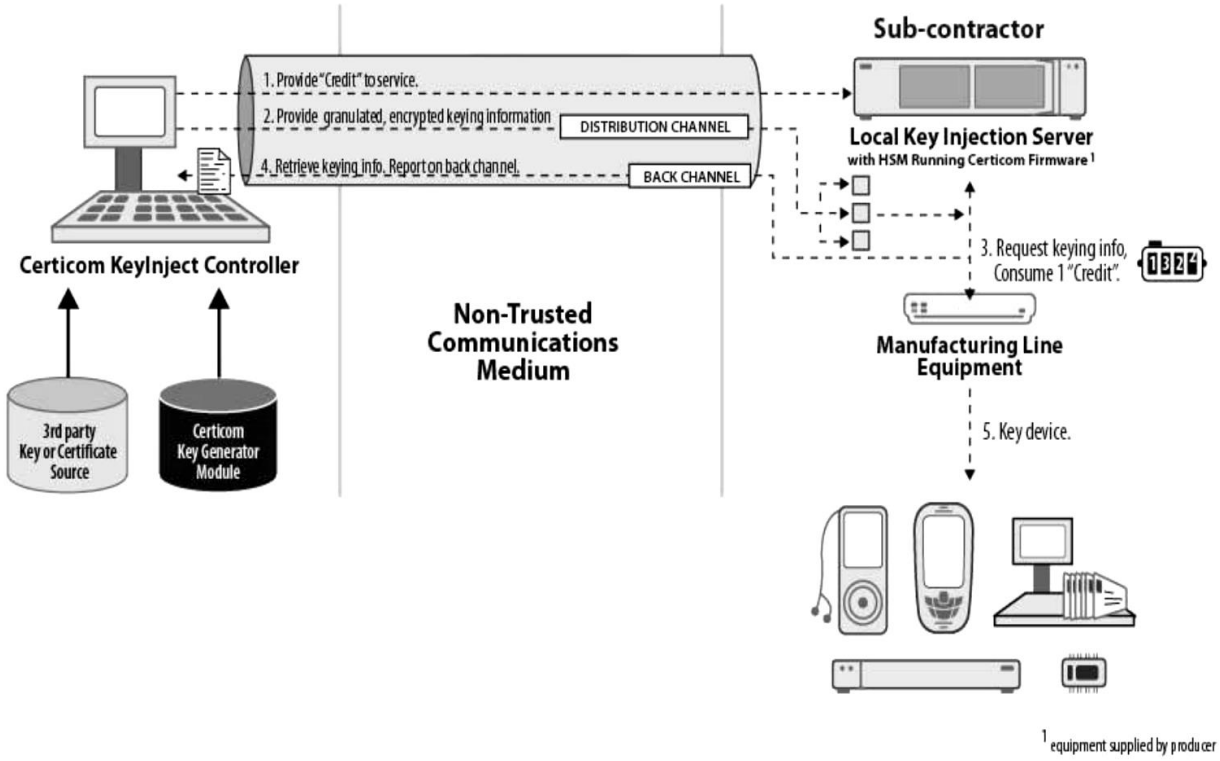

Figure V-4 Secure device manufacturing in an untrusted environment

As mentioned elsewhere in this section, device management also involves potential updates to device software to support technology updates and, importantly, in support of potential device recall scenarios. Certicom discussed Blackberry's OTA update service used for updating, configuring, and managing software and applications. Their updates leverage the existing Blackberry exclusive secure infrastructure for global distribution. This system also gathers status and data to support fleet monitoring capabilities for device operation. A graphic overview of the system is shown in Figure V-5.

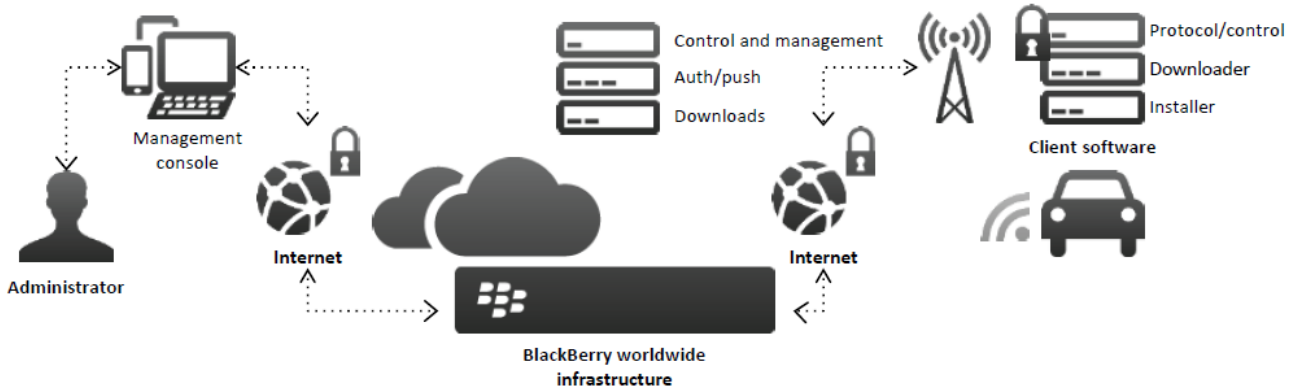

Figure V-5 Blackberry over the air (OTA) device update system

With end-of-life and misbehavior being key elements of a national V2V deployment, the agency inquired about approaches for managing devices under these conditions. Certicom indicated that Blackberry devices can be remotely made non-functional ("bricked") when a device is determined to be out of service, stolen, not functioning properly or potentially "misbehaving." Reactivation of a "bricked" device requires interaction with Blackberry.

(7) SiriusXM Satellite Radio

SiriusXM Satellite Radio provided a response to the SCMS RFI and also met with the V2V NPRM team as follow-up. Their written response to the RFI focused on the opportunity for satellite transmission to perform non-safety-critical, "back haul" type operations for a SCMS. This could include certificate distribution, over the air updates, and certificate revocation list distribution, among other potential supporting transactions. SiriusXM commented that employing a satellite network as an alternative distribution path for safety certificates and the CRL would promote the development of a V2V system by enhancing scalability and the SCMS network footprint, and enable faster distribution of security information for V2V-equipped vehicles.

SiriusXM indicated that satellite transmission could potentially "bridge the gap" between initial V2V deployment and roadside unit deployment and, in the longer term, support more remote regions that may not have roadside units deployed. SiriusXM indicated that their infrastructure "could provide the ubiquitous, simultaneous, and robust distribution of security certificates and the certificate revocation list ("CRL") in a V2V system." SiriusXM's satellite network covers the contiguous United States and portions or Canada and Mexico, which could possibly assist with potential cross-border challenges. Their network also includes signal repeating equipment to supplement service in urban areas where satellite reception could be blocked by buildings or other obstacles.

According to SiriusXM, 69 million vehicles are currently equipped with their radios, and they expect this to increase to 100 million vehicles by 2017 as approximately 70% of new vehicles are equipped with their receiver.

When discussing privacy, SiriusXM indicated that no subscription would be required to receive satellite V2X data and that it would be available to any vehicle equipped with their satellite receiver. SiriusXM did not present any potential revenue generation concepts during the discussion. Additionally, SiriusXM stated V2X will be a transparent data service on its system, meaning that no V2X-related data is collected on the vehicle, and that the satellite delivery system has no knowledge of which vehicles are active and receiving data or where vehicles are located.

In terms of device management, SiriusXM suggested a hardware security module (HSM) for V2V-enabled devices as part of a trusted, secure data exchange environment. SiriusXM provided very detailed technical descriptions of how device-level security could be implemented

and managed using satellite radio service. This included discussing the potential use of group codes, interaction with the HSM, in-use certificate downloads, available service channels, and revoked vehicle identification, all of which leverages its experience with the development and deployment of its satellite radio network that appears to have addressed many similar challenges found in V2V device deployment and management.

(8) Ford Motor Company and Volkswagen Group of America

Ford Motor Company ("Ford") and Volkswagen Group of America ("Volkswagen") submitted joint comments to the SCMS RFI. Together, Ford and Volkswagen indicated they are encouraged by the progress made in the collaborative activities between NHTSA and CAMP, in which they participate. However, they state in their comments that remaining items need resolution to enable an effective deployment of a V2V communications system, such as: 1) NHTSA's authority to mandate an SCMS; 2) an acceptable and stable funding model, and; 3) measures to address potential liabilities associated with participating in and/or being subject to a SCMS.

Ford and Volkswagen commented that the SCMS cannot be a private entity because vital functions of the SCMS cannot be delegated to a "private" entity, "which lacks the authority to require all participants in a V2V (let alone V2X) communication system to adhere to the system's necessarily rigorous operational policies, and enforce revocation based on unacceptable performance." Ford and Volkswagen stated that they, other OEMs, and others that will necessarily rely on the SCMS must have a role, along with government, in establishing SCMS operational policy. Additionally, they stated that Federal authority over the SCMS is essential and a binding governance board for SCMS management is needed.

Finally, Ford and Volkswagen stated that funding for centralized SCMS components or functions should come from a federal source. They do not support any funding model relying on the sale of data to third parties, and, additionally, the SCMS funding model "should not be based on a potential requirement that specific services must be enabled within the vehicle to offset operational costs." Conversely, non-centralized components, like the certificate management entity (CME) or registration authority (RA), could be established independently for their own use.

(9) SAE International

The Society of Automotive Engineers ("SAE") responded to the RFI with interest in playing a supporting role in SCMS deployment. SAE indicated interest in working with SCMS stakeholders in a partnership and/or larger consortium to support the SCMS functions, "through a combination of standards development, conformance programs and training."

SAE International standards J2735 and J2945 were revised and are being developed to support a national V2V deployment by providing a consistent, standardized approach to V2V device implementation across the industry.

(10) The American Motorcyclist Association

The American Motorcyclist Association ("AMA") commented to the SCMS RFI by urging DOT to test the V2Vcommunication systems to ensure that motorcyclists' safety and privacy are secure. AMA expressed their support for DOT's position "for further testing before adopting the rule authorizing U-NII devices (e.g., Wi-Fi) to operate in the band to ensure vehicles using advanced crash-avoidance and vehicle-to-vehicle technologies are not compromised." AMA also expressed concern about the potential for "hacking" into a future V2V network, and specifically, the potential to manipulate traffic signals which could be "especially disconcerting for motorcyclists who comprise the most vulnerable roadway user group." AMA closed their comments stating that the safety of all highway users should always be a priority whenever new technologies are considered.

(11) Alliance of Automobile Manufacturers, Inc.

The Alliance of Automobile Manufacturers, Inc. ("Alliance") reiterated their comments to NHTSA's V2V ANPRM where they "agreed with NHTSA's assessment that a strong SCMS is necessary for a properly functioning V2V communications system." The Alliance also reiterated its ANPRM comments expressing concerns with how a privately-run SCMS could address the broad structural and governance challenges that an SCMS manager would need to address, such as:

- Funding, deployment, operation and maintenance of a DSRC-based V2X security communications network
- Sustainable funding for V2X PKI security system operations and management
- Governance of a V2X security system (Rules of Use, Certification, and system access)
- Protection of consumer privacy
- Liability, risk management, and intellectual property protections
- International considerations including possible Canada-US-Mexico cross-border traffic, international agreements, or standards harmonization.

The Alliance maintained in its RFI response that addressing the above policy issues, which are necessarily national in scope, requires strong unified Federal leadership, not just presence.

(12) Association of Global Automakers

The Association of Global Automakers ("Global Automakers") provided general comments along with direct responses to the RFI questions. In its comments, Global Automakers strongly supported a public-private partnership model for SCMS operation by stating that "the agency has underestimated the necessary governmental role in managing the SCMS and too narrowly constrained the participation of other agencies in SCMS operations.

Contractor operation of many aspects of the SCMS is feasible but must be conducted under the authority and supervision of a significant governmental entity."

Global Automakers further stated that, to be effective, the SCMS must be a monopoly, which is not allowed under law for a private entity, and that funding for the SCMS should come from the government rather than from revenue generated by consumers; less potential consumer subscription funding opportunities for some potential V2I services. Additionally, the SCMS should be developed to support V2V and V2X holistically, at the outset, in partnership with the Federal Highway Administration (FHWA) and possibly other agencies such as the Federal Communications Commission and the Federal Trade Commission where privacy is of concern. Global Automakers stated that cross-agency coordination and harmonization is critical to the effective operation of the SCMS.

Global Automakers expressed concern with the potential approach for the "Device Non-compliance and Potential Recalls" discussion in the RFI materials, specifically, that it believed that the approach suggested by the agency would undermine consumer privacy, be impractical, and be redundant to systems that are already in place to manage recalls. It commented that the proposed "link between specific installed V2V devices or production lots of devices and enrollment certificates" would create a potential perception that V2V communications could be traced to individual vehicles and drivers.

(13) Verizon Communications, Inc.

Verizon Communications' RFI response focused on potential steps and pathways to achieving a National SCMS deployment and focused on three key approaches to SCMS policies and operations standards and potential adjustments to the PKI implementation. In more detail, Verizon suggested that: (1) NHTSA should define a system of policies, regulations, workflows, and technical interoperability that provides for the management and control of the overall SCMS; (2) implement an "identity PKI" as a baseline and "bootstraps" anonymously allowing linkage between certificates and supporting potential device recalls; and (3) an "anonymity PKI" solution that allows the device to perform any necessary operations anonymously.

(14) General Motors, LLC

General Motors, LLC ("GM") submitted comments to the SCMS RFI that also included broader V2V rulemaking comments. GM stated, in the broader context of V2V, that they support NHTSA's rulemaking initiative for all passenger cars and light trucks to be sold in the United States, and that "a comprehensive and connected ecosystem must be developed and implemented offering seamless and trusted communication between vehicles" to obtain all the potential benefits of V2V technology. GM commented that it strongly believes that a NHTSA rulemaking process is the only method to successfully establish a V2V ecosystem; that, as envisioned, the system cannot be established and managed by a single manufacturer or industry group.

Focused comments regarding the SCMS stated its belief in the requirement for Federal oversight of the SCMS Manager, the central root authority organization, direct engagement with the Misbehavior Authority and coordination of certification labs.

(15) CTIA–The Wireless Association

CTIA is an international nonprofit organization representing the wireless communications industry. CTIA's members include wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products. CTIA's comments to the SCMS RFI focused on the benefit of leveraging existing authentication and security technology, along with utilizing existing networks and infrastructure to promote standardization and interoperability. CTIA also stated that the private sector is best positioned to address V2V SCMS cybersecurity and privacy concerns and should be utilized to help implement cybersecurity best practices.

(16) Tesla Motors, Inc.

Tesla Motors, Inc. ("Tesla") commented primarily on the security of the SCMS design presented in the V2V Readiness Report by urging NHTSA "to ensure that all possible security aspects are considered and accounted for when implementing its chosen design." Tesla commented that much more analysis and consideration needs to be given to the SCMS before it is implemented as proposed. Tesla acknowledges that it has not been involved with the Crash Avoidance Metrics Partnership (CAMP) consortium and that this brings a new perspective to the CAMP SCMS design.

Tesla believes that, as envisioned, the CAMP system fails to consider adequately how the system could be attacked or the vast amounts of information that will necessarily pass between vehicles and that NHTSA's proposed system has gaps that must be addressed before it is implemented.

Tesla narrowed its primary concerns into the following: 1) because inputs are insecure, false messages are likely, even with secure V2V subsystems; 2) vehicles must have some way to determine whether messages, particularly misbehavior reports, are legitimate; 3) certificate revocation lists ("CRLs") do not scale well for widespread use; 4) public-key cryptography is poorly suited to the demands of an embedded, high-speed environment; and 5) transmitted messages could be the source of privacy breaches.

Tesla concluded their comments by stating that "the Company believes that the CAMP system has fundamental issues and challenges that must be revisited in order to allow for successful implementation of the SCMS."

(17) Intercede Ltd.

Intercede, Ltd. is a software company solely focused on producing and delivering identity and credential management solutions to entities such as Government, Aerospace and Defense,

Finance, Healthcare, Large Corporations and Managed Service Providers. Intercede's response to the RFI focused on the need for the SCMS to provide a secure and trusted environment for V2X, and stated that it will be necessary to consider the V2X communication devices over their entire lifetime, which was defined as:

- Initial manufacture;
- Upgrade;
- Maintenance;
- Transfer of ownership;
- Renewal;
- Compromise;
- Natural end of life.

Intercede's response went on to state that "it is also important to consider the interactions beyond the communication channels that must be established into a secure trust system. Failure to do so would open up potential back doors into this trust system that could allow for compromise to occur from within." Follow-up discussion with Intercede stressed its views regarding the need for a complete, systems approach to security – encompassing "cradle to grave" for devices. And that, "By adopting a controlled and secure approach to device identity management, NHTSA will enable a strong trust environment to be established that can then be built on for large-scale key generation during the lifetime of the device in the field for V2X communications."

b) SCMS RFI Agency Response

The RFI responses and subsequent meetings benefitted NHTSA greatly by providing additional technical perspectives on the SCMS PKI design. For example, DOT had originally dismissed the use of satellites as a viable communications media for transmission of security materials between the SCMS and OBE, but our meeting with Sirius XM Radio brought to NHTSA's attention the fact that, due to advances in technology and the close working relationship between the auto and satellite industries, satellite could in fact be a technologically and economically viable, secure and private media for such security transmissions. Similarly, the PKI technical model put forth by NHTSA in its Readiness Report assumes that a single root must form the basis for trust system-wide. However, as a result of meetings with CSS, NHTSA now is aware of the possibility that, through use of a trust bridge, one or more SCMS organizations, possibly representing different regions or even manufacturers, may be able to co-exist and together, provide more redundancy in security for V2V and V2X DSRC communications.

5. SCMS ANPRM Comments and Agency Response

a) ANPRM SCMS Comments

With limited exception, comments received in response to the ANPRM generally endorsed the PKI design as an appropriate security solution for V2V and V2I DSRC communications. For example, GM, the Alliance, Toyota, and the Automotive Safety Council all concurred that the SCMS design described in the ANPRM and the V2V Readiness Report should provide the required level of security while also protecting the privacy of the end users. Throughout all the comments there were two major concerns with the SCMS design that were cited by multiple commenters: (1) the overall complexity of the design; and (2) a fallback plan for a compromised root.

One of the recurring comments in the ANPRM focused on the overall complexity of the design of the SCMS and the plan for implementing such a system. The design of the SCMS is more complicated than any existing PKI systems due primarily to the need to protect the privacy of the end users both from outsider and insider attacks. As such the various functions in the system are separated logically and organizationally in an attempt to ensure that one organization does not have access to all the information needed to identify the end users. Therefore, this level of complexity is necessitated by the system requirements.

The second technical concern highlighted in the comments is the impact on the system if the private key of the SCMS root certificate authority is compromised. If the root CA is compromised, then this would compromise certificates for all V2V devices, roadside infrastructure devices, and SCMS components. Reissuing the certificates for over 350 million end users would require a significant amount of time and resources to complete. For example, all V2V devices would need to be re-initialized in order to receive a new enrollment certificate; however, this process must occur over a secure communications channel. This may require all devices to return to the dealership or service center in order to have access to the secure communications channel required for the initialization process.

b) ANPRM Agency Response

In response to the first concern, the agency agrees that the level of complexity of the design does increase the risk associated with the implementation and deployment of this system. To combat that risk, one commenter suggested that the system be implemented through a phased development approach where components of the system are developed, tested, and deployed incrementally. This approach would ensure that the deployed components are secure and reliable for additional components are deployed into the system. The agency agrees with this recommendation and is employing in it the development of the SCMS Proof-of-Concept. This system is being developed using an incremental approach that focuses on first implementing and testing the core components of the system, followed by the non-core components. After the system is developed and tested, it will be operated for a significant period of time by DOT. During this operational period, existing V2V and V2I test beds will be integrated with the SCMS POC, and it will provide the necessary security credential materials to these test beds. The

knowledge gained from the operation of the SCMS POC will inform the development of the National SCMS that will be required to support an eventual FMVSS.

The agency also concurs that it would be a catastrophic event for the root CA to be compromised, and as such we are exploring various approaches for disaster recovery that can be implemented to mitigate this risk. The SCMS Proof-of-Concept will implement and test root management and disaster recovery solutions that will allow a root CA to be revoked without requiring the recall and re-initialization of all the V2V and V2I devices in a secure environment. One of the solutions to be tested in the SCMS POC is a distributed root management approach that utilizes root electors to manage the trust relationships in the system. Another solution being evaluated includes the use of redundant root CAs where only a single root is active at any one time. These approaches will be tested and evaluated during the operation of the SCMS POC to ensure that in the event of a compromised root, the system can be recovered without the need to recall every V2V and V2I device.

6. SCMS Industry Governance

a) The SCMS "Industry"

Deployment of an SCMS PKI to secure V2V DSRC communications will require governance of a wide range of complex functions and involve numerous public and private stakeholders, which together we refer to here as the SCMS "industry" or SCMS "ecosystem." We expect that SCMS stakeholders will include: manufacturers of OBE, RSU, and aftermarket safety devices (ASD); certification labs that test OBE (and potentially ASDs); organizations supporting V2V communications; auto manufacturers; standards organizations; PKI experts; State and local government users, and others. In Figure V-6, below, the shapes represent different groups of organizations that interact with the SCMS in some way. Some of these organizations will need to be stood up, while others currently exist today and will likely expand their operations to play a role in the SCMS. The overlapping of shapes represents mutual reliance in executing operations, and the arrows represent communication and the need for inter-organizational arrangements. The SCMS is the focal point of the certificate management industry, as it encompasses the CMEs that oversee all PKI functions responsible for establishing the foundation of security in the V2V/V2I/V2X system.

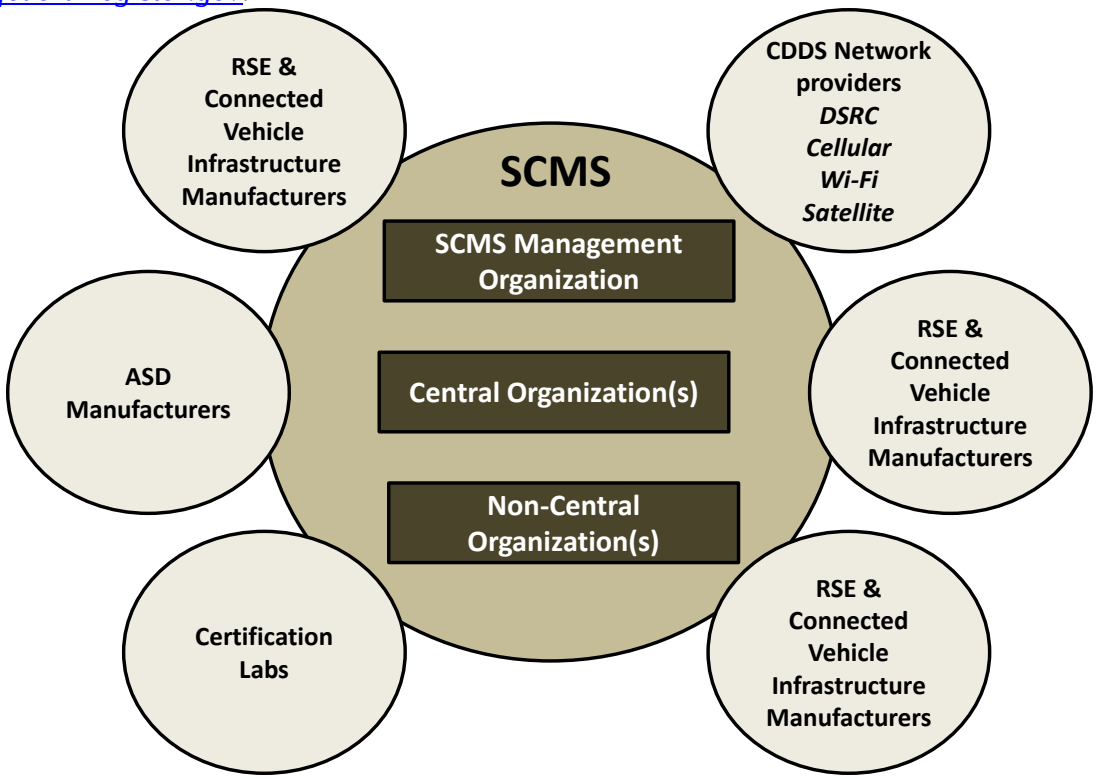

Figure V-6 Certificate Management Industry Diagram

Some of the questions that NHTSA raised in the V2V Readiness Report about industry governance structure for the SCMS include:

- How and by whom are decisions made about various policies, standards, requirements, and practices?
- Who has the authority to mandate and enforce compliance with the policies, standards, and industry requirements?
- Who makes up the overseeing financial, legal, management, and executive operations of the entities in the SCMS?
- Is there a central industry body and, if so, who oversees it? Who is part of this central industry body?
- How do the various entities interact with each other?
- How is risk and liability allocated across the organizations?
- Who will own the intellectual property (data and software) of the system and how will it be licensed (allocated) among responsible entities?

In answering these questions, NHTSA continues to explore a variety of governance models (ranging from public to public-private to private) as potential options for governing the SCMS industry. Due primarily to the absence of Federal funds to support a public SCMS, to date NHTSA has focused primarily on fleshing out a model of private SCMS ownership and

governance that assumes costs will be covered by increases in the purchase price of new vehicles and V2V safety devices. As we noted our V2V Readiness Report, in a private SCMS industry the organizational structure and operation of the SCMS would be determined largely by private owners and operators of CME components, under oversight of an SCMS Manager (ideally an industry-wide coalition of CME owners and other stakeholder representatives who, together, agree on the terms of self-governance and system-wide rules and policies). The SCMS Manager would provide critical system management by enforcing and auditing compliance with uniform technical and policy standards and guidance system-wide. Uniform standards and guidance would establish and ensure consistency, effectiveness, interoperability, sustainability, and appropriate privacy protections across the CMEs to facilitate necessary communications, sharing of information, and operational connections, and would be based in large part on existing technical and policy standards applicable to PKI systems.

The Readiness Report explained NHTSA's view that, in the context of a privately owned SCMS "industry," a private model could be a viable mechanism for SCMS governance in which NHTSA would have only a minimal role in ensuring system integrity, largely through its traditional regulatory activities. We also indicated that NHTSA's existing legal authority would accommodate the use of grants, cooperative agreements, or other agreements to facilitate stakeholder -- and even DOT – input into governance of a private SCMS.

b) ANPRM Governance Comments

Comments to the ANPRM and Readiness Report relating to SCMS ownership and governance came mostly from members of the automotive industry and their trade groups. While agreeing with NHTSA's assertion that a V2V system is not complete without a robust SCMS, almost without exception, industry commenters vehemently disagreed that a private self-governing industry coalition could be a viable mechanism for SCMS system governance. Commenters believed that a private SCMS could not provide the security, privacy, certainty, stability, long-term functionality, or management of costs and risk required for a nationwide SCMS to support V2V DSRC communications, and lacked the legal authority to address cross-border issues or require industry-wide participation and compliance with uniform requirements. For these reasons, virtually all industry commenters took the position that a strong leadership role for the Federal government in the SCMS would be required for successful deployment of V2V and V2X DSRC communications.

For example, both the Alliance and Mercedes described the SCMS as a "core government responsibility." Noting that "for V2V to work effectively, every vehicle manufacturer will have to participate in the SCMS and abide by its rules," the Alliance explained that:

> a private organization, such as a voluntary coalition of manufacturers, cannot compel unwilling manufacturers to join the organization, and cannot enforce deviations from the organization's rules except by expelling misbehaving members. There is no effective mechanism to ensure the universal participation of all manufacturers and to compel their obedience to the necessary common SCMS requirements…

The Alliance also stated that "resolution of policy issues requires coordination among multiple federal agencies (FHWA, FTC, FCC, EPA)," and that "Congress was best positioned to provide the needed coordination and nationwide-scope for addressing infrastructure, governance of networks and SCMS, consumer privacy, sustainable funding, international cross-border and liability/IP policy issues."

Global commented that "private sector options for operating the Security Credential Management System (SCMS) do not guarantee certainty over the management or the cost of operation the system and its long-term stability." GM, likening the issuance of security certificates to the minting of coinage by the Federal government, argued that ensuring a secure V2V system would require that the Federal government: (i) operate or support operation of a central root CA that all V2V certificates must use, or mandate that all V2V certificates use a central root CA; and (ii) review and approve minimum levels of security for the keys and cryptography used by the root CA and subordinate CAs authorized by the root CA. Mercedes described the SCMS as a "backbone infrastructure, which must be set up and controlled with the leadership of state and federal authorities" and echoed the comments of the Alliance that only Federal government oversight would ensure industry-wide participation in an SCMS and compliance with its requirements. Similarly, Honda commented that the federal government should be responsible to ensure the safe and efficient operation of the V2V security framework, and should consider a public-private partnership as an option for the operation and management of the SCMS, with federal oversight, supervision and funding.

The agency agrees with commenters that, for a variety of policy reasons, ideally the Federal government should play a more central leadership role in the establishment and governance of a V2V SCMS. For this reason, as detailed above, DOT now has taken the lead in working with SCMS stakeholders to develop the policies and standards that should form the basis for governance of a National V2V SCMS, as well as to model and prototype organizational options for a governance entity to manage SCMS operations.

c) A Comparative Industry Example: ICANN

In analyzing SCMS governance options, NHTSA and its research partners have investigated a variety of industries with characteristics similar to those seen as critical for a V2V SCMS governance model, including security, privacy protection, stability, sustainability, multi-stakeholder representation and technical complexity.[227] We investigated an array of public, public-private and private governance models, with particular emphasis on safety-critical and privacy-sensitive systems. We also examined how risk was managed in the context these models. Some of the industries researched included:

---

[227] VIIC Assessment of Key Governance Policy Considerations for a Connected Vehicle Cooperative Safety Communications System," dated March 12, 2013, at page 11 http://www.regulations.gov/#!documentDetail;D=NHTSA-2014-0022-0046 (last accessed Dec. 8, 2016)

- Internet Corporation for Assigned Names and Numbers (ICANN)
- DTE Energy Company
- Aeronautical Radio Incorporated (ARINC)
- End of Life Vehicle Solutions Corporation (ELVS)
- The FAA's Next Gen Air Transportation System
- The FRA's Positive Train Control
- Smart Grid
- The Rail/Transit Train Control Systems (ATC and CBTC)
- FMCSA's EOBR
- Coast Guard's MSSIS
- Army Corp of Engineer's MRGO
- Medical Devices failure and liability
- Security in nuclear industry and liability
- Warning / Signal Failures
- UAVs
- HIPAA / Health Care industry / Electronic Health Records (EHRs) / CONNECT system
- Credit Card Payment industry and PCI standards
- Hospital/Health care industry

Of the governance models we examined, governance of the internet naming protocol systems (DNS) by the Internet Assigned Numbers Authority (ICANN) possessed numerous characteristics that seem to translate most directly to a private or public-private governance model for the V2V SCMS. ICANN is a private, not-for-profit corporation created by private sector entities in direct response to efforts by the Federal government to privatize certain Internet-related tasks in a manner that permits robust competition and international participation in its management. ICANN is managed by a multi-stakeholder Board of Directors (representative of the functional and geographic diversity of the Internet) that oversees a number of Internet-related functions previously performed directly on behalf of the Federal government by other organizations, notably the Internet Assigned Numbers Authority (IANA) (formerly located within the Department of Commerce but now operated by ICANN). Pursuant to various Memoranda of Understanding with ICANN (ICANN MOUs), the Department of Commerce agreed gradually to transfer to ICANN certain Internet-related functions, with the goal of having ICANN carry out operational responsibility for these functions in a financially self-sustaining manner after a limited transition period. At the same time, the Department of Commerce also entered into a series of funded project agreements with ICANN, on a sole source basis, to

perform technical and policy activities required to facilitate the transition of authority for those functions to ICANN.[228]

The ICANN MOUs and project agreements called for the Federal government to exercise significant oversight of ICANN's activities until such time as ICANN was stable and could provide certain stability, sustainability and policy assurances to the Federal government. After 11 years, the Department of Commerce gave up its oversight of ICANN with respect to the operation and governance of specific Internet naming protocol functions, but committed to ongoing participation in ICANN's Governmental Advisory Committee (GAC). ICANN continues to perform certain technical maintenance tasks under contract to Commerce, as do other Commerce contractors. In 2014, Commerce announced its intention to work with ICANN to privatize key Internet domain name functions still remaining under its control.

How is ICANN relevant to governance of the V2V SCMS? ICANN provides NHTSA with a potential road map for how it can work with public and private stakeholders to develop a successful governance structure for a multi-stakeholder, geographically and functionally diverse technology-intense system not unlike V2V. Like the V2V SCMS, successful deployment of an Internet naming protocol required uniform and consistent application of technical and policy standards enabling interoperability and system-wide confidence. As would be required for enforcement in a privately governed SCMS, ICANN uses a binding Registry Agreement as the enforcement mechanism through which it ensures that its policy and technical standards are applied Internet-wide. Like the SCMS ecosystem or "industry," the Internet "industry" involves numerous commercial, academic, geopolitical, and other private and public stakeholders involved in a broad range of Internet-related functions, the success of which requires system-wide, coordinated governance. As would be likely in the SCMS context, ICANN was developed and operates on a foundation of the fundamental principles of security, stability, resiliency, multi-stakeholder participation, openness, fairness and robust completion. Additionally, as detailed in the ICANN MOUs, after a period of direct government oversight and funding, the privatized functions governed and coordinated by ICANN were designed to be financially self-sufficient (i.e. financed by fees paid for services).

We agree with Dura and the VIIC that ICANN's organizational structure could translate well to a potential V2V SCMS governance model. The details of ICANN's mission, core values, powers, responsibilities, governing principles and procedures are set forth in its Articles of Incorporation, Bylaws, Charter, and other publicly available documents. In accordance with those documents, ICANN is governed by the binding decisions of a Board of Directors, consisting of both voting Directors and non-voting liaisons. The voting Directors consist of members selected by a functionally and regionally diverse nominating committee that reflects the diversity of Internet ecosystem, as a whole: the Address-Supporting Organization (ASO), the

[228] ICANN background information, contract and agreement content can be found at http://www.ntia.doc.gov/page/docicann-agreements (last accessed Dec 8, 2016)

Country-Code Names Supporting Organization (CCNSO), the Generic Names Supporting Organization (GNSO), the At-Large Community and the President ex officio. Directors may not be officials of countries or multinational geo-political entities. Only ICANN's President can be both a Director and ICANN employee. Non-voting liaisons are a means for the Board to obtain input from world-wide governments, through the Government Advisory Committee (GAC), and three function-specific expert committees, the Internet Engineering Task force (ETF), Security and Stability Advisory Committee (SSAC) and Root Server System Advisory Committee (RSSAC). The organization has an Ombudsman appointed by the Board to act as a neutral dispute resolution practitioner and provide an independent internal evaluation of complaints by members of the ICANN community who believe that the ICANN staff, Board or an ICANN constituent body has treated them unfairly.

NHTSA also found quite instructive the procedures used by the Department of Commerce to effectuate the process of successfully privatizing certain Internet-related functions. In July 1997, the Department of Commerce first published a Request for Comments on behalf of an interagency working group examining the appropriate future role of the Federal government in the DNS and other issues related to the administration of the DNS. The following year, in early 1998, based on the 1400 pages of comments it received to its Request for Comments, it issued a rulemaking notice proposing certain actions designed to privatize the management of Internet names and addresses in a manner that allowed for the development of robust competition and facilitates global participation in Internet management.[229] The proposed rulemaking addressed a variety of issues relating to DNS management including private sector creation of a new not-for-profit corporation (the "new corporation") managed by a globally and functionally representative Board of Directors. The rulemaking proposed, among other things, the new corporation's authorities, detailed the role of the federal government in policy oversight during the transition, identified funding, and contained a detailed proposed governance structure (specific to the number of seats on the Board of Directors) with substantive stakeholder participation and openness requirements. The rulemaking explained that, the new corporation would:

> "Act much like a standard-setting body. To the extent that the new corporation operates in an open and pro-competitive manner, its actions will withstand antitrust scrutiny. Its standards should be reasonably based on, and no broader than necessary to promote its legitimate coordinating objectives. Under U.S. law, a standard-setting body can face antitrust liability if it is dominated by an economically interested entity, or if standards are set in secret by a few leading competitors. But appropriate processes and structure will minimize the possibility that the body's actions will be, or will appear to a court to be, anti-competitive."[230]

---

[229] http://www.gpo.gov/fdsys/pkg/FR-1998-02-20/html/98-4200.htm (last accessed Dec 8, 2016)
[230] http://www.ntia.doc.gov/files/ntia/publications/022098fedreg.txt, at page 8818 (last accessed Dec 8, 2016)

Later the same year, in July 1998, the Department of Commerce opted to proceed with privatizing management of the internet DNS not through rulemaking but by issuing a Statement of Policy expressing the Government's intent to "recognize, by entering into agreement with, and to seek international support for, a new, not-for-profit corporation formed by private sector Internet stakeholders to administer policy for the Internet name and address system."[231] In a July 7, 2000 report,[232] the GAO confirmed the appropriateness of the Department of Commerce's actions. The GAO determined, among other things, that:

- Department of Commerce had the authority to support privatization of the DNS on the basis of its general authority[233] to foster, promote, and develop foreign and domestic commerce and NTIA's more specific authority to coordinate the telecommunications activities of the executive branch;[234]

- The APA notice and comment requirements did not apply to the Department of Commerce's general statement of policy, as it contained not substantive regulatory requirements but a general framework for privatizing the DNS;

- Establishment of ICANN by the private sector was not subject to the Government Corporation Control Act or various other legal requirements applicable to entities that are part of or controlled by the Federal Government;

- Department of Commerce had authority to enter into the MOUs, cooperative agreements and sole source contracts with ICANN based on its general legal authority to work with and enter into these types of agreements with non-profit entities.

It must be noted that the circumstances that led to creation of ICANN are different, in significant respects, than those that now necessitate the creation of an SCMS to support V2V DSRC communications. When it issued its Policy Statement, Department of Commerce had funds dedicated to administration of the DNS it sought to privatize and already had taken on responsibility for performing that function, in accordance with Federal law. For this reason, the Department of Commerce had a legal obligation closely to oversee ICANN's assumption of responsibility for the DNS during a transition period. It also continued to fund ICANN in the performance of certain additional functions previously performed by IANA, even after it ceased to oversee ICANN's policies and operation of the DNS in 2009. By contrast, to date, NHTSA has not assumed responsibility for carrying out any security functions relative to mandated

---

[231] See https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses (last accessed Dec 8, 2016)
[232] See Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers, July 7, 2000 (B-284206) http://www.gao.gov/new.items/og00033r.pdf (last accessed Dec 8, 2016)
[233] In so doing, GAO noted that "there is no explicit legislation requiring the government to exercise oversight over the domain name system." Id at 3.
[234] 47 U.S.C. 902(b)(2)(H).

automobile equipment, so no infrastructure or funding for this purpose now exists. Additionally, NHTSA seeks not to privatize existing federal security functions or infrastructure, but to work closely with public and private V2V stakeholders to take the technical design, intellectual property and body of policy developed through DOT's SCMS research and facilitate the creation of a new operational entity – a National SCMS to support V2V, V2I, and V2X DSRC communications.

Despite these differences, NHTSA believes that ICANN serves as a strong comparative industry model of how NHTSA can work with stakeholders in the SCMS ecosystem to facilitate creation and support of a multi-stakeholder private sector entity to govern and coordinate operation of the V2V SCMS.

d) Potential SCMS Implementation Model

It is clear that there are numerous different paths that government and private stakeholders theoretically could follow in implementing a National SCMS to support the V2V ecosystem – paths the organization, governance and financial viability of which DOT expects its expanded policy research to develop and assess. There may even be other viable security models that could provide sufficient confidence and consumer privacy protection to V2V messages. However, if NHTSA mandates V2V communications equipment in light motor vehicles and moves forward with implementing the SCMS technical design described above, the agency believes that one promising path was that pursued by Department of Commerce when it spurred private sector establishment of ICANN. Specifically, DOT could facilitate the creation of a multi-stakeholder entity capable of governing and coordinating operation of a National SCMS. DOT's expanded policy research, including stakeholder input, modeling, and prototyping of potential governance models, as well as comments on the NPRM, will help determine whether such an SCMS should be a purely private entity in which DOT plays an advisory role -- or whether the Federal government should assume control over some critical SCMS functions (for example, ownership of the definitive root).

The process followed by the Department of Commerce as it privatized certain DNS functions could be a useful roadmap for how NHTSA might work with the private sector to establish a new, multi-stakeholder entity to take on governance and coordinate operation of a V2V SCMS. NHTSA's 2014 ANPRM, V2V Readiness Report and SCMS RFI could be viewed as the first steps in this process. NHTSA used the input the agency received in response to these public documents, in meetings with RFI respondents, and through SCMS policy research performed by the VIIC and others, to expand the scope its planned SCMS governance and policy research discussed in Section V.B.6. This critical SCMS policy research is intended to give DOT a central role in, and direct control over, development of draft policies, procedures and standards that could the basis for governance of a National SCMS, including draft a Certificate Policy, Certificate Practice Statement, Registration Agreements, and Privacy Policy. Another central aspect of DOT's planned SCMS policy research will be working with PKI and organizational consultants and stakeholders to prototype a multi-stakeholder governance structure (much like ICANN's Board of Directors) capable of satisfying the needs of the broad

range of diverse participants in the SCMS ecosystem. If successful, this prototype could serve as a model for a private sector entity that could establish and oversee a deployed National SCMS.

If appropriate based on the Department's planned research, DOT then could issue a draft V2V SCMC Policy Statement describing a process (similar to that followed by DOC and ICANN) by which the Department could, if it chooses to, work collaboratively with a new multi-stakeholder private entity to develop the binding policies and technical standards required for stable and sustained operation of a V2V SCMS. After an initial period of joint policy development and direct DOT oversight under contract, prior to full SCMS deployment, DOT gradually could terminate some or all its oversight of the new entity's activities, completing the transition of authority prior to full SCMS deployment. Thereafter, representatives of NHTSA and other Federal government agencies, both within DOT (DOT-R, FHWA, FMCSA, and the others) and elsewhere in the Federal Government (FCC, FTC), could serve in an advisory capacity on a Government Advisory Committee or as nonvoting SCMS Manager Board Members.

e) SCMS Proof-of-Concept Operational Model Development Plan

As a result of a better understanding obtained from operating the prototype security system during Model Deployment, as well as feedback from the SCMS Request for Information, ITS-JPO and NHTSA realized that expanding to a National level SCMS would require an intermediate step. Specifically, that additional research was required to prove the concept and develop a SCMS working model that allows for investigating the full range of technical, policy, and organizational elements involved in deploying and operating the SCMS. Investigating these components includes providing security certificate management services to continuing vehicle communications research activities and early deployments.

As part of developing a working SCMS model, DOT will:

- Develop and implement a proof of concept SCMS (the SCMS PoC) that is fully representative of the Final SCMS design, and which will provide certificate management services to early deployments and demonstrations, including but not limited to CV pilots,

- Act as the overall SCMS PoC Manager, including developing policy and procedures that will govern the interactions between the various entities involved in the V2X eco-system, and

- Based on stakeholder input, will advanced and adapt SCMS PoC policies and protocols such that they would represent possible policies and protocols suitable for the establishment and operations of a SCMS that could support a national deployment of vehicle communication technology.

The SCMS proof-of-concept (PoC) will be fully representative of a production SCMS in terms of functionality, features, and capabilities. It will support all certificate management "use-cases" envisioned for a production system, and incorporates all elements of the final design developed by DOT and its industry partners. While not intended to be "full-scale", the SCMS

PoC will be capable of servicing up to 17 million vehicles annually. The SCMS PoC is being developed to:

1. Support end-to-end testing of the certificate management use-cases thus demonstrating feasibility and practicality of system;

2. Demonstrate the extensibility of the SCMS design (multiple non-central components);

3. Support scalability testing through modeling, simulation, and real-world deployments;

4. Support integrity, robustness and system vulnerability testing;

5. Will be used in actual connected vehicle operations by servicing a variety of early deployments and demonstrations including the Connected Vehicle pilots (Tampa, NYC, Wyoming), the Smart City Challenge program recipient, as well as other government sponsored (state & local) and private sector deployments that we anticipate emerging over the next several years; and

6. Will be able to support future connected vehicle application demonstrations programs for FMCSA, FTA, and FRA (e.g., wireless roadside inspections; electronic credentialing; grade-crossing safety; transit-pedestrian safety; and other applications).

NHTSA and its industry partners (CAMP) are currently in the process of prototyping an SCMS system that is capable of executing all the core use-cases associated with the security certificate management life cycle including enrollment, certificate generation, certificate request and fulfillment, and revocation. This proof-of-concept SCMS (the SCMS PoC) is being developed to support real-world operations of early V2V deployments at connected vehicles pilots sponsored by DOT (in Florida, New York City, and Wyoming and elsewhere). NHTSA and its industry partners will continue to refine, test and mature the design of the SCMS—including addressing the functions and features listed above—by leveraging this prototype environment. To support these refinement efforts, we are establishing multiple instantiations of the SCMS including Production, Quality Assurance and Development environments. Further, we are in the process of retaining an additional (in addition to MITRE) independent cyber-security testing and evaluation Team to conduct a thorough design review on the Final SCMS design, and to complete focused penetration testing and vulnerability discovery on the actual SCMS prototype by leveraging the Development environment platform.

DOT will develop, operate, and manage the SCMS PoC through multiple contract/agreements with multiple entities, illustrated via Figure 1. Figure 1 identifies five research activities including the SCMS PoC Governmental Management that represent the SCMS PoC Manager Environment. This environment depicts the boundaries of the SCMS PoC Governmental Management activities. DOT has already established an agreement that is currently developing an initial prototype of the SCMS PoC that will be the basis for the operational environment and support ongoing functional (refinement) development. SCMS PoC Governmental Management includes the development of policies that support the technical

processes and procedures and the organizational protocols that establish interfaces (communications) between entities that support policy and operational execution. DOT, with the support provided by the Governmental Management contractor, will be the SCMS Manager and set policies and protocols that will address threats in relation to access and change authority. The SCMS Manager will develop and establish a Certificate Policy and Certificate Practice Statement that sets the policies and protocols that must be accepted and followed to be approved to participate in the SCMS environment.

A separate agreement will establish the operational SCMS PoC (provides the technical functions that enables generation, distribution and monitoring of SCMS security materials). Related to the separate agreement that establishes PoC operations is an agreement that provides for the technical management that encompasses the development and documentation of technical process and procedures end entities will use to initialize devices and obtain security materials. Another contract will provide Connected Vehicle Support Service that supports the initial interactions regarding end entity applications for device initiations, technical support questions, and questions about policies and procedures. The Connected Vehicle Support contractor will establish and operate the initial interface with end users.

Beyond the SCMS PoC manager environment, the SCMS PoC Governmental Manager will in most cases indirectly interface with other research activities such as the CV Pilots, and other support entities that include Certification Service entities, and Device Suppliers. The most direct outside relationship will be with the National SCMS Prototype Policy Development research. The SCMS Governmental Management effort will need to interface with the National SCMS Prototype Policy Development research to support national level SCMS prototype policy development.

The SCMS PoC environment, together with the connected vehicle pilot sites sponsored by DOT, will provide an opportunity to refine the SCMS Manager concept and other non-technology related policies and procedures needed to address security threats.

f) SCMS Request for Comment

NHTSA has invested considerable resources and effort in refining and maturing the Security Credential Management System Design. The Agency has enlisted the assistance of leading PKI experts in developing the design[235], and the design has been formerly reviewed by MITRE Corporation[236] (see Section V.B.3 for summary of MITRE review) and other Federal Agencies including DARPA and NIST have also reviewed the design. NHTSA believes that the SCMS concept and design offers a practical, efficient and effective means for addressing the

[235] Will list all key entities who have assisted CAMP including Escrypt, Trust Point, Security Innovations, Booz Allen and others
[236] List reference to MITRE reports

need for confidence in V2V and V2I communications—while simultaneously addressing privacy concerns arising from potential vehicle tracking using V2V communications. Nevertheless, a fully representative prototype of the SCMS system has not yet been developed and tested, although NHTSA and the JPO are in the process of doing just that, (see Section V.B.6.e) for details).

In addition, the SCMS concept calls for periodic (or routine) communications between the vehicle and various certificate management entities (which reside in the "infrastructure" on the internet) to execute a variety of certificate management life-cycle services including: re-provisioning of on-board pseudonym certificates; distribution of certificate revocation lists; and potential a component for sending misbehavior detection reports from vehicles to the Misbehavior Authority of the SCMS as described in the Proposal . While NHTSA believes that such periodic vehicle to infrastructure communications can readily be accommodated thru either V2V DSRC communications (using roadside units, or RSUs), or through the rapidly increasing connectivity of vehicles using commercial wireless services (cellular or satellite services that are either integrated into vehicle or made available through links with an operator's cell phone), NHTSA nevertheless recognizes that security certificate management concepts that inherently minimize the need for such periodic V2I communications may offer advantages relative to maintaining proper on-board certificate credentials.

To manage the normal risk associated with any new and complex information security system, and to address a means for potentially reducing the need for V2I security communications, NHTSA has been, and continues to investigate alternatives to the SCMS concept.

NHTSA seeks comments on all aspects of the SCMS In technical design, development, and potential deployment, including DOT's proposal to expand its governance role in development of a viable organizational model and policies and procedures applicable to a National SCMS, and the use of ICANN as a possible roadmap for how to facilitate establishment of a private, multi-stakeholder entity to manage and oversee operation of the National SCMS.

C. Vehicle Based Security System (VBSS)

In late 2012 NHTSA began investigating a certificate management concept termed the "vehicle based security system" (VBSS). VBSS is based on principals associated with Group Manager concepts for managing cryptographic materials—and adapted for vehicular application by NHTSA engineers.

The major difference between SCMS and VBSS is in generating short-term certificates. The SCMS approach relies on individual vehicles to periodically request pseudonym certificates from infrastructure-based entities, (most notably a Pseudonym Certificate Authority, or PCA) which in turn generates and signs short-term certificates. Vehicles then download batches of certificates which are used to digitally sign BSM messages. In contrast, the VBSS concept calls for delegating this authority to individual vehicles, and as a result the communications with the infrastructure are reduced.

DOT funded a Feasibility Study of the VBSS concept in 2014 (completed by Oakridge National Laboratory, ORNL) and the first phase of study was completed in December, 2015[237]. Figure X depicts a high level comparison of the VBSS and SCMS architectures.

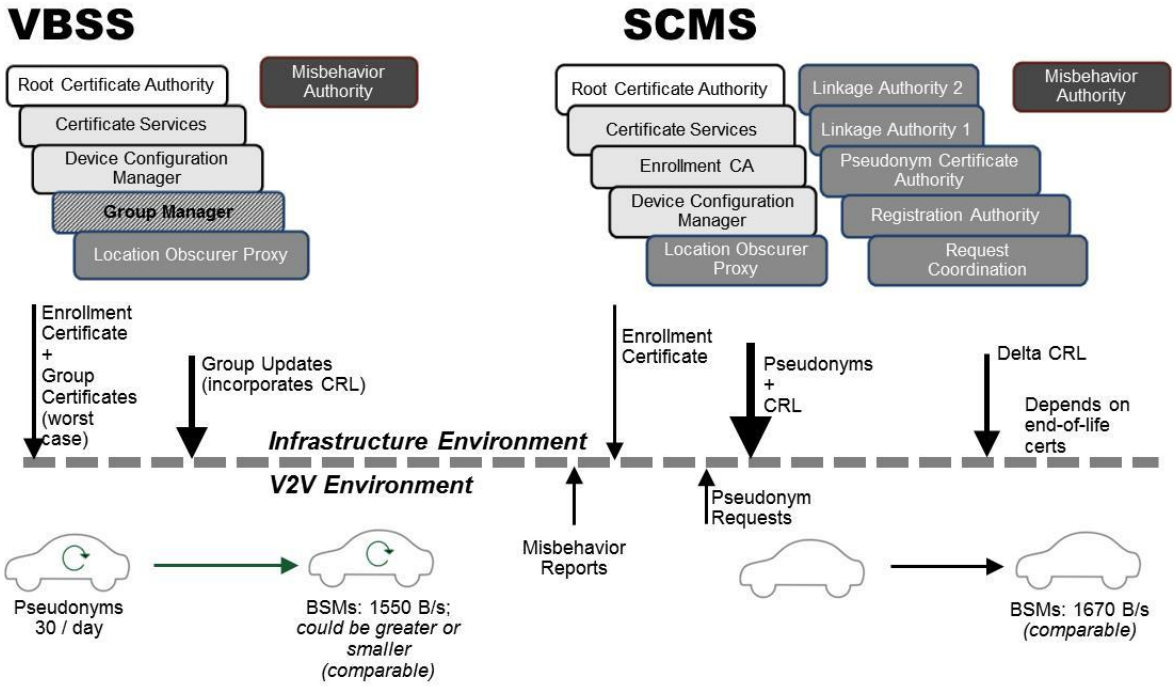

Figure V-7 VBSS versus SCMS High Level Architecture

Under the VBSS concept, the Pseudonym Certificate Authority (PCA), Registration Authority (RA), Linkage Authorities (LAs) and Request Coordination, that are fundamental components in SCMS, are eliminated. VBSS establishes a Group Manager/Group Managers (GM) to provide credentials that make it possible for each vehicle to act as a certificate authority – an entity that can generate short-term certificates.

Each vehicle is a member of a group and is assigned a unique membership secret, a signing key. All member signing keys for a particular group are associated with a single group certificate. A vehicle generates its own ephemeral pseudonym certificates by signing the public key from a self-generated key pair with its group signing key; vehicles act as subordinate Certificate Authorities and pseudonyms are generated on demand based on travel requirements. Pseudonym verifiers use the group certificate to authenticate the pseudonym certificate, and then the pseudonym certificate to verify safety messages. The pseudonym generator remains anonymous, since the receiver uses a single group certificate to authenticate signatures made by

[237] "Vehicle Based Safety Systems: A Feasibility Study: December 23, 2015, ORNL

all members from a particular group. Groups are managed by one or more infrastructure-based authorities. Members may be removed from groups by distributing information that allows participants to update their group credentials; this provides a means to revoke misbehaving vehicles since the pseudonyms they create will no longer be authenticated by vehicles that have updated their group credentials.

Use of pseudonyms (short-lived identifiers) and separation of distributed identifiers are the primary means of achieving an acceptable level of privacy. Within a VBSS, how groups are designed will also affect the preservation of individual privacy. As the number of distinct groups increases within a geographical area, privacy protection decreases; if every vehicle within a geographic area were in its own group (the extreme case); the group identifier becomes a unique vehicle identifier. This situation can be mitigated by ensuring group diversity is minimized regionally.

Misbehavior detection and reporting, and revocation are maintenance operations that are common to both SCMS and VBSS. There are misbehavior reporting alternatives discussed in SCMS security section of this proposal. In relation to misbehavior and revocation, VBSS may offer some advantages relative to managing communications associated with revoked vehicles. With SCMS, as the number of revoked vehicles grows—including those vehicles revoked because they are at the end of their useful life, the CRL list must also grow. NHTSA and its industry partners are investigating mechanisms for managing the size the CRL but nevertheless remains a challenge. With VBSS, instead of sending out CRLs to revoke vehicles, a Group Broadcast (GB) distributes group credential updates to participating vehicles; this occurs when a sufficient number of vehicle misbehavior reports have been validated resulting in one or more revocations; otherwise, group credentials do not change. With comparison to the SCMS using CRL list to remove compromised devices from the V2V communication system, the size of CRL will increase with the number of compromised devices, VBSS revocation mechanism's advantage is that the size of group credential updates will not increase with the number of compromised devices.

The Phase I study of VBSS and comparisons with other approaches suggests VBSS is feasible because group-based credentials provide a means to delegate infrastructure-based operations to vehicles in an effective way while facilitating the basic requirements of authentication, privacy, and maintenance of confidence. However, while Group-based signature schemes are an active area of research they are evolving and much less mature than other cryptographic systems. For this reason, VBSS remains in its preliminary stages.

NHTSA is continuing its research of the VBSS concept and is beginning a Phase II research Study in 2016. This work will focus on modeling a Group Manager and enhancing our understanding of the Group Manager software engineering requirements. NHTSA seeks comment on the viability of the VBSS certificate management approach including potential advantages and disadvantages relative to the SCMS approach. Specifically, we seek comment on the following:

- Could requirements to update an entire group's credentials (to enable revocation of selected vehicles) actually increase V2I communications during early deployment (versus distribution of a CRL)?
- Are there CRL distribution schemes that could limit, or otherwise manage, the growth of the CRL—particular as vehicles reach the end of their life and are place on the CRL?
- How will requirement to self-generate short-term certificates onboard the vehicle impact processing and memory requirements onboard the vehicle—as well as the need to provide high integrity hardware security modules to support such operations?

D. Multiple Root Authority Credential Management

U.S. DOT research, performed in partnership with European, Australian, and Japanese partners, has recognized that the world will evolve into a multi-root world and that crypto-agility will be a required capability as a response to increasing cybersecurity attacks.[238]

While these capabilities are not required at the initiation of a connected, cooperative environment, they are useful technical and policy constructs to incorporate as the threat profile shifts and as the operational environment grows.

There are three potential paths to consider, all with advantages and disadvantages (we further note that these paths are not exclusive and that as the technologies evolve, they may converge):

(1) There is the path of establishing a single chain to the Root Authority that allows for devices/equipment or operational entities to become enrolled and implicitly trusted by the system. In such a system:
   a. The Root Authority requires a significant level of security to ensure that it is not comprised.
   b. The root authority can authorize intermediate certificate authorities which can support a diversity of operational parameters. However, all intermediate certificate authorities under a single root authority must operate with the allowable policies of the root authority.
   c. There is a requirement for a mechanism to manage root authorities which is capable of transitioning the fundamental cryptographic elements if the Root Authority is compromised. This mechanism must be similarly as highly secured as the root authority and has the ability to revoke the compromised root and add a new root in a

[238] This work and its outcomes are described at: https://ec.europa.eu/digital-single-market/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international.

controlled and efficient way for all participants in the security system.[239] While allowing for some diversity of operational usage within the policies of the root, there is a minimum of interfaces between the root and other nodes, consequently, the threat surface remains smaller.

d. The mechanism for managing the root, although requiring (and incurring costs for) a high level of security, allows for orderly migration of the security system to incorporate root replacements and cryptographic improvements (as long as the devices within the system are capable of adopting such new cryptographic processes), thus future-proofing the overall system to the extent possible within known parameters.

This is the path that the US is taking to establish initial operations to support emerging connected vehicle environments.

(2) There is the path of establishing multiple, co-existing roots in which each Root Authority must have an agreement with other root authorities that describe an appropriate level of trust. Based on the trust level, a host of interfaces have to be enacted for data transfer that assures one operational root that the other operational root remains trusted. See the report titled, ***Cooperative-ITS Credential Management System Functional Analysis and Recommendations for Harmonization Document HTG6-4 Version: 2015-09***[240] for greater details on the trust levels and how to enact the trust levels from both a policy perspective as well as a data flow perspective.

A benefit to this path is that with multiple operational roots, if one is compromised, another root could potentially take over operations (although this is highly dependent upon the trust levels—if the other operating root that has to take over does not trust the credentials of the compromised root (even if the credentials in use are still valid and not compromised), then all actors enrolled in the compromised root will have to cease operations of the cooperative applications until they can be proven to be trusted actors and enrolled in the uncompromised root authority).

Understanding the different trust levels is the key to understanding whether there are benefits to a multiple root world. A key conclusion to the analysis on how to enact different trust levels is that adding even one additional root to the system increases the number of interfaces among entities which exponentially increases the attack surface of the inter-related systems. This model also increases costs of running different organizations, increases the costs associated with data analysis, and increases the costs of auditing and updating policies. In addition, it seems that agreement of common security policies under the initialization of

---

[239] See Root Elector System Design at http://www.mycreativeregistry.net/IPCOM/000245336 (last accessed Dec 4, 2016)

[240] http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=11398

parallel operational roots, operated by different organizations with different priorities, is likely to be very difficult, adversely affecting the level of trust that may be established among various root authorities.

Furthermore the Government will have no authority to compel one Root Authority to interface with another Root Authority. This would adversely affect interoperability given the equipment under the different roots would not interact in crash avoidance situations reducing the effectiveness of V2V. For example a group of OEMs could be covered under one Root Authority were as a group of aftermarket suppliers could be covered under a different Root Authority. If the OEM group decides that the aftermarket devices do not meet the OEM level of performance then no agreement would be implemented and equipment in the OEM group would not interact with equipment in the aftermarket group. This could create market disparity and reduce consumer choice.

(3) There is one additional path that is very similar to path #2, but also incorporates the use of different types of security credentials (or security certificates). The use of the NIST elliptical curve SHA-256 offers a significant advantage over other types of credentials in that it includes the lowest amount of overhead for an appropriate level of trust and authentication among vehicle moving at very high speeds.

This version of the model would allow for different credentials (such as "brainpool" or other curves) to also be used in operations. This version of the model significantly increases the complexity of the system. While it offers greater crypto-flexibility, having the ability to recognize and use different credentials will require that ALL equipment/devices/applications will have to be able to recognize and trust messages created with either type of credential in order to ensure continued interoperability. This path may increase the cost and complexity of equipment on the vehicle and/or change the nature of the equipment, as the receivers will have to recognize the different cryptographic technologies and perform additional/different validity checks for the different cryptographic technologies. Also, this capability/path is not yet proven and would need to be demonstrated under a number of conditions to ensure that the transactions and timing can still meet the safety applications requirements for latency of the exchange and scalability of the dedicated spectrum available for low-latency communications, such as the V2V Basic Safety Message.

This is the path that is under consideration within the European Union at this time.

All of these paths are, in some sense, multi-root in that it is necessary to have at least a back-up root as part of an internal system. The analysis of the different paths highlights some of the key issues that will need to be addressed as the future evolves:

- Security credentials: At some point, we can expect that the security credentials based upon the current cryptographic level will be broken due to quantum computing and that new security approaches and/or new cryptographic curves will be needed. Research is needed into new curves to ensure that new security approaches do not significantly increase the

communications overhead in order support the latency requirements for V2V communications.

- Governance/Certificate Policies: New root management and recovery solutions will need to be developed as the initial, smaller connected vehicle environments evolve into more complicated, region-wide, overlapping environments that may operate at different levels of security. This has been addressed in the first path through the innovative creation of Root Electors that provide the ability to revoke a compromise Root and establish a new Root without having to re-initialize devices.[241]

VI. What is the agency's legal authority to regulate V2V devices, and how is this proposal consistent with that authority?

A. What can NHTSA regulate under the Vehicle Safety Act?

NHTSA has broad statutory authority to regulate motor vehicles and items of motor vehicle equipment under the National Traffic and Motor Vehicle Safety Act (the "Safety Act").[242] As applied in this context, the agency's authority includes all or nearly all aspects of a V2V system. Congress enacted the Safety Act in 1966 with the purpose of reducing motor vehicle crashes and deaths and injuries that occur as a result of motor vehicle crashes and non-operational safety hazards attributable to motor vehicles.[243] The Safety Act, as amended, is now codified at 49 U.S.C. §§ 30101 et seq.

The vehicle technologies that enable vehicles to send messages to and receive messages from each other are vastly different from those that existed when the Safety Act was enacted. Then, the vehicle operating systems were largely mechanical and controlled by the driver via mechanical inputs and linkages. Components and systems were either designed into the vehicle at the time of original manufacture or were later attached to or physically carried into the vehicle. Sensing of a vehicle's performance and the roadway environment was done solely by the driver.

---

[241] See Root Elector System Design at http://www.mycreativeregistry.net/IPCOM/000245336 (last accessed Dec 4, 2016)

[242] For more discussion and analysis of NHTSA's authority to regulate advanced crash avoidance technologies, including V2V technologies, under the Safety Act, see the Potential Regulatory Challenges of Increasingly Autonomous Vehicles, 52 Santa Clara L. Rev. 1423 (Wood et al., 2012) at http://digitalcommons.law.scu.edu/lawreview/vol52/iss4/9/ (last accessed Dec. 6, 2016).
For example, the agency's authority to address the privacy and security of vehicle data associated with the operation of those technologies is discussed at length. Id., at pp. 1448, 1465-72. Addressing data security is necessary to safeguard the effectiveness of these technologies and promote their acceptance by vehicle users. Addressing privacy is similarly necessary to promote public acceptance. The views expressed in that article fairly encompass the agency's views of its regulatory authority.

[243] H.R. Rep. No. 89-1776, at 10 (1966).

Today, in contrast, an increasing number of vehicle functions are electronic. These functions can be activated and controlled automatically and do not necessarily require driver involvement, unlike the mechanical functions of previous generations of vehicles. V2V technologies require no driver involvement in order to send and receive information that can be used for vehicle safety functions. Other ways in which V2V technologies differ from the mechanical technologies prevalent when the Safety Act was first enacted include the fact that how they operate can be substantially altered by post-manufacture software updates, and that advances in communications technology make it possible for nomadic devices with vehicle-related applications to be brought into the vehicle.

The language of the Safety Act, however, is broad enough to comfortably accommodate this evolution in vehicle technologies. NHTSA's statutory authority over motor vehicles and motor vehicle equipment would allow the agency to establish safety standards applicable both to vehicles that are originally manufactured with V2V communications devices, and to those devices added after original manufacture.

In the Safety Act, "motor vehicle" is defined as a "vehicle driven or drawn by mechanical power and manufactured primarily for use" on public roads.[244] The definition of "motor vehicle equipment," as cited below, is broader and thus effectively establishes the limit of the agency's authority under the Safety Act:

> (A) any system, part, or component of a motor vehicle as originally manufactured;
> (B) any similar part or component manufactured or sold for replacement or improvement of a system, part, or component, or as an accessory or addition to a motor vehicle; or
> (C) any device or an article or apparel, including a motorcycle helmet and excluding medicine or eyeglasses prescribed by a licensed practitioner, that –
> i) is not a system, part, or component of a motor vehicle; and
> ii) is manufactured, sold, delivered, or offered to be sold for use on public streets, roads, and highways with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death.[245]

---

[244] 49 U.S.C. § 30102(a)(6).

[245] § 30102(a)(7)(C); MAP-21, Pub. L. 112-141, § 31201, 126 Stat. 405. Congress added subparagraph (C) to the statutory definition of "motor vehicle equipment" in 1970 when it amended the definition in order to clarify the Department's authority over additional objects such as motorcycle helmets. See S. Rep. No. 91-559, at 5 (1970). However, Congress did not seek to limit the extension of the Department's authority only to motorcycle helmets and instead utilized the broad terms "device, article, and apparel" to describe the universe of objects that are within the agency's authority. See id. Acknowledging the concerns of those who authored the House version of the amendatory language that utilizing the terms "device, article, and apparel" might unduly extend the Department's authority to objects that have only a tangential relation to motor vehicle safety, the conference committee added a use restriction. See id. Congress relaxed this use restriction in the statutory definition of "motor vehicle equipment" as part of the amendments to the Safety Act in MAP-21. See MAP-21, Pub. L. 112-141, § 31201, 126 Stat. 405. Thus, the

NHTSA's authority over these groups of items – (1) systems, parts, and components installed or included in a vehicle, (2) replacements and improvements to those systems, parts, and components, (3) accessories and additions to motor vehicles, and (4) devices or articles with an apparent safety-related purpose – is very broad. The status of these items as motor vehicle equipment does not depend on the type of technology or its mode of control (mechanical or electronic), or whether an item is tangible or intangible. The transition from mechanical to electromechanical systems has thus had no effect on the extent of NHTSA's authority over motor vehicle performance. NHTSA has regulatory authority under the Safety Act over all the systems, parts, and components installed on new motor vehicles, even as motor vehicle control systems become increasingly electronic, and perhaps increasingly automated, in the future.

Put in the context of V2V-related motor vehicle equipment, NHTSA considers the following items subject to the agency's regulatory authority:

(1) Any integrated original equipment (OE) used for V2V communications or safety applications reliant on V2V communications
(2) Any integrated aftermarket equipment used for V2V communications or safety applications reliant on V2V communications, under § 30102(a)(7)(B), if the equipment "improves" an already-existing function of the vehicle or is an "addition" to the vehicle
(3) Some non-integrated aftermarket equipment, depending on its nature and apparent purpose, under § 30102(a)(7)(B), if the equipment is a motor vehicle "accessory" (something to be used while the vehicle is in operation, that enhances that operation), or § 30102(a)(7)(C), if the equipment is a device used for the apparent purpose of traffic safety (purpose would be clearly observable from the characteristics of the object and the context of its use, rather than necessarily defined by the manufacturer's intent for the equipment)
(4) Software that provides or aids V2V functions, and software updates to all of this equipment, because, under § 30102(a)(7)B), updates can be considered as replacements or improvements
(5) Potentially some roadside infrastructure (V2I), under § 30102(a)(7)(B) and (C), because if its apparent purpose is safety, it may be an "accessory" or a "device…manufactured…with the apparent purpose of safeguarding users of motor vehicles against accident, injury, or death." We currently anticipate that only a small subset of roadside infrastructure may fall within this category.

Department's regulatory authority under subparagraph (C) is limited to those devices, articles, or apparel that are used for "the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death." See id. (Emphasis added.)

A number of commenters to the ANPRM and Readiness Report raised issues with the agency's discussion of the bounds of its authority. While most commenters agreed that the agency has clear authority to require V2V communications devices in new vehicles and to regulate aftermarket V2V devices,[246] the Alliance argued that it appeared that the agency sought to regulate "the relationship between the vehicle manufacturers and their customers,"[247] given that NHTSA had discussed the potential need for additional security certificates during a V2V communications device's lifetime, as well as the possibility of software updates as needed. The Alliance argued that the Safety Act did not authorize a "lifetime maintenance mandate" to cover the potential need to provide additional certificates or software updates.[248] Moreover, the Alliance argued, NHTSA could not require consumers to renew security certificates or accept downloaded certificates pushed directly to the vehicle, or to ensure that DSRC remained operable over the lifetime of the vehicle, and therefore a FMVSS would not be publicly accepted, and therefore inconsistent with the agency's authority under the Safety Act, because consumers might not be confident that DSRC would continue to work properly over the vehicle's lifetime.[249] The Alliance even suggested that it could violate the Computer Fraud and Abuse Act (18 U.S.C. 1030) to push new certificates to consumers without their consent.[250]

In response, NHTSA agrees that we have authority under the Safety Act to require V2V communications devices in new vehicles and mandate specific aspects of their performance, and to require similar performance from aftermarket V2V devices designed to participate in the V2V system, as long as those standards are consistent with Safety Act requirements.

We disagree, however, with the points raised by the Alliance regarding certificate and software updates. At this time, NHTSA is not requiring that certificate and software updates be pushed to vehicles without consumers' consent – we are simply requiring that manufacturers alert consumers, via a telltale or message center indicator, to the fact that V2V will not work if they are out of certificates or in need of some other kind of update, and that devices be capable of receiving such updates.[251] Consumers will need to know what action the telltale or message center indicator is telling them to take in order to continue to obtain the safety benefits of V2V, so vehicle or device manufacturers will need to ensure either that the message center indicator is clear about the needed action and the consequences of not taking that action, or that the explanation for the message or telltale is contained somewhere (like the owner's information) where the consumer can easily find it and understand what to do. Alternatively, vehicle manufacturers could obtain consumer consent for automatic certificate and software updates at the time of first sale, although that consent would not cover subsequent vehicle owners. Even if manufacturers make it necessary for consumers to consent to each new download, NHTSA

---

[246] Alliance, at 13, 15.
[247] Alliance, at 7.
[248] Alliance, at 15.
[249] Id, and at 15, 47-48.
[250] Alliance, at 15.
[251] See Section III.E.13, above.

expects that the need to do so would be sufficiently infrequent and well-explained by vehicle manufacturers in order to ensure that consumers recognize the significant safety risk of failing to accept the download. We assume that, at this point in time, nearly all consumers are already well-accustomed to the need for software updates on their electronic devices, like computers and smartphones, and regularly accept and initiate such updates. We seek comment from manufacturers on how they plan to develop succinct and compelling explanations to accompany these consent requests that would encourage consumers to accept the updates in a timely manner. We also seek additional comment regarding all aspects of consumer consent.

Alternatively, if manufacturers are concerned that consumers would not accept new certificate downloads and would thereby lose the safety benefits of V2V communications, manufacturers could install V2V devices that are pre-loaded with all the certificates that the device would need over its lifetime. This approach would presumably necessitate more storage capacity on the V2V device (and thus more cost), and could also present a potentially bigger security risk if the device were somehow compromised. We seek comment on whether requiring devices to come pre-loaded with a lifetime's worth of certificates could be a better approach than requiring consumers to consent to (and obtain) new downloads, and if so, why.

Besides certificates, however, we expect that software associated with both the V2V communications device itself, and with any accompanying applications that rely on V2V communications for information, would likely need updating during the vehicle's lifetime. As explained above, as for certificate updates, we are proposing to require that manufacturers include a means to communicate to the driver if and when a software update is needed. If the driver then chooses not to accept the update, the system must continue to warn them that V2V functionality is not available. If manufacturers choose not to update software when issues with it are discovered, and safety problems result, NHTSA may choose to pursue those problems under its enforcement authority.

Some commenters disagreed with the agency's statements in the Readiness Report that our Safety Act authority extended to cover RSE.[252] The Alliance argued that RSE only indirectly served a safety purpose, because they would perform non-safety functions as well, and therefore could not be motor vehicle equipment. CTIA and others presented a similar argument regarding the agency's authority to regulate mobile devices and applications for mobile devices, as it has elsewhere.[253]

With regard to the agency's authority under the Safety Act over RSE, although we are not proposing in this NPRM to regulate any RSEs, we disagree that a device that performs non-safety functions in addition to safety functions is necessarily not motor vehicle equipment. Tires, for example, perform the non-safety function of helping a vehicle travel down the road by

[252] Alliance, at 7, 16.
[253] CTIA in general; TIA at 6; CEA at 2-9; Wi-Fi Alliance at 7.

creating friction between the wheel and the road, but that friction also plays a safety role by helping the vehicle stop rapidly when the driver hits the brakes. Brakes and steering wheels, for that matter, help drivers execute turns which may be necessary to reach their intended destination, but they also help drivers avoid crashing their vehicles. Many items of motor vehicle equipment that NHTSA regulates perform safety functions in addition to being generally necessary for the driving task. NHTSA can regulate those items insofar as they affect vehicle safety. By providing a link between the SCMS and the vehicle, and potentially being the mechanism by which the vehicle's V2V communications device is able to obtain new security certificates and information about which other vehicles to trust and not to trust, the RSE may play a vital role in creating the environment needed for safety. A BSM cannot be sent without a certificate, and a V2V communications device must not trust an untrustworthy partner vehicle, or safety applications may not function properly.

That said, NHTSA does not currently anticipate the need to specify requirements for the RSE that may participate in the overall V2V system. We note that FHWA has already issued specifications for roadside units that are publicly available,[254] and at this point, we would expect the ones participating in the overall V2V system and interacting with V2V-equipped vehicles to conform to these specifications, or to updated specifications if and when they exist. We seek comment on whether additional regulation of RSE/RSU by NHTSA might be important to ensure that, among other things, they do not collect information that could be unnecessarily harmful to privacy; pose no cybersecurity threat to the overall V2V system; or perform (or risk failing to perform) any other task that could be harmful to vehicles or the V2V system or in any way negatively impact safety benefits associated with V2V.

Thus, the agency believes that our existing Safety Act authority comfortably allows us to require V2V communications devices in new motor vehicles and aftermarket equipment. The following section examines what the Safety Act requires NHTSA to consider in developing an FMVSS, and how the proposal in this NPRM may meet those requirements.

B. What does the Vehicle Safety Act allow and require of NHTSA in issuing a new FMVSS, and how is the proposal consistent with those requirements?

Under the Safety Act, NHTSA's motor vehicle safety standards are generally performance-oriented.[255] Further, the standards are required to be practicable and objective, and

---

[254] U.S. DOT Federal Highway Administration, "DSRC Roadside Unit (RSU) Specifications Document, Version 4.0, April 15, 2014." Available at http://docplayer.net/11087167-Dsrc-roadside-unit-rsu-specifications-document.html (last accessed Dec. 6, 2016).

[255] 49 U.S.C. § 30102(a)(8) (defining "motor vehicle safety" as "the performance of a motor vehicle . . . in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle"); and § 30102(a)(9) (defining "motor vehicle safety standard" as "a minimum standard for motor vehicle or motor vehicle equipment performance"). See also: S. Rep. No. 89-1301, at 2713-14

to meet the need for safety.[256] The following paragraphs will discuss briefly the meaning of each of these requirements, and then explore how the agency believes that the proposal may meet those requirements.

1. "Performance-oriented"

In the Safety Act, the Secretary is directed to issue motor vehicle safety standards. "Motor vehicle safety standards" are defined as "minimum standard[s] for motor vehicle or motor vehicle equipment performance."[257] One point to note at the outset is the party of whom performance is required: NHTSA's safety standards apply to manufacturers of new motor vehicles and motor vehicle equipment. It therefore falls to those "manufacturers" – from vehicle OEMs to OE suppliers to aftermarket device manufacturers to creators of V2V safety applications – to certify compliance with any safety standards established by NHTSA, and to conduct recalls and remedy defects if NHTSA finds them.[258] Vehicle owners are not required to comply with NHTSA's safety standards, which means that for vehicles already on the roads, participation in the V2V system would be entirely voluntary: NHTSA can regulate how aftermarket devices function, but it cannot require manufacturers or drivers to add them to used vehicles. The one exception to this rule against retrofit is that NHTSA has authority to require retrofit of commercial heavy-duty vehicles,[259] but that is not part of this proposal on light-duty vehicles.

While NHTSA is directed to establish performance standards, the case law and the legislative history indicate that when necessary to promote safety, NHTSA can be quite specific in drafting its performance standards and may require or preclude the installation of certain equipment. The cases have reinforced this concept by determining that NHTSA is "generally charged"[260] with setting performance standards, instead of becoming directly involved in questions of design.[261] The legislative history further illustrates that NHTSA's standards are to "[specify] the required minimum safe performance of vehicles but not the manner in which the

---

(1966) (stating that motor vehicle standards issued by NHTSA should specify a minimum level of safety performance).

[256] 49 U.S.C. § 30111(a) (establishing requirements for NHTSA to follow when issuing motor vehicle safety standards).

[257] Id.; see also: § 30102(a)(9) (emphasis added).

[258] 49 U.S.C. § 30115(a), "Certification of compliance; In general"; § 30116, "Defects and noncompliance found before sale to purchaser"; § 30117(a), "Providing information to, and maintaining records on, purchasers; Providing information and notice"; § 30118, "Notification of defects and noncompliance"; § 30119, "Notification procedures"; § 30120, "Remedies for defects and noncompliance."

[259] Per 49 CFR 1.95, which delegates to NHTSA the Secretary's authority under Sec. 101(f) of the Motor Carrier Safety Improvement Act of 1999 (Pub. L. 106-159; Dec. 9, 1999) to promulgate safety standards for "commercial motor vehicles and equipment subsequent to initial manufacture." NHTSA's retrofit authority is coextensive with FMCSA's.

[260] Washington v. Dept. of Transp., 84 F.3d 1222, 1224 (10th Cir. 1996) (citations omitted).

[261] Id. at 1224 (citations omitted).

manufacturer is to achieve the specified performance."[262] An example cited in the legislative history points to "a building code which specifies the minimum load-carrying characteristics of the structural members of a building wall, but leaves the builder free to choose his own materials and design."[263] In that example, the agency could require the wall to be built (analogous to requiring certain equipment in vehicles) but would be expected to measure the wall's regulatory compliance by its performance rather than its design.

Although the Safety Act directs NHTSA to issue performance standards, however, Congress understood that the agency may preclude certain designs through these performance standards. "Motor vehicle safety" is defined in the Safety Act as the performance of a motor vehicle in a way that protects the public from unreasonable risks of accident due to (among other things) the design of a motor vehicle.[264] The legislative history indicates that this language is not intended to afford the agency the authority to promulgate design standards, "but merely to clarify that the public is to be protected from inherently dangerous designs which conflict with the concept of motor vehicle safety."[265] This clarification is evidence that Congress recognized that performance standards inevitably have an impact on the design of a motor vehicle.[266]

The courts have further elaborated on the framework established by Congress and have recognized that, when necessary to achieve a safety purpose, NHTSA can be quite specific in establishing performance standards even if certain designs will be precluded. For example, the Sixth Circuit found that an agency provision permitting rectangular headlamps, but only if they were of certain specified dimensions, was not an invalid design restriction and "serve[d] to ensure proper headlamp performance," reasoning that "the overall safety and reliability of a headlamp system depends to a certain extent upon the wide availability of replacement lamps, which in turn depends upon standardization."[267] Thus, the court found it permissible for the agency to establish very specific requirements for headlamps even though it would restrict design flexibility.[268]

Further, the cases indicate that NHTSA can establish standards to require the installation of certain specific equipment on vehicles and establish performance standards for that equipment. For example, the Tenth Circuit found in Washington v. DOT that "NHTSA's regulatory authority extends beyond the performance of motor vehicles per se, to particular items

---

[262] S. Rep. No. 89-1301, at 2713-14 (1966).
[263] Id.
[264] § 30102(a)(9).
[265] H.R. Rep. No. 89-1919, at 2732 (1966).
[266] Courts have also recognized this fact. See Chrysler Corp. v. Dept. of Transp., 515 F.2d 1053, 1058-59 (6th Cir. 1975); see also: Washington, 84 F.3d at 1224 (stating "the performance-design distinction is much easier to state in the abstract than to apply definitively-so …. . This is particularly true when, due to contingent relationships between performance requirements and design options, specification of the former effectively entails, or severely constrains, the latter.").
[267] Chrysler Corp., 515 F.2d at 1058-59.
[268] Id.

of equipment."[269] In that case, the validity of NHTSA's FMVSS No. 121 requiring ABS systems on air-braked vehicles was challenged as "imposing design specifications rather than performance criteria."[270] The court's conclusion was based not only on the fact that prior courts had upheld NHTSA's standards requiring particular equipment,[271] but also on the fact that Congress had recognized NHTSA's former rulemakings and left NHTSA's authority unchanged when it codified the Safety Act in 1994.

Thus, in summary, NHTSA is required to issue performance standards when regulating motor vehicles and motor vehicle equipment. However, NHTSA is able to be quite specific in establishing performance standards and may preclude certain designs that are contrary to the interests of safety. Further, NHTSA may require the installation of certain equipment and establish performance standards for that equipment.

As Section III.E discusses at length and as the regulatory text at the end of this preamble discusses at length, NHTSA has developed a set of proposed performance requirements for DSRC performance. These sections explain: (1) what information needs to be sent to the surrounding vehicles; (2) how the vehicle needs to send that information; (3) how a vehicle shows that it is a valid source of information; and (4) how a vehicle makes sure the prior three functions work in various operational conditions (i.e., broadcast under congested conditions, detect/report misbehavior, and obtain new security materials). The proposal draws from existing voluntary standards while also explaining why a particular threshold or requirements from a voluntary standard is appropriate. The proposal contains a mandatory Privacy Statement, set forth in Appendix A. Finally, the proposal includes a test method for evaluating many of these aspects of performance. Having a clear test method helps inform the public as to how the agency would evaluate compliance with any final FMVSS. While research is ongoing in a few areas (namely message congestion mitigation, explicit details for misbehavior detection, SCMS policies and procedures), we have described for the public the potential requirements that we are considering for an NPRM and the potential test methods for evaluating compliance with those requirements. We believe that the public comments that we will receive in response (coupled with the agency's ongoing research) will produce a robust record upon which the agency can make a final decision.

The provisions allowing alternative technologies to satisfy the mandate are performance-oriented, but do not specify a particular way of communicating. The goal of this is to maximize

---

[269] Washington, 84 F.3d at 1222, 1225 (citations omitted).
[270] Id. at 1223.
[271] Id. at 1225 (citing Chrysler Corp. v. Rhodes, 416 F.2d 319, 322, 322 n. 4) (1st Cir. 1969) ("motor vehicles are required to have specific items of equipment . . . These enumerated items of equipment are subject to specific performance standards," including lamps and reflective devices requiring "specific items of equipment")); Wood v. Gen. Motors Corp., 865 F.2d 395, 417 (1st Cir. 1988) ("requiring seat belts or passive restraints . . . has elements of a design standard"); Automotive Parts & Accessories Ass'n v. Boyd, 407 F.2d 330, 332 (D.C. Cir. 1968) ("factor equipped . . . head restraints which meet specific Federal standards").

industry's ability to innovate and potentially employ future communication technologies that may be able to meet the performance requirements (like, for example, latency) for V2V-based safety warning applications. While alternative technologies would be subject to several aspects of the test procedures set forth for DSRC-based devices, it leaves open for industry to develop a number of aspects of performance, including interoperability with all other V2V communications technologies that transmit BSMs. We believe that the inclusion of some performance tests makes these provisions consistent with the Safety Act requirement of standards being "performance-oriented." We seek comment on this tentative conclusion.

2. Standards "meeting the need for motor vehicle safety"

As required by the Safety Act, standards issued by the agency must "meet the need for motor vehicle safety."[272] As "motor vehicle safety" is defined in the statute as protecting the public against "unreasonable risk" of accidents, death, or injury,[273] the case law indicates that there must be a nexus between the safety problem and the standard.[274]

However, a standard need not address safety by direct means. In upholding NHTSA's authority to issue a safety standard requiring standardized vehicle identification numbers, the Fourth Circuit Court of Appeals found that an FMVSS requiring VINs met the need for motor vehicle safety by such indirect means as reducing errors in compiling statistical data on motor vehicle crashes (in order to aid research to understand current safety problems and support future standards, to increase the efficiency of vehicle recall campaigns, and to assist in tracing stolen vehicles).[275]

We believe that there is a clear nexus between the safety problem and the proposals in this document. In the case of DSRC-based devices, DSRC can enable all of the safety applications under consideration by the agency, such as Intersection Movement Assist, Left Turn Assist, and Electronic Emergency Brake Light, which means that DSRC can help to address the safety problems of, e.g., intersection collisions, collisions with forward stopped or slowing vehicles, collisions that occur because a driver chose to pass a forward vehicle without enough room to do so safely, etc. For some of the other safety applications, which can also be enabled by other technologies besides DSRC, such as on-board sensors, radar, or cameras, DSRC can add robustness to an on-board system. DSRC will either be the sole enabler of some safety

---

[272] 49 U.S.C. § 30111(a).
[273] 49 U.S.C. § 30102(a)(8).
[274] See, e.g., Nat'l Tire Dealers Ass'n v. Brinegar, 491 F.2d 31, 35-37 (D.C. Cir. 1974) (stating that the administrative record did not support a significant nexus between motor vehicle safety and requiring retread tires to have permanent labels because there was no showing that a second-hand owner would be dependent on these labels and no showing as to how often such situations would arise); see also H&H Tire Co. v. Dept. of Transp., 471 F.2d 350, 354-55 (7th Cir. 1972) (expressing doubt that the standard met the need for safety because there was little evidence that the required compliance tests would ensure that retreaded tires would be capable of performing safely under modern driving conditions).
[275] Vehicle Equip. Safety Comm'n v. NHTSA, 611 F.2d 53, 54 (4th Cir. 1979).

applications or present a possible enhancement to on-board systems with regard to other applications. In either case, DSRC will address safety needs.

Moreover, case law supports that DSRC need not directly create more safety itself, as long as it is enabling other safety applications. If VINs could be upheld as meeting the need for motor vehicle safety simply by virtue of the fact that they aid research in understanding safety problems and supporting future standards, as well as aiding recall campaigns and tracking of stolen vehicles, then DSRC, which would directly enable half a dozen safety applications at its inception and perhaps many more eventually, seems even more clearly to meet the need for safety in that respect.

Non-DSRC devices should have a similar nexus to the safety problem.

3. "Objective" standards

A standard is objective if it specifies test procedures that are "capable of producing identical results when test conditions are exactly duplicated" and performance requirements whose satisfaction is "based upon the readings obtained from measuring instruments as opposed to subjective opinions."[276] The requirement that standards be stated in objective terms matches the overall statutory scheme requiring that manufacturers self-certify that their motor vehicles or motor vehicle equipment comply with the relevant FMVSSs.[277] In order for this statutory scheme to work, the agency and the manufacturer must be able to obtain the same result from identical tests in order to objectively determine the validity of the manufacturer's certification.[278]

Using those two elements of objectivity (capable of producing identical results and compliance based on measurements rather than subjective opinion), the Sixth Circuit Court of Appeals found that the test procedure in question in an early version of FMVSS No. 208 was not objective because the test dummy specified in the standard for use in compliance testing did not give consistent and repeatable results.[279] The court in this case was unconvinced that the

---

[276] Chrysler Corp. v. Dept. of Transp., 472 F.2d 659, 676 (6th Cir. 1972); see also Paccar, Inc., v. Nat'l Highway Traffic Safety Admin., 573 F.2d 632, 644 (9th Cir. 1978).
[277] 49 U.S.C. § 30115(a).
[278] Chrysler Corp., 472 F.2d at 675.
[279] As the court stated,

> The record supports the conclusions that the test procedures and the test device specified . . . are not objective in at least the following respects: (1) the absence of an adequate flexibility criteria for the dummy's neck; the existing specifications permit the neck to be very stiff, or very flexible, or somewhere in between, significantly affecting the resultant forces measured on the dummy's head. (2) Permissible variations in the test procedure for determining thorax dynamic spring rate (force deflection characteristics on the dummy's chest) permit considerable latitude in chest construction which could produce wide variations in maximum chest deceleration between two different dummies, each of which meets the literal requirements of SAE J963. (3) The absence of specific, objective specifications for construction of the

standard met the objectivity requirements even though NHTSA based its test procedure on a test dummy in a voluntary automotive industry standard (Society of Automotive Engineers Recommended Practice J963). The court rejected NHTSA's explanation that, although J963 "may not provide totally reproducible results," "dummies conforming to the SAE specifications are the most complete and satisfactory ones presently available."[280] Further, the court rejected NHTSA's reasoning that, in the event that the agency's test results were different from those of the manufacturers because of the difference in the test dummies, NHTSA's test results would not be used to find non-compliance, stating that "there is no room for an [ ] agency investigation [ ] in this procedure" that enable the agency to compare results of differing tests.[281]

Other courts have also reached similar conclusions. The Ninth Circuit Court of Appeals, relying on the same reasoning adopted by the Sixth Circuit, found that a compliance road test specifying the use of surfaces specifically rated with quantifiable numbers (defining the "slickness" of the surfaces) was objective despite "[t]he fact that it is difficult to create and thereafter maintain a road surface with a particular coefficient of friction," which the court held "does not render the specified coefficient any less objective."[282] In this case, both NHTSA and the manufacturer would perform road tests on surfaces with identically rated friction coefficients.[283] In a later case, the Sixth Circuit upheld NHTSA's decision not to incorporate a test suggested by a commenter for wheelchair crashworthiness performed with a "test seat" that "shall be capable of resisting significant deformation" during a test as not sufficiently objective.[284] In the absence of language quantifying how much deformation is significant, terms such as "significant deformation" do not provide enough specificity to remove the subjective element from the compliance determination process.

As discussed above, under the proposal, we have developed and are proposing performance requirements, including compliance test procedures, for DSRC. We will continue evaluating the compliance test procedures further and receiving public input during the comment period that can assist us in fine-tuning the procedures and ensuring that they meet our statutory requirements. For alternative technologies, given that the testing to this point that led to the development of the test procedures for interoperability did not evaluate the use of non-DSRC

---

dummy's head permits significant variation in forces imparted to the accelerometer by which performance is to be measured.
Id. at 676-78.
[280] Id. at 677.
[281] Id. at 677-79.
[282] Paccar, Inc. v. Nat'l Highway Traffic Safety Admin., 573 F.2d 632, 644 (9th Cir. 1978), cert. denied, 439 U.S. 862 (1978).
[283] Id. (stating that the "skid number method of testing braking capacity meets the [objectivity] definition. Identical results will ensue when test conditions are exactly duplicated. The procedure is rational and decisively demonstrable. Compliance is based on objective measures of stopping distances rather than on the subjective opinions of human beings.").
[284] Simms v. Nat'l Highway Traffic Safety Admin., 45 F.3d 999, 1007-08 (6th Cir. 1995).

communication technologies, we seek comment on how the regulatory text alternative technologies can achieve interoperability in an objective manner.

4. "Practicable" standards

In general, the practicability of a given standard involves a number of considerations. The majority of issues concerning the practicability of a standard arise out of whether the standard is technologically and economically feasible. An additional issue is whether the means used to comply with a standard will be accepted and correctly used by the public.

First, significant technical uncertainties in meeting a standard might lead a court to find that a standard is not practicable. For example, the Sixth Circuit Court of Appeals upheld NHTSA's decision to amend FMVSS No. 222 to include requirements for wheelchair securement and occupant restraint on school buses with a static[285] compliance test instead of a dynamic test,[286] noting that the administrative record showed that this particular dynamic test was underdeveloped and had many unresolved technical problems.[287] The court noted that it is not practicable "[t]o attempt to fashion rules in an area in which many technical problems have been identified and no consensus exists for their resolution …. ."[288] In another example, the Ninth Circuit Court of Appeals found a compliance test procedure using a specified friction (slickness) coefficient to be impracticable due to technical difficulties in maintaining the specific slickness test condition. As mentioned above, the Ninth Circuit found the specified coefficient test condition to be objective.[289] However, simply being objective did not also make the test condition practicable. Thus, the cases show that when significant technical uncertainties and difficulties exist in a standard promulgated by NHTSA, those portions of the standard can be considered impracticable under the Safety Act.

---

[285] Static testing tests the strength of individual components of the wheelchair separately, while dynamic testing subjects the entire wheelchair to simulated real-world crash conditions. See Simms, 45 F.3d at 1001.

[286] Id. at 1006-08. Petitioners argued that NHTSA had acted unlawfully in promulgating standards for the securement of wheelchairs on school buses based only on "static" instead of "dynamic" testing. Id. Static testing tests the strength of the individual components of a securement device. Id. Dynamic testing is a full systems approach that measures the forces experienced by a human surrogate (test dummy) in a simulated crash that replicates real-world conditions and assesses the combined performance of the vehicle and the securement device. Id.

[287] Id. at 1005-07. NHTSA agreed that dynamic testing is the preferred approach (because it more fully and accurately represents the real-world conditions in which the desired safety performance is to be provided), but explained that it was not practicable at that time to adopt dynamic testing because there was:

> (1) [N]eed to develop an appropriate test dummy; (2) need to identify human tolerance levels for a handicapped child; (3) need to establish test conditions; (4) need to select a "standard" or surrogate wheelchair; (5) need to establish procedures for placing the wheelchair and test dummy in an effective test condition; and (6) need to develop an appropriate test buck to represent a portion of the school bus body for securement and anchorages.

Id. at 1005.

[288] Id. at 1010-11.

[289] Paccar, Inc. v. Nat'l Highway Traffic Safety Admin., 573 F.2d 632, 644 (9th Cir. 1978).

However, the requirement that a standard be technologically feasible does not include the additional requirement that the agency show that the technology to be used to comply with the standard is already fully developed and tested at the time that the standard is promulgated. The Sixth Circuit upheld a NHTSA standard requiring "Complete Passive Protection," that required the installation of airbags as standard equipment by a future date, rejecting petitioner's contention that NHTSA may only establish performance requirements which can be met with devices which, at the time of the rulemaking, are developed to the point that they may be readily installed.[290] Relying on the legislative history of the Safety Act, the court found that the agency "is empowered to issue safety standards which require improvements in existing technology or which require the development of new technology, and is not limited to issuing standards based fully on devices already developed."[291] Thus, the requirement that standards be technologically feasible is sufficiently broad that it can be satisfied by showing that new technology can be developed in time to comply with the effective date of the standard.[292]

Second, a standard can be considered impracticable by the courts due to economic infeasibility. This consideration primarily involves the costs imposed by a standard.[293] In the instances in which a court has been called upon to assess whether a standard is economically feasible, typically with respect to an industry composed largely of relatively small businesses, the courts have asked whether or not the cost would be so prohibitive that it could cause significant harm to a well-established industry. In essence, this consideration generally establishes a non-quantified outer limit of the costs that can be reasonably imposed on regulated entities. If compliance with the standard is so burdensome, i.e., costly, so as to create a

---

[290] See Chrysler Corp. v. Dept. of Transp., 472 F.2d at 671-75. Stages one and two required vehicle manufacturers to provide "Complete Passive Protection" or one of two other options on vehicles manufactured between January 1, 1972 and August 14, 1973 (for stage one) and after August 15, 1973 (stage two). See id. at 666-67. Stage three, requiring solely "Complete Passive Protection," was required by August 15, 1975. Id. at 667.

[291] Id. at 673. In making its decision, the court stated

> [I]t is clear from the Act and its legislative history that the Agency may issue standards requiring future levels of motor vehicle performance which manufacturers could not meet unless they diverted more of the ir resources to producing additional safety technology than they might otherwise do. This distinction is one committed to the Agency's discretion, and any hardships which might result from the adoption of a standard requiring . . . a great degree of developmental research, can be ameliorated by the Agency under . . . The section [that] allows the Secretary to extend the effective date beyond the usual statutory maximum of one year from the date of issuance, as he has done [here].

Id. at 673.

[292] A corollary of the agency's authority to issue technology-driving standards is that the agency can rely on data other than real-world crash data in justifying those standards. Technology that is not yet either fully developed or being installed on production vehicles cannot generate real-world performance data. Thus, in justifying the issuance of technology-driving standards, it is permissible, even necessary, for the agency to rely on analyses using experimental test data or other types of non-real world performance information in determining whether such standards "meet the need for vehicle safety."

[293] E.g., Nat'l Truck Equip. Ass'n v. Nat'l Highway Traffic Safety Admin., 919 F.2d 1148, 1153-54 (6th Cir. 1990); Ctr. for Auto Safety v. Peck, 751 F.2d 1336, 1343 (D.C. Cir. 1985) (panel opinion by Circuit Judge Scalia).

significant harm to a well-established industry, courts have generally found that the standard is impracticable in its application to that industry.

Finally, a standard might not be considered practicable if the public were not expected to accept and correctly use the technologies installed in compliance with the standard. When considering passive restraints such as automatic seatbelts, the D.C. Circuit stated that "the agency cannot fulfill its statutory responsibility [in regard to practicability] unless it considers popular reaction."[294] While the agency argued in that case that public acceptance is not one of the statutory criteria that the agency must apply, the court disagreed. The court reasoned that "without public cooperation there can be no assurance that a safety system can 'meet the need for motor vehicle safety.'"[295] Thus, as a part of the agency's considerations, a standard issued by the agency will not be considered practicable if the technologies installed pursuant to the standard are so unpopular that there is no assurance of sufficient public cooperation to meet the safety need that the standard seeks to address.[296]

We believe that the proposal is consistent with these requirements. Technologically, DSRC has existed for over a decade, and is currently being used in Japan to support V2I applications and electronic toll collection. The performance requirements and test procedures being proposed to help ensure interoperability should also ensure the technological practicability of the proposal. In terms of economic practicability, NHTSA currently assumes that the cost of a DSRC standard would include costs for device hardware and software, as well as costs for the security and communications system that would be necessary in order for DSRC to function properly. As discussed in Section VII below, we estimate the likely total cost for a V2V system to the consumer (vehicle equipment costs, fuel economy impact, SCMS costs, and communication costs) at approximately $350 per new vehicle in 2020. Economic practicability requires that compliance with the standard should not be so burdensome as to create a significant harm to a well-established industry. It does not seem likely that a court would find the standards economically impracticable either for the auto industry, or for any small business interests potentially implicated, since those would more likely be in the context of aftermarket devices (phone apps and so forth), which are entirely voluntary and do not represent a mandate.

For the question of public acceptance, the main concerns with regard to the proposal likely relate to security and privacy. To address such concerns, the requirements in the proposal include tests to ensure tamper-resistance of the DSRC unit; security requirements for the messages themselves; express requirements that certain identifying information not be included in the BSMs, and so forth. We are also proposing that manufacturers alert drivers when software

---

[294] Pac. Legal Found. v. Dept. of Transp., 593 F.2d 1338, 1345-46 (D.C. Cir.), cert. denied, 444 U.S. 830 (1979).
[295] Id.
[296] Pursuant to concerns about public acceptance of various seat belt designs, NHTSA issued a final rule in 1981 adding seat belt comfort and convenience requirements to Standard No. 208, Occupant Crash Protection. Federal Motor Vehicle Safety Standards; Improvement of Seat Belt Assemblies, 46 Fed. Reg. 2064 (Jan. 8, 1981) (codified at 49 CFR Part 571).

upgrades and patches and certificate updates are needed, and we are hopeful that such updates would be as seamless as possible.

With respect to comments on the agency's authority received to the ANPRM and Readiness Report, commenters tended to support generally the agency's authority to establish an FMVSS for V2V communications, while some commenters offered their own interpretations of what would be necessary for a standard to be consistent with the Safety Act. The Alliance, for example, argued that a proposal to mandate DSRC in new vehicles and set standards for DSRC aftermarket devices would not meet the Safety Act criteria if (1) NHTSA could not prove that the standard would improve safety as compared with not adopting a new FMVSS; (2) NHTSA did not present how a security system would be "established, funded, governed and operated": and (3) FCC opened the 5.9 GHz spectrum to unlicensed wireless devices and the operation of those devices resulted in harmful interference to V2X communications.[297] Additionally, the Alliance underscored the importance of addressing public perception issues in order to ensure that consumers are willing to accept DSRC technology, because otherwise a mandate would not be practicable and the market failure would not be cured.[298] The Alliance suggested that the agency consider working with other federal agencies with more direct experience in addressing health and privacy concerns to address potential public acceptance issues.[299] Global Automakers agreed that it was important to a DSRC mandate that NHTSA work carefully with other Federal agencies (i.e., FCC and NTIA) to ensure that DSRC communications can be effective and interoperable without harmful interference.[300] Toyota stated that a necessary pre-condition for a DSRC mandate was a limited deployment of a production-ready, DSRC-equipped fleet to confirm product design.[301] TIA commented that any FMVSS for V2V communications should be entirely technology agnostic and focus on performance requirements (data latency, size, interoperability) that could be met by any technology, not only DSRC, and allow technologies to evolve over time.[302]

As discussed above, NHTSA continues to believe that the proposal is consistent with the Safety Act. As Section III.E discusses at length and as the proposed regulatory text for the proposal at the end of this preamble discuss at length, NHTSA has developed proposed requirements for DSRC performance. These sections explain: (1) what information needs to be sent to the surrounding vehicles; (2) how the vehicle needs to send that information; (3) how a vehicle shows that it is a valid source of information; and (4) how a vehicle makes sure the prior three functions work in various operational conditions (i.e., broadcast under congested conditions, detect/report misbehavior, and obtain new security materials). The proposal draws from existing voluntary standards while also explaining why a particular threshold or

---

[297] Alliance at 6-7, 13-14.
[298] Alliance at 9, 14.
[299] Alliance at 10.
[300] Global at 11.
[301] Toyota at 1.
[302] TIA at 4, 5.

requirements from a voluntary standard is appropriate. Finally, the proposal includes a test method for evaluating many of these aspects of performance. Having a clear test method helps inform the public as to how the agency would evaluate compliance with any final FMVSS based on the proposal. While research is ongoing in a few areas (namely message congestion mitigation, explicit details for misbehavior detection, SCMS policies and procedures), we have described for the public the potential requirements in the proposal and the potential test methods for evaluating compliance with those requirements. We believe that the public comments that we will receive in response (coupled with the agency's ongoing research) will produce a robust record upon which the agency can make a final decision.

We do not agree with commenters that the proposed standard must be perfectly neutral regarding technology, nor that all possible issues associated with ensuring the long-term success of V2V must be resolved prior to issuing a proposal. As explained above, case law supports the principle that an FMVSS may restrict design flexibility if certain designs would be contrary to the interests of safety. Additionally, we do not believe that waiting to issue a proposal until, for example, DSRC is more thoroughly tested in the fleet, or an SCMS is fully funded and operational, or every potential consumer concern is resolved, would be in the best interest of safety. S9 of the regulatory text, however, is directly responsive to the TIA comment requesting that the agency consider a technology agnostic approach. As covered in the discussion concerning why we are proposing to require V2V communications, for a technology like V2V, where a critical mass of equipped vehicles is needed to create the environment for safety benefits to be possible, the agency does not believe that sufficient quantities of V2V-equipped vehicles will be introduced in the market absent a mandate. By proposing this FMVSS, we aim to create an information environment which, we believe, will then enable the market to bring forth the safety, mobility, and environmental benefits that we anticipate V2V can provide. We intend to continue working closely with other Federal agencies and industry stakeholders on spectrum issues, with industry stakeholders and consumer groups and others on consumer-related concerns, and with all relevant parties on developing an SCMS to support a V2V network. We will also continue our research to improve and refine potential performance requirements and test procedures, as discussed above. Again, public comment on the proposal will facilitate our careful consideration of these issues, and we look forward to hearing from commenters on how to resolve them to best serve the interests of safety.

C. How are the regulatory alternatives consistent with our Safety Act authority?

Besides the proposal, the agency is considering two regulatory alternatives – the first, a "mandate V2V communications and safety applications" alternative, under which the agency also requires new vehicles to have IMA and LTA capabilities; and the second, an "if-equipped" alternative, that would set baseline requirements for V2V communications, but not require new vehicles to have this technology on any specific schedule. Under both the "mandate V2V communications" proposal and the "and safety applications" alternative, the phase-in rate for V2V communications for new vehicles would be 50 percent in the first required year, 75 percent in the second year, and 100 percent in the third year and beyond. We have evaluated the "and

safety applications" alternative in terms of two different phase-in scenarios – in the first scenario, safety applications would be required for new vehicles at a phase-in rate of 0 percent – 50 percent – 75 percent – 100 percent over four years; while in the second scenario, safety applications would be required for all new vehicles in the first year that V2V communications are required. The "if-equipped" alternative, on the other hand, faces much greater uncertainty regarding the technology adoption. Based on the estimated costs of V2V radios and the SCMS, and the "network" nature of V2V communication, the agency believes that Alternative 2 is unlikely to lead to meaningful deployment of V2V communications. Consequently, Alternative 2 would delay, potentially for a significant period of time, the anticipated benefits of V2V communications. Furthermore, there is a high probability that the designated spectrum for V2V safety applications would be lost if a mandate was not pursued. For these reasons, the "if-equipped" alternative is not a viable alternative. Due to this, as well as to the significant uncertainty surrounding the technology adoption, the PRIA does not examine the costs and benefits for this alternative.

The "if-equipped" alternative is consistent with the agency's Safety Act authority, which does not require NHTSA to require technology for new vehicles. It is therefore not discussed further in this section.

The agency evaluated our authority to mandate specific safety applications in the Readiness Report[303] and sought comment on that evaluation in the ANPRM.[304]

As discussed in the Readiness Report, an FMVSS for a safety application must include minimum requirements for its performance. This first requires a determination of what tasks the safety applications need to perform, which would vary based on the types of safety risks/crash scenarios that the application is intended to address. The agency explained in the Readiness Report that it is examining the currently-available (research-stage) performance and test metrics associated with each safety application, and analyzing these metrics against the available safety data to determine whether these metrics cover the relevant safety problem.

The Readiness Report explained that the agency envisioned that an FMVSS for one of the analyzed safety applications would set performance requirements that could be met by any technology, but that if V2V communications performance requirements made it reasonable to require more robust performance, we could require that performance if V2V communications were mandated. The agency recognized for some applications, like IMA and LTA, performance requirements can likely be met only with V2V communications-based technologies due to their ability to detect crossing-path vehicles, but for others, a variety of technologies could potentially be used.

---

[303] See Readiness Report at Section IV.B.3.
[304] 79 FR at 49271 (Aug. 20, 2014).

With regard to other Safety Act requirements for an FMVSS, the Readiness Report concluded as follows:

- Meet the need for safety: FMVSSs for the V2V-based safety applications would be issued to address safety problems that continue to cause crashes in the absence of regulation or market forces driving their adoption, and would address those problems by warning drivers of dangerous conditions and triggering a response to avoid the danger. However, given that research continues at this point to develop driver-vehicle interfaces for each of the safety applications, and given that the agency was not yet able to demonstrate how effective the DVIs we may eventually mandate are at warning the drivers and inducing them to avoid the dangerous situation, our evidence could be stronger that the V2V safety applications will meet the need for safety.
- Objective test procedures and performance requirements: Test procedures and performance requirements for the V2V safety applications are still being developed, but NHTSA would ensure that any test procedures it may require would meet the criteria of being objective.
- Technological practicability: Because test procedures and requirements (including those for DVIs) are still being developed for the V2V safety applications, additional lead time could be helpful to meet eventual standards in order to ensure that manufacturers have the opportunity to work out how to comply.[305] More research will be helpful in informing future assessments of technological practicability.
- Economic practicability: NHTSA currently assumes using preliminary cost estimates that the cost of standards for the V2V-based safety applications would primarily include costs for software that would be used by the vehicle to interpret V2V signals and make decisions about whether to warn the driver, as well as costs for any hardware that would be necessary to make those warnings happen via the DVI. While it seems unlikely that economic practicability would be an issue for potential safety application FMVSSs, more research to determine costs more precisely would be beneficial to this assessment.
- Public acceptance: Based on the research we have so far from the Safety Pilot, driver enthusiasm for individual V2V safety applications varies. Given that DVI requirements remain under development, and given the need for continued research to avoid a high false positive rate, more work needs to be done before we can be confident that eventual FMVSSs for V2V safety applications will not have public acceptance risks.

Commenters generally agreed with the agency's authority to issue FMVSSs for V2V-based safety applications (both in terms of mandating their installation and regulating their performance), and also agreed that more work was likely needed before such FMVSSs would be consistent with Safety Act requirements. The Alliance, for example, agreed that NHTSA could specify levels of performance for safety applications that "indirectly eliminate[d] some forms of

[305] See discussion above regarding the Sixth Circuit's finding in *Chrysler*, 472 F.2d at 659, 666, and 671-75 (6th Cir. 1972).

delivering the safety application within the motor vehicle," but stated that much work was needed before it would be clear that an FMVSS for any safety application met Safety Act criteria.[306] Global commented that DSRC should be widespread in the fleet and manufacturers should already have experience with applications before the agency should mandate them;[307] Honda provided similar comments.[308] Ford commented that NHTSA should not mandate applications.[309] Toyota, in contrast, stated that NHTSA should require IMA and LTA at the same time as it mandates DSRC capability, in order to speed introduction of safety benefits,[310] although it also stated that any FMVSS for a safety application must meet Safety Act criteria.[311] Advocates for Highway and Auto Safety provided similar comments.[312] Hyundai, TIA, and Delphi commented that if the agency decided to mandate safety applications like IMA and LTA, it should ensure that standards were entirely performance-based and technology-neutral.[313] A number of commenters raised concerns about the need for additional research with regard to DVIs and false positive alerts.[314]

NHTSA agrees with some commenters that earlier introduction of safety applications would guarantee earlier achievement of safety benefits associated with V2V capability, and we also agree with other commenters that additional work would likely be necessary in order for the agency to ensure that potential FMVSSs for safety applications were objective and practicable. Developing minimum standards for safety application performance requires a determination of what tasks the safety applications need to perform, which varies based on the types of safety risks/crash scenarios that the application is intended to address. The agency is examining the currently-available (research-stage) performance and test metrics associated with a variety of safety applications, including IMA and LTA, and analyzing these metrics against the available safety data to determine whether these metrics cover the applicable safety problem(s). Although this research is currently underway, we request comment now on whether and, if so, how the agency could design requirements to mandate certain safety applications.

In response to comments that FMVSSs should be performance-oriented and technologically neutral, we envision that each FMVSS for one of these safety applications would set performance requirements that could be met by any technology. However, if V2V communication performance requirements made it reasonable to require more robust performance, we could require that performance when V2V communication is mandated.

---

[306] Alliance at 17.
[307] Global at 3.
[308] Honda at 6.
[309] Ford at 3-4.
[310] Toyota at 1.
[311] Toyota at 4.
[312] Advocates at 1-2.
[313] Hyundai at 2; TIA at 4; Delphi at 1.
[314] Bendix at 10-11.

We continue to believe that any FMVSSs for the V2V safety applications would meet the need for safety, insofar as we would issue them to address safety problems that continue to cause crashes in the absence of regulation or market forces driving the adoption of these technologies. The safety applications are clearly intended to relate to safety – they warn drivers of dangerous conditions and are intended to promote safety by triggering a response to avoid the danger.

There are several things that the agency could do to help solidify the nexus of safety application warning and driver response. For example, and as raised by commenters, research continues at this point to develop driver-vehicle interfaces for each of the safety applications. We will want to be able to demonstrate how effective the DVIs we may eventually mandate are at warning the drivers and inducing them to avoid the dangerous situation. We currently have reason to believe that the V2V safety applications will meet the need for safety, but additional information and analysis will make that case stronger and we request comment on this.

FMVSSs for V2V safety applications also need to be objective, meaning that they specify test procedures that are "capable of producing identical results when test conditions are exactly duplicated" (meaning that the agency and the manufacturer must be able to obtain the same result from identical tests) and performance requirements whose satisfaction is "based upon the readings obtained from measuring instruments as opposed to subjective opinions." As discussed above, test procedures and performance requirements for the V2V safety applications are still being developed, but NHTSA would ensure that any test procedures it may require would meet the criteria of being objective, and also technologically practicable. NHTSA would provide appropriate lead time for any FMVSSs to ensure these criteria are met, as well.[315] More research and additional public comment will be helpful in informing future assessments of technological practicability.

In terms of economic practicability, NHTSA currently assumes using preliminary cost estimates that the cost of standards for the V2V-based safety applications would primarily include costs for software that would be used by the vehicle to interpret V2V communications signals and make decisions about whether to warn the driver, as well as costs for any hardware that would be necessary to make those warnings happen via the DVI. As discussed above, it seems unlikely that economic practicability would be an issue for potential safety application FMVSSs, but more research to determine costs more precisely would be beneficial to this assessment.

While the Safety Pilot Model Deployment provided participating manufacturers with useful real-world experience in tuning prototype applications to maximize effectiveness and minimize false positives, DVI requirements remain under development, and more work needs to be done before we can be confident that eventual FMVSSs for V2V safety applications will not have public acceptance risks.

---

[315] See discussion above regarding the Sixth Circuit's finding in Chrysler, 472 F.2d at 659, 666, and 671-75

D. What else needs to happen in order for a V2V system to be successful?

1. SCMS

Under both the Vehicle Safety Act and the Highway Safety Act, NHTSA has other ways of affecting the parts of the V2V system that cannot be regulated directly. For example, 49 U.S.C. § 30182 provides NHTSA authority to enter into contracts, grants, and cooperative agreements with a wide range of outside entities to conduct motor vehicle safety research and development activities, including activities related to new and emerging technologies. Separately, the Highway Safety Act (23 U.S.C. § 401 et seq.) authorizes NHTSA to enter into contracts, grants, cooperative agreements, and other transactions for research and development activities with a similarly wide range of outside entities in "all aspects of highway and traffic safety systems … relating to [ ] vehicle, highway, [and] driver … characteristics" (§ 403(b)), as well as collaborative research and development, on a cost-shared basis, to "encourage innovative solutions to highway safety problems" and "stimulate the marketing of new highway safety related technology by private industry" (§ 403(c)). Because issues related to V2V are cross-cutting, spanning both the Vehicle Safety Act and the Highway Safety Act, these separate authorities provide the agency with sufficient flexibility to enter into a variety of agreements related to the development of a V2V security system (although the agency currently lacks sufficient appropriations to incur any significant Federal expenditures for these purposes).

A principle of appropriations law known as the "necessary expense doctrine" allows NHTSA to take the next step of entering into contracts or agreements to ensure the existence of sufficient communications and security systems to support deployment of V2V technologies, if V2V communications are mandated or otherwise regulated by a Federal Motor Vehicle Safety Standard or other NHTSA regulation. According to that principle, when an appropriation is made for a particular purpose, it confers on the receiving agency the authority to incur expenses necessary to carry out the purpose of the appropriation.[316] Under the necessary expense doctrine, the spending agency has reasonable discretion to determine what actions are necessary to carry out the authorized agency function. Here, the agency assumes that the deployment and operation of the SCMS is necessary in order for V2V technology and on-board equipment to function in a safe, secure and privacy-protective manner.[317] As designed, V2V technology cannot operate

---

[316] Under the necessary expense doctrine, an expenditure is justified if it meets a three-part test: (1) the expenditure must bear a logical relationship to the appropriation sought to be charged (i.e., it must make a direct contribution to carrying out either a specific appropriation or an authorized agency function for which more general appropriations are available); (2) the expenditure must not be prohibited by law; and (3) the expenditure must not be otherwise provided for (i.e., it must not be an item that falls within the scope of some other appropriation or statutory funding scheme. See U.S. Gen. Accounting Office, Principles of Federal Appropriations Law 4–22 (3d ed.2004) (the "GAO Redbook"), available at http://www.gao.gov/special.pubs/3rdeditionvol1.pdf (last accessed Dec. 6, 2016).

[317] Potentially, under some alternatives of this proposal, the agency would not assume the future presence of an SCMS, and would leave security requirements more open. In this instance, presumably the agency would not need

without a sufficient security system, and absent such a security system, misbehavior by hackers or others could compromise V2V functionality and participant privacy. If the problem of "misbehavior" were sufficiently widespread, it might even cause widespread disregard of or delayed response to V2V warnings. Hence, a robust SCMS is imperative in the V2V regulatory environment.

For these reasons, in addition to NHTSA's research, development, and collaboration authority under the Vehicle Safety Act and the Highway Safety Act, the necessary expense doctrine provides sufficient authority under the Vehicle Safety Act to take the next step of entering into agreements or contracts, either for cost or no-cost, with the goal of ensuring the existence (i.e., the development and operation) of sufficient communications and security systems to support the reliability and trustworthiness of V2V communications. As is the case under the agency's research and development authority, discussed above, the current limiting factor is the absence of sufficient appropriations to incur any significant expenses in this regard.

NHTSA received comments to the ANPRM and Readiness Report from some stakeholders suggesting that NHTSA itself must obtain funding for and develop at least parts of the SCMS as a Federal project.[318] While NHTSA agrees that we would have authority, as discussed directly above, to facilitate the development of an SCMS if we had the appropriations to do so, conditions have not changed since our issuance of the ANPRM and Readiness Report that would allow us to do so.

2. Liability

The Readiness Report discussed the issue of legal liability in the context of V2V,[319] and the ANPRM sought comment on that discussion.[320] For purposes of that discussion, the agency separated potential liability issues for V2V into two categories: (1) liability associated with equipment on the vehicle, particularly warning systems that rely on V2V systems, and (2) liability associated with the SCMS.

For the first category, NHTSA stated that from a products liability standpoint, V2V safety warning technologies, analytically, are quite similar to on-board safety warnings systems found in today's motor vehicles, and that therefore, V2V warning technologies do not create new or unbounded liability exposure for industry, because the driver remains responsible for failing to avoid a crash when the technology only warns and does not intervene. Consequently, NHTSA stated that it is not necessary, nor would it be appropriate to advocate the liability limiting agenda sought by industry in connection with potential deployment of V2V safety warning

---

to ensure the existience of communications and security systems to support V2V, so the invocation of the necessary expense doctrine would not be necessary.

[318] GM, at 4; Alliance, at 19.

[319] See Section X of the Readiness Report.

[320] 79 FR at 49273 (Aug. 20, 2014).

technologies via government regulation – and that, in any event, only Congress has the authority to provide the V2V-based liability relief sought by industry.

For the second category, NHTSA indicated that it was premature to take a position on the need for liability limiting mechanisms applicable to operators and owners of the SCMS, and that the appropriateness of such liability limiting/risk sharing measures will turn on: (1) the constitution and governance of the SCMS; and (2) the extent to which the primary and secondary insurance markets make insurance coverage available to SCMS entities and other owners and operators of V2V infrastructure.

NHTSA received a number of comments in response. Generally, commenters felt that NHTSA should conduct additional research on liability before proceeding with a V2V mandate, including with respect to the liability of automobile manufactures, owners and operators of the SCMS and V2V communications and security infrastructure, and vehicle owners. While NHTSA will continue to research and analyze potential liability issues stemming from a mandated V2V System, the Agency does not believe that additional research or work with stakeholder and consultants on this issue should delay the rulemaking process or the deployment of this important new safety technology.

Bendix and Cohda agreed with the agency's assessment of liability issues,[321] while other commenters expressed less certainty on the topic and requested that the agency consider liability issues further.

Several commenters stated that additional mechanisms to limit liability are necessary before V2V can be deployed. The National Motorists Association stated that Congress needed to define liability for individual motorists and expressly distribute liability among OEMs, operators, drivers, and other public and private stakeholders.[322] Infineon and Harley-Davidson similarly commented that Federal and/or state liability limitations were necessary prior to V2V rollout.[323] Automotive Safety Council stated that liability should be based on "well-defined performance standards, and should align with other global standards for vehicle safety systems,"[324] while Texas DOT commented more specifically that laws will have to be enacted allowing OEMs to 'mandate' specific operational standards of the cars they sell.[325] Meritor WABCO argued that in order to reduce liability, all involved parties needed to understand that "the V2V system is not a failsafe method to prevent crashes, the V2V system will never be in 100 percent of the motor vehicle population, and that there is a big difference between active safety systems and V2V safety applications."

---

[321] Bendix at 3, Cohda at 12.
[322] National Motorists Association at 1.
[323] Infineon at 5, Harley-Davidson at 2-3.
[324] ASC at 7.
[325] TX DOT at 2.

A number of commenters disagreed with the agency's assessment that V2V-based safety warnings created no additional liability than what already exists for current on-board safety warnings systems.[326] The Alliance argued that V2V-based warnings are different from existing on-board-sensor-based warnings, because their operation depends on input from another manufacturer's vehicle, because V2V is a cooperative technology, and that this changes the nature of "failure to warn" claims.[327] Mr. Dennis provided similar comments.[328] Mercedes-Benz stated more specifically that because V2V systems depend on the "functionality, quality, and timing of signals from surrounding vehicles," failure to warn is no longer solely traceable to onboard sensors of the manufacturer, which will significantly increase the complexity of liability claims.[329] The National Motorists Association offered several specific research topics previously cited also by the VIIC, including (1) whether, and if so, how V2V warning applications increase the risk of liability for OEMs, operators, and drivers; (2) whether owners may be legally accountable for shutting off or failing properly to maintain V2V warning systems; and (3) whether the DVI required for V2V warnings systems will increase driver distraction in a way that could affect liability.[330] The Alliance argued, in summary, that "the traditional paradigm of automotive product liability, in which driver error is presumed to be at fault most of the time, will not apply after V2V and other autonomous technologies become more prevalent."[331] The Alliance also took the position that NHTSA's reliance on a Risk Assessment Report prepared by the Dykema law firm was misplaced because that report assumed that a public or quasi-public entity would run V2V infrastructure when NHTSA itself had assumed that the SCMS would be private.

With regard to the agency's assessment of liability mitigation through insurance, the Alliance argued that it did not believe insurance would necessarily be available to cover entities involved in the SCMS since no data existed yet on which to base underwriting estimates, citing cybersecurity insurance as an example of another area where the insurance industry is unwilling or hesitant to provide insurance.[332] The Alliance and FCA both commented that costs associated with defending against SCMS-related lawsuits could be significant.[333] On whether terms of use could limit liability for V2V, the Alliance further argued that the agency had overlooked "the strong disapproval of liability-limiting clauses in contracts with consumers," and that while such clauses might help in "allocating risk among businesses," the would not work for "limiting liability for negligence that allegedly causes personal injury to a consumer."[334]

---

[326] Alliance at 13, 18-20; CEI at 5; Mr. Dennis at 16; Global at 23; Harley-Davidson at 2; Mercedes-Benz at 9-10.
[327] Alliance at 18
[328] Mr. Dennis at 16.
[329] Mercedes-Benz at 10.
[330] National Motorists Association at 1.
[331] Alliance at 21.
[332] Alliance at 20-21.
[333] Alliance at 31; FCA at2.
[334] Alliance at 20.

Other liability issues raised by commenters included concerns about liability associated with infrastructure. Michigan DOT requested more discussion of liability issues for owners/operators of public RSE infrastructure.[335] Additional potential liability sources cited by commenters included false or inaccurate sensing data,[336] in-vehicle network hacking,[337] and certificate revocation.[338]

It is clear that potential liability stemming from V2V communications is a policy issue of great concern to the automotive industry and certain other stakeholders. It also is true that V2V safety warnings rely on cooperative technology that is different than the technologies deployed in existing on-board safety warnings systems, which do not rely on data received from devices and infrastructure outside of a motor vehicle. The primary policy issues in the OEM context are whether liability related to the V2V System can be addressed by the existing product liability paradigm (i.e., statutory or common law tort principles) – and, if not, whether Congress is willing to change the existing statutory scheme for V2V-related claims in order to support deployment of V2V technology.

The agency has researched, analyzed and continues to grapple with this difficult and potentially quite broad question. We do not, as suggested by some commenters, dismiss the critical importance of potential legal liability to V2V stakeholders. We recognize fully that liability is a potential impediment to deployment of V2V technology. Nevertheless, from a policy perspective, the agency continues to believe that V2V safety warnings should not create liability risks for automobile manufacturers that differ in any meaningful way from risks posed by existing vehicle-based safety warnings systems – and that it is premature to propose or advocate the liability-limiting agendas sought by some stakeholders.

We first address some primary V2V liability risks to automotive manufacturers raised by commenters. We then discuss potential liability risks to owners and operators of SCMS entities, and the extent to which it is appropriate for NHTSA to develop or advocate liability-limiting mechanisms applicable to such providers.

a) Potential Liability Risks to Automobile Manufacturers

Product liability law, which varies from State-to-State, generally concerns the liability of designers, manufacturers and distributors for harm caused to consumers and bystanders by "defective" or "unreasonably dangerous" products. [339] The purpose of these laws is:

---

[335] Alliance at 19; MI DOT at 3.
[336] Rene Struik at 2.
[337] Systems Research Associates at 9.
[338] Alliance at 56.
[339] Dykema at 9-10.

> … to ensure that the costs of injuries resulting from defective products are borne by those who placed the defective products in the market, rather than the injured person. Thus, in an effort to encourage the development of safer products, the responsibility for the injuries caused by defective products is placed on those who are in the best position to guard against defects and warn of their potential dangers.[340]

There is a broad range of product liability theories and defenses that could be applicable to liability litigation involving the V2V System. For purposes of this discussion, we focus on the product liability theory of "failure to warn," which the Alliance, Mr. Dennis, and Mercedes Benz raised in their respective comments. A "failure to warn" claim is based on the theory that even a properly designed and manufactured product may be defective as a result of its manufacturer's failure to warn consumers of any dangerous characteristics in its product about which it knows or should know and which the user of the product would not ordinarily discover.[341] There are four basic elements of a "failure to warn" claim:

1. The manufacturer knew or should have known of the risks inherent in the product;
2. There was no warning, or the warning provided was inadequate;
3. The absence of a warning made the product unreasonably dangerous; and
4. The failure to warn was the cause-in-fact or proximate cause of the plaintiff's injury.[342]

To avoid liability for failure to warn, a product's instructions or warnings must sufficiently alert the user to the possibility of danger. [343]

The Alliance, Mr. Dennis, and Mercedes-Benz all took the position that the cooperative nature of V2V safety warnings and the external data sources on which V2V warnings are based change the fundamental nature of "failure to warn" claims and make them more complex.[344] It is possible -- perhaps even likely -- that the factual inquiry underlying a failure to warn claim will be more complex in the context of a V2V System than it would be in the context of a vehicle-based warning system. Additionally, not just message quality and timing (as noted by Mercedes-Benz), but a vehicle's operating environment (roadway, topographic and environmental factors) may adversely affect the performance of a consumer's V2V System. For these reasons, manufacturers' consumer warnings and instructions will be particularly critical to the successful defense of V2V failure claims. As they have done in the context of new safety technologies such as lane-departure warning, backover-detection warnings and forward vehicle detection systems, manufacturers will need to carefully describe the operation and limitations of V2V and V2I

---

[340] Dykema at 9-10.
[341] Dykema at 13.
[342] Dykema at 13.
[343] Dykema at 13.
[344] Alliance at 18.

Systems in the safety context and in the foreseeable operating environment.[345] NHTSA expects that, by appropriately warning consumers of the uses and limitations of their V2V System, automobile manufacturers can sufficiently limit their liability for failure to warn claims, despite operational differences between on-board and V2V safety warning technologies.

In the context of V2V OBE failure claims, it also may be quite difficult for consumers to prove that a vehicle's V2V equipment caused or contributed to an accident. However, to the extent that the V2V communications proposed in this rule are used as a warning system, not a control system, then, as with existing vehicle-based warning systems, the V2V System is an aid to help drivers safely operate their vehicles. As discussed in varying places in this NPRM and the accompanying PRIA, at this time, NHTSA does not assume that V2V communications will be used as the sole basis for any safety system that exercises actual control of the vehicle. Thus, we assume that any liability concerns related to safety systems that do take control of the vehicle will not be affected by the presence of V2V.

In its comment, the Alliance stated that "conclusions about the applicability of the state of the law with respect to traditional failure to warn claims involving on-board warning technologies grossly oversimplifies the way such claims are likely to evolve in the V2X litigation. "[346] We agree that it is difficult for NHTSA (or anyone) to know exactly how products liability litigation will evolve in the context of V2V, V2I and V2X communications. However, NHTSA's assessment of potential V2V liability to date has been based, in part, on risk analyses conducted by Dykema PLLC. Dykema is a Detroit-based law firm that specializes in automotive-related legal issues and provides legal services to many major automobile manufacturers. It is also the firm that the VIIC selected as its subcontractor to analyze and report on, among other legal policy topics, potential V2V-related liability risks to automobile manufacturers and public sector entities under a cooperative agreement with DOT. That said, the agency welcomes and will carefully consider the content of submissions of other legally substantive risk analyses in response to its proposal. NHTSA received no such analyses in response to the Readiness Report and ANPRM, including from the Alliance or any foreign or domestic automobile manufacturers.

On a related note, the Alliance commented that NHTSA's reliance on Dykema's OEM Risk Assessment Report is misplaced, as that report assumes that a public or quasi-public entity will run V2V infrastructure when NHTSA assumes that the SCMS will be private. NHTSA respectfully disagrees with the Alliance on this point. Dykema's OEM Report contains no assumptions, explicit or implied, that would limit the utility or applicability of its analysis of OEM risk for V2V-related product liability claims. Additionally, with respect to infrastructure-based liability claims, the report specifically notes, without limitation and without referencing public ownership of such infrastructure, that "[a]lthough the structure of VII described herein

---

[345] Dykema at 35.
[346] Alliance at 8.

focuses on a hypothetical DSRC-enabled system, the analysis and conclusions in this deliverable generally will apply to any VII network that communicates information V2V or V2I."[347]

Dykema's OEM Report also notes that a lawsuit might allege that a crash was caused, in whole or in part, by a failure in the communications infrastructure supporting V2V (e.g., an RSE). However, as evidenced by the numerous lawsuits claiming that failure of a traffic light contributed to an accident, such cases typically are brought against public or quasi-public entities and not against vehicle manufacturers.[348] For this reason, Dykema concluded (and NHTSA agrees) that "we would not expect alleged failures in V2V infrastructure to impact OEM liability in a significant way."[349]

b) Potential Liability Risks to SCMS Owners and Operators

From NHTSA's perspective, the critical policy issues in the SCMS context are whether concerns about liability will be a stumbling block to creation and operation of a private SCMS – and, if so, whether a need exists for DOT to work with stakeholders to develop Federal liability-limiting options that would incentivize private participation in a National SCMS.

In the Readiness Report (as in Proposal A in this document), NHTSA focused on a private model of SCMS governance that did not involve Federal funds or liability protections -- but instead functioned through industry self-governance by an SCMS Manager that would work with SCMS entities to determine the appropriate distribution of liability for harm and establish minimum insurance requirements. In response, commenters such as the Alliance took the position that private insurance would not necessarily be available to cover entities involved in the SCMS since no claims data existed yet on which to base underwriting estimates, citing cybersecurity insurance as an example of another area where the insurance industry has been unwilling or hesitant to provide insurance.

The agency acknowledges that SCMS entities may not be able to obtain adequate liability insurance without Federal intervention of some sort – but it is simply too early to tell. As we noted in the Readiness Report, the extent to which the primary and secondary insurance markets will make insurance coverage available to SCMS entities will be a factor in whether DOT supports development of liability-limiting mechanism to incentivize private SCMS participants. To this end, the agency expects that the issue of liability as a potential impediment to the establishment of a National SCMS will be among the issues that NHTSA and V2V stakeholders continue to grapple with going forward – and one that DOT's planned PKI and organizational policy research will explore fully (including through consultations with the insurance and reinsurance industries). However, due to the lack of substantive evidence that the private

[347] Dykema at 4.
[348] Dykema at 33.
[349] Dykema at 33.

insurance market is unwilling to underwrite SCMS risks, NHTSA continues to believe that it is premature to take a position on the need to develop and advocate for Federal liability-limiting mechanisms for a National SCMS.

The agency also is of the view that potential liability based on failures in the SCMS may be limited substantially by lack of causation due to drivers' roles in failing to avoid crashes. However, NHTSA wishes to clarify a comment in the Readiness Report relating to limitations on consumer liability – specifically, the statement that:

> It also is not clear to the agency why an SCMS Manager could not require that individuals and entities participating in an SCMS to agree to terms of use that would limit the liability of the SCMS and its component entities, either explicitly or via the same type of instructions and explanations of system limitations that the OEMs would use to limit liability. [350]

In its comment, the Alliance noted that NHTSA appeared to be promoting the use of liability limitations in terms of use agreements with consumers, which can be legally problematic and, generally, are disfavored by courts.[351] To clarify, NHTSA does not sanction the use coercive liability limitation provisions in agreements between SCMS entities and consumers. As the Alliance noted "such clauses can be effective in allocating risk among businesses" and the application of such clauses should be limited to entities doing business with SCMS components, not consumers.

VII. Estimated Costs and Benefits

A. General Approach to Costs and Benefits Estimates

In this NPRM, the agency proposes that all light vehicles be equipped with technology that allows for V2V communications. The agency believes that this technology will facilitate the "free-market" development of various applications; both safety and non-safety related that would not be possible without a network of devices "talking" to each other.

However, at this time, the agency has decided to mandate V2V technology, but not mandate any specific applications. The agency believes this is the appropriate course for several reasons. First and foremost being that the agency believes V2V communication's cooperative nature needs a government mandate as the "spark" to establish a shared "open" platform that can be utilized to move this technology into the mainstream while not stifling potential, unforeseen innovations. In addition, the agency does not currently possess sufficient information to mandate

[350] Readiness Report at 214.
[351] Alliance, Attachment B at 3.

particular safety applications, although, throughout this NPRM, we request additional information that could inform a potential decision to mandate certain applications.

This free-market approach to app development and deployment, though, makes estimating the potential benefits of V2V quite difficult. In a traditional NHTSA analysis of a safety technology, the agency would determine benefits by looking to the target population for the type of crash it is trying to avoid or mitigate and the effectiveness of the mandated performance requirement or safety technology in addressing those crashes. However, here, the technology being mandated by the agency, V2V communication, would only indirectly create safety benefits. Widespread adoption of V2V would facilitate the development of new safety applications that would not be possible otherwise, as well as help improve the performance of safety applications that already exist based on cameras or sensors. Further, V2V technology is expected to speed-up the deployment of various V2I technologies, which could have significant safety and congestion-relief applications.

The agency is confident that these technologies will be developed and deployed once V2V communications are mandated. The difficulty, though, is that the agency does not currently have sufficient information to definitively predict how or when this will occur. Thus, the agency has projected an adoption period based upon research conducted on the deployment of other advanced technologies as well as other information obtained during the development of this proposed rule. In addition, the agency demonstrates the potential safety benefits by analyzing two safety applications, IMA and LTA, both of which the agency believes are likely to lead to significant safety benefits that are likely only possible using V2V technology. The agency has therefore not quantified any benefits attributable to the range of other potential uses of V2V, although we acknowledge that such uses are likely to exist. The agency believes that, by focusing on only two of the many potential uses of V2V technology and given our experience with other technologies;, we have taken a reasonable approach in estimating the potential benefits of the proposed rule and have likely understated the. The agency, though, requests comments on these assumptions to better inform the analysis that would support a final rule. Is there more detailed information concerning manufacturer's plans to introduce safety impacts associated with widespread adoption of V2V technology applications? If so, what applications and on what timeline?

B. Quantified Costs

The agency was able to use information obtained from the V2V Readiness Report in developing the cost estimates in this proposal. Where appropriate, the V2V Readiness Report cost estimates were adjusted to align with any new information obtained by the agency such as: that provided through comments to the V2V ANPRM, experience from the SCMS RFI activity, and by developing the proposed performance requirements.

The costs and benefits are presented in two measures: annual and by model year (MY) vehicles (MY costs). The annual costs represent the yearly financial commitment while the MY costs represent the total investment born by the indicated MY vehicle, plus the lifetime fuel economy impact from those vehicles. In either accounting measure, the vehicle equipment,

communication, and SCMS costs are assumed to be paid by new vehicle owners when their vehicles were purchased. The only difference between the two cost measures is the calculation of any potential fuel economy impact. The annual fuel economy impact measures the collective fuel impact from all V2V-equipped vehicles for a specific calendar year. In contrast, the lifetime fuel economy impact measures the fuel impact specifically for a MY vehicle through its operational life. All cost estimates are adjusted for 2014 dollars.

For this analysis, the agency is considering two potential technology implementation approaches that could meet the safety, security, and privacy specifications of the proposed rule. These two approaches are (1) utilizing one DSRC radio dedicated to V2V safety communications paired with secondary cellular, Wi-Fi, or Satellite communications ("one-radio" approach) and (2) utilizing two DSRC radios, one dedicated to V2V safety communications and one used for secondary communications such as SCMS or other "back office" type communications (two-radio approach). As a result, both the annual and MY costs are presented as a range which covers the costs from these two approaches.

The following sections describe the four parts of quantified costs, followed by the summary of the total quantified costs and non-quantified costs, and estimated cost per vehicle. This normalized per vehicle cost allows a straightforward comparison between various technology approaches and regulatory alternatives. All costs were estimated under the DSRC and app sales scenario specified in the Estimated Benefits portion of this chapter – Section VII.D.

1. Component Costs

a) Unit costs to OEMS

As shown in Table VII-1, the total direct component costs to OEMs were estimated to be $162.77 for one DSRC radio and $229.91 for two radios. The total weight of one DSRC radio is approximately 2.91 lbs. whereas the weight of two radios is slightly heavier, about 3.23 lbs. For the two-radio approach, as previously discussed, two DSRC antennas are necessary: The first DSRC radio sends and receives the BSM, and the second radio handles security aspects of receiving certificates, the certificate revocation list, etc. We estimated that the second radio will be $10.33[352] cheaper than the first radio since these two radios would most likely be packaged together, thereby resulting in lower labor costs in assembling the combined package at the supplier, as well as lower hardware costs in packaging them together rather than individually. Therefore, the cost for two radios would be $134.29 (=$72.31 * 2 – $10.33) instead of $144.64 (=$72.32 *2), as shown in Table VII-1. No such assumption was made for the antenna, since the antennas have to remain physically separate in order to avoid interfering with each other.

[352] Adjusted from the $10 in 2011 dollars that was estimated in the ANPRM

Table VII-1 Estimated Component Unit Weight and Costs to OEMs

Component	Costs	One Radio		Two Radios	
	(2012 $)	Weight (lbs)	Costs (2014 $)	Weight (lbs)	Costs (2014 $)
DSRC Transmitter/Receiver	$70	0.55	$72.31	0.65	$134.29
DSRC Antenna	$5	0.22	$5.17	0.44	$10.33
Electronic Control Unit	$45	0.55	$46.49	0.55	$46.49
GPS	$14		$14.46		$14.46
GPS Antenna	$4	0.22	$4.13	0.22	$4.13
Wiring	$9	1.20	$9.30	1.20	$9.30
Displays	$4.79	0.17	$4.95	0.17	$4.95
HSM		0.00	$4.65	0.00	$4.65
For 2 Apps		0.00	$1.32	0.00	$1.32
Total	$151.79	2.91	$162.77	3.23	$229.91

Overall, for this analysis the vehicle equipment costs are based on an OEM integrated device built into vehicles during their manufacture. This example device includes the costs of DSRC radios, DSRC antenna, GPS, HSM, and installation of relevant equipment (DSRC radios in short) and loaded with two safety applications. With specific regard to the safety applications, the app costs include software engineering and development costs since the agency is not assuming any additional interface beyond the DVI or equipment costs for the apps. The software engineering and development costs will be shared by millions vehicles, and thus is expected to be minimal across the fleet. The OEM integrated device is used as a basis for cost estimation as this device type provides a more accurate cost expectation associated with finalizing this proposal.

The agency also estimated potential costs for aftermarket devices that could enter the marketplace as a result of finalizing this proposal and enabling more consumers to benefit from V2V technology. As described elsewhere, aftermarket devices could be available in three distinct varieties: retrofit, standalone, and a simple awareness device. The agency estimates that the three aftermarket device types would cost $400.28 for a retrofit device; $278.33 for a standalone device, and $101.74 for a simple awareness device.

b) Consumer Costs

The costs in Table VII-2 reflect the costs that OEMs pay to a component (Tier 1) supplier to purchase these components for the vehicles they manufacture, not the projected cost of these systems to consumers. To obtain the consumer costs, each variable cost is multiplied by 1.51 (i.e., 51 percent makeup) to estimate a retail price equivalent (RPE; i.e., consumer cost). The 51 percent markup represents fixed costs (research and development, selling and administrative costs, etc.), as well as OEM profits, transportation costs, and dealer costs and profits. Table VII-2 presents the component consumer costs. As shown, the total component costs to consumers were estimated to be $245.79 for one radio and $347.18 for two radios.

Table VII-2 Estimated Component Consumer Unit Costs (2014 $)

Component	One Radio	Two Radios
DSRC Transmitter/Receiver	$109.19	$202.78
DSRC Antenna	$7.80	$15.60
Electronic Control Unit	$70.19	$70.19
GPS	$21.84	$21.84
GPS Antenna	$6.24	$6.24
Wiring	$14.04	$14.04
Displays	$7.47	$7.47
HSM	$7.02	$7.02
Two Safety Applications	$2.00	$2.00
Total	$245.79	$347.18

c) Installation costs

Component installation costs are primarily attributable to the labor needed to perform the installation, but the agency also accounts for potential, additional costs associated with materials used in the installation such as minor attachments brackets, or plastic tie downs to secure wires, etc. In Table VII-3, the installation costs are separated into "Material Costs" (for the minor attachments), "Labor Costs," and "Variable Burden" (i.e., other costs that are not direct labor or direct material used in the part, but are costs that vary with the level of production, such as set-up costs, in-bound freight, perishable production tools, and electricity). Overall, the agency estimates the variable cost to OEMs to install the V2V equipment is $11.79 per vehicle and the cost to consumers will be $17.80 using a 1.51 retail price equivalent factor (e.g. markup).

Table VII-3 Consumer Installation Cost Estimates (2014 dollars)

Part	Material Cost	Labor Cost	Variable Burden	Total Variable	Total Consumer Cost
DSRC Transmitter/Receiver	0.04	1.61	1.04	2.69	4.06
DSRC Antenna	0.04	0.10	0.07	0.21	0.31
Electronic Control Unit	0.02	1.84	1.19	3.05	4.60
GPS	0.04	0.10	0.07	0.21	0.31
GPS Antenna	0.04	0.10	0.07	0.21	0.31
Wiring	0.19	0.93	0.60	1.72	2.59
LEDs (5) Displays + Malfunction	0.00	0.63	0.40	1.03	1.56
Light Bar	0.04	1.61	1.04	2.69	4.06
HSM	0.00	0.00	0.00	0.00	0.00
Total	0.38	6.92	4.48	11.79	17.80

d) Adjustment for GPS Installation

When researching installation costs, the agency identified the need to make adjustments for GPS installation. Today, many vehicles are already equipped with GPS receivers and the percentage equipped as standard installation is likely to increase going forward. The agency

estimates approximately 43 percent of MY 2013 light vehicles were equipped with GPS receivers.[353] This percentage increases to approximately 50 percent when combined with the number of vehicles equipped with automatic collision notification (ACN). Current information available to the agency indicates that navigation-grade GPS units are sufficient for the V2V safety applications. In these cases, the GPS component is not a cost that is directly attributable to V2V. Overall, 50 percent of applicable vehicles would not incur costs to add GPS for V2V technology. Thus, the total cost associated with vehicles equipped with GPS (i.e., 50%) was subtracted from the total costs of equipping all applicable vehicles with V2V safety applications.

e) Summary of Component Costs

Table VII-4 summarizes consumer costs for original equipment manufacturers (OEMs) for the first year of equipping a vehicle with V2V components. The consumer unit cost is estimated to be $249.19 for one radio and $350.57 for two radios in 2014 dollars.

Table VII-4 Summary of V2V Component Consumer Costs per Affected Vehicle

Cost	**One Radio**		**Two-Radios**	
Items	Weight (lb.)	Consumer Costs	Weight (lb.)	Consumer Costs
Parts*	2.91	$245.79	3.23	$347.18
Installation	0.26	$17.74	0.26	$17.74
Subtotal	3.17	$263.53	3.49	$364.92
Minus Current GPS Installation**	0.11	$14.35	0.11	$14.35
Total	3.06	$249.18	3.38	$350.57

*including app software costs
** taking into account the 50 percent GPS installation rate

f) Learning Curve Effect

As manufacturers gain experience through production of the same product, they refine production techniques, better manage raw material and component sources, and assembly methods to maximize efficiency and thus reduce production unit costs. Learning curves reflect the impact of experience and volume on the cost of production and are especially evident when a completely new product is introduced to the marketplace. V2V systems are expected to be installed on a growing portion of the vehicle fleet as manufacturers ramp up to the meet the proposed rule which would require 100% new vehicle installation by 2023, which is projected to be over 16 million units annually. This large scale production provides manufacturers with opportunities to reduce system costs through the learning process. Additional information on the

[353] Ward's Automotive Yearbook 2014, based on vehicles with factory-installed navigation systems or concierge systems

agency's learning curve development and the derivation for learning curves related to V2V are detailed in Chapter 7 of the PRIA that accompanies this proposed rule.

NHTSA routinely performs evaluations of the costs and benefits of safety standards that were previously issued in an effort to estimate learning curve impacts, among other economic impacts, and provide the most accurate possible information at the time a rule is proposed and finalized. To estimate costs, the agency conducts a teardown study of the technologies used to meet the standards. In some cases, the agency has performed multiple evaluations over a span of years. For example, a teardown study may be performed to support the agency's initial estimates of costs that will result from the regulation, and again five years later to evaluate the impacts of the regulation after it has been in effect. These data, together with actual production data, supply the necessary information required to develop a learning curve for the technology.

For V2V, the agency estimates that learning would reduce the unit cost for two radio implementations, including two safety applications, from approximately $350.57 in 2021 to $218.85 in 2060, which is about 62.5 percent. Applying the same learning pattern, the unit cost for a one radio system would decrease it from $249.18 in 2021 to $155.47 in 2060. Details of how learning would affect unit costs for both one to two radio implementations can be found in Table VII-5.

Table VII-5 Annual Progress Rates and Component Unit Costs After Learning

	Calendar	Progress Rates		Unit Costs			Total Unit Costs	
Year	Year	Radio	Apps	1 Radio	2 Radio	Apps	1 Radio	2 Radios
1	2021	1.000	1.000	$247.18	$348.57	$2.00	$249.18	$350.57
2	2022	0.908	1.000	$224.44	$316.50	$2.00	$226.44	$318.50
3	2023	0.853	0.872	$210.95	$297.47	$1.74	$212.69	$299.22
4	2024	0.821	0.782	$202.91	$286.14	$1.56	$204.47	$287.70
5	2025	0.798	0.726	$197.21	$278.10	$1.45	$198.66	$279.56
6	2026	0.780	0.681	$192.83	$271.93	$1.36	$194.19	$273.29
7	2027	0.766	0.647	$189.27	$266.91	$1.29	$190.57	$268.21
8	2028	0.754	0.623	$186.28	$262.69	$1.25	$187.53	$263.94
9	2029	0.743	0.606	$183.71	$259.07	$1.21	$184.92	$260.28
10	2030	0.734	0.593	$181.45	$255.88	$1.19	$182.63	$257.06
11	2031	0.726	0.582	$179.44	$253.04	$1.16	$180.60	$254.20
12	2032	0.719	0.573	$177.62	$250.48	$1.15	$178.77	$251.63
13	2033	0.712	0.565	$175.98	$248.16	$1.13	$177.11	$249.29
14	2034	0.706	0.558	$174.47	$246.03	$1.12	$175.58	$247.15
15	2035	0.700	0.552	$173.07	$244.06	$1.10	$174.17	$245.17
16	2036	0.695	0.546	$171.77	$242.23	$1.09	$172.87	$243.32
17	2037	0.690	0.541	$170.56	$240.52	$1.08	$171.64	$241.60
18	2038	0.685	0.537	$169.42	$238.92	$1.07	$170.49	$239.99
19	2039	0.681	0.532	$168.35	$237.40	$1.06	$169.41	$238.47
20	2040	0.677	0.528	$167.33	$235.97	$1.06	$168.39	$237.03
21	2041	0.673	0.525	$166.37	$234.61	$1.05	$167.42	$235.66
22	2042	0.669	0.521	$165.48	$233.36	$1.04	$166.52	$234.40

23	2043	0.666	0.518	$164.64	$232.17	$1.04	$165.68	$233.21
24	2044	0.663	0.515	$163.84	$231.04	$1.03	$164.87	$232.07
25	2045	0.660	0.512	$163.07	$229.96	$1.02	$164.09	$230.98
26	2046	0.657	0.509	$162.33	$228.92	$1.02	$163.35	$229.94
27	2047	0.654	0.507	$161.63	$227.93	$1.01	$162.64	$228.94
28	2048	0.651	0.504	$160.95	$226.97	$1.01	$161.96	$227.98
29	2049	0.649	0.502	$160.30	$226.05	$1.00	$161.30	$227.05
30	2050	0.646	0.500	$159.67	$225.16	$1.00	$160.67	$226.16
31	2051	0.644	0.498	$159.07	$224.31	$1.00	$160.06	$225.31
32	2052	0.641	0.496	$158.48	$223.49	$0.99	$159.48	$224.48
33	2053	0.639	0.494	$157.93	$222.70	$0.99	$158.91	$223.69
34	2054	0.637	0.492	$157.39	$221.94	$0.98	$158.37	$222.93
35	2055	0.635	0.490	$156.87	$221.21	$0.98	$157.85	$222.19
36	2056	0.633	0.488	$156.36	$220.50	$0.98	$157.34	$221.48
37	2057	0.631	0.486	$155.88	$219.82	$0.97	$156.85	$220.79
38	2058	0.629	0.485	$155.41	$219.15	$0.97	$156.38	$220.12
39	2059	0.627	0.483	$154.95	$218.51	$0.97	$155.92	$219.48
40	2060	0.625	0.482	$154.51	$217.89	$0.96	$155.47	$218.85

Table VII-6 summarizes the total annual vehicle component costs. As shown, total annual vehicle component costs would range from $2.0 billion to $4.9 billion. The cost per vehicle would range from $123.59 to $297.65. The lower bound is for one radio at year 2021 and the higher bound is the cost for two radios in 2023. In 2023, 100 percent of vehicles would be required to be equipped with the DSRC radios and more vehicles would be expected to have apps. Although the projected number of new vehicles that would have DSRC radios and safety applications continues to increase after 2023, the additional costs are offset by the falling component costs.

g) Annual Component Costs

In

Table VII-6 presented below the cost per vehicle is the average cost spread across all new vehicles, not just affected vehicles. Due to the proposed phase-in schedule, the cost per vehicle in 2021 and 2022 is significantly lower than the unit cost shown in Table VII-5. Furthermore, the agency predicts complete safety application deployment would not be achieved until 2028, resulting in a slightly lower cost per vehicle for 2023 to 2027 than that shown in Table VII-2.

Table VII-6 Total Annual Vehicle Component Costs (2014 $ and Vehicles in Millions)

Year	Calendar Year	Vehicles With		Total Costs (Radios + Apps)		Cost Per Vehicle	
		Radios	Apps	1 Radio	2 Radios	1 Radio	2 Radios
1	2021	8.10	0.00	$2,000.92	$2,821.67	$123.59	$174.29
2	2022	12.26	0.61	$2,751.72	$3,879.94	$168.40	$237.45
3	2023	16.44	1.64	$3,470.84	$4,893.35	$211.12	$297.65
4	2024	16.53	4.13	$3,360.54	$4,736.34	$203.30	$286.53
5	2025	16.67	6.67	$3,297.19	$4,645.68	$197.79	$278.68
6	2026	16.75	10.89	$3,244.74	$4,569.60	$193.72	$272.81
7	2027	16.88	15.19	$3,214.60	$4,525.12	$190.44	$268.08
8	2028	17.03	17.03	$3,193.60	$4,494.87	$187.53	$263.94
9	2029	17.13	17.13	$3,167.72	$4,458.56	$184.92	$260.28
10	2030	17.30	17.30	$3,159.58	$4,447.19	$182.63	$257.06
11	2031	17.44	17.44	$3,149.66	$4,433.29	$180.60	$254.20
12	2032	17.56	17.56	$3,139.20	$4,418.61	$178.77	$251.63
13	2033	17.67	17.67	$3,129.51	$4,405.01	$177.11	$249.29
14	2034	17.84	17.84	$3,132.41	$4,409.12	$175.58	$247.15
15	2035	18.00	18.00	$3,135.14	$4,412.99	$174.17	$245.17
16	2036	18.16	18.16	$3,139.24	$4,418.78	$172.87	$243.32
17	2037	18.34	18.34	$3,147.91	$4,431.00	$171.64	$241.60
18	2038	18.49	18.49	$3,152.45	$4,437.40	$170.49	$239.99
19	2039	18.66	18.66	$3,161.27	$4,449.84	$169.41	$238.47
20	2040	18.87	18.87	$3,177.54	$4,472.75	$168.39	$237.03
21	2041	19.14	19.14	$3,204.34	$4,510.49	$167.42	$235.66
22	2042	18.56	18.56	$3,090.70	$4,350.52	$166.52	$234.40
23	2043	18.66	18.66	$3,091.52	$4,351.69	$165.68	$233.21
24	2044	18.76	18.76	$3,092.91	$4,353.66	$164.87	$232.07
25	2045	18.87	18.87	$3,096.45	$4,358.65	$164.09	$230.98
26	2046	18.97	18.97	$3,098.81	$4,361.98	$163.35	$229.94
27	2047	19.08	19.08	$3,103.22	$4,368.19	$162.64	$228.94
28	2048	19.18	19.18	$3,106.39	$4,372.65	$161.96	$227.98
29	2049	19.28	19.28	$3,109.91	$4,377.61	$161.30	$227.05
30	2050	19.39	19.39	$3,115.37	$4,385.30	$160.67	$226.16
31	2051	19.39	19.39	$3,103.57	$4,368.70	$160.06	$225.31
32	2052	19.39	19.39	$3,092.23	$4,352.74	$159.48	$224.48
33	2053	19.39	19.39	$3,081.32	$4,337.38	$158.91	$223.69
34	2054	19.39	19.39	$3,070.79	$4,322.57	$158.37	$222.93
35	2055	19.39	19.39	$3,060.63	$4,308.27	$157.85	$222.19
36	2056	19.39	19.39	$3,050.82	$4,294.46	$157.34	$221.48
37	2057	19.39	19.39	$3,041.33	$4,281.11	$156.85	$220.79
38	2058	19.39	19.39	$3,032.14	$4,268.17	$156.38	$220.12
39	2059	19.39	19.39	$3,023.24	$4,255.64	$155.92	$219.48
40	2060	19.39	19.39	$3,014.60	$4,243.49	$155.47	$218.85

2. Communication Costs

a) Methodology

The communication cost estimates are based on the same model created by Booz Allen Hamilton under the contract with the DOT's Intelligent Transportation Systems Joint Program and used for the V2V Readiness Report. The model, Cost Model for Communications Data Delivery System (CDDS), is a Microsoft Excel-based model.[354]

The communication cost estimates include the cost of in-vehicle communication components and any service fee that would be required with a specific communication network. For system design, four communication network technologies were evaluated for the CDDS: cellular, Wi-Fi, Satellite, and DSRC. The four technologies can be combined in various ways to form the communication system to support the vehicle to SCMS communication activities. The CDDS report and various cost estimates were published in the V2V Readiness Report and referenced specifically in the ANPRM in an effort to gather feedback on the estimated costs.

In response to the V2V ANPRM, and the Request for Interest (RFI) regarding the SCMS, the agency received information and feedback on cellular and satellite and how these technologies can support national V2V deployment.[355] These new findings led the agency to conclude that two systems can meet the proposed security requirements:

- Hybrid - This system would use cellular, Wi-Fi, and satellite for vehicles to SCMS communication.
- DSRC - This protocol would use DSRC exclusively for V2V communications and for vehicles to SCMS communications through Roadside Equipment (RSE).

The hybrid system allows for the potential use of the three communication mediums cellular, Wi-Fi, and satellite. Each serves as a complement system to the other. In an effort to address potential security concerns, the agency added the cost of an in-vehicle hardware security module (HSM). The HSM, based on agency conversations with security experts, can potentially address the over-the -air communication security issues. Furthermore, the agency also recognized that satellite communication will not be as expensive as detailed in the BAH' estimates since 70 percent of light vehicles are currently equipped satellite radio receivers. Since only 30 percent of vehicles will need satellite radio receivers reduces the overall component cost for satellite communication in reduced increasing its viability.

A DSRC-exclusive system would communicate with SCMS through RSUs, small "base stations" that allow vehicles to "phone home" using DSRC. A separate DSRC antenna will be

[354] Docket No. NHTSA-2014-0022
[355] Docket No. NHTSA-2014-0023

used exclusively for communicating updates ensuring continual "listening" for safety component update related communications,. This dedicated DSRC communication channel would exist in addition to the dedicated V2V safety communications channel used for V2V safety communications, and, therefore, two DSRC radios would be required for this DSRC-exclusive communication system.

BAH estimated the potential number of RSUs needed to support a national deployment. First, RSU deployment was considered on three different road types: secondary roads, interstate highways, and National Highway System roads (NHS). Each type is defined by BAH as the following:[356]

- Secondary roads refer to collector roads, State highways, and county highways that connect smaller towns, subdivisions, and neighborhoods.
- Interstate highways are the network of freeways that make up Dwight D. Eisenhower National System of Interstate and Defense Highways.
- The NHS roads are the collection of interstate highways, principal arteries, strategic highways, major network connectors, and intermodal connectors.

BAH then used spatial optimization and information from the 2009 National Household Transportation Survey (NHTS) to estimate the required number of RSE to achieve the desired amount of coverage. The usage of NHS roads (with 19,749 sites) was deemed the most logical because it achieves greater coverage than the interstate option (with 8,880 sites) while also requiring fewer RSE than secondary roads (with 149,434 sites) to achieve the same coverage, as shown below in Figure VII-1. As shown, NHS roads are the most realistic scenario, though secondary roads could achieve more coverage given more resources. Ultimately, the NHS road deployment method was deemed to be the most realistic.

[356] BAH CDDS Final Report, at 27. See Docket No. NHTSA-2014-0022

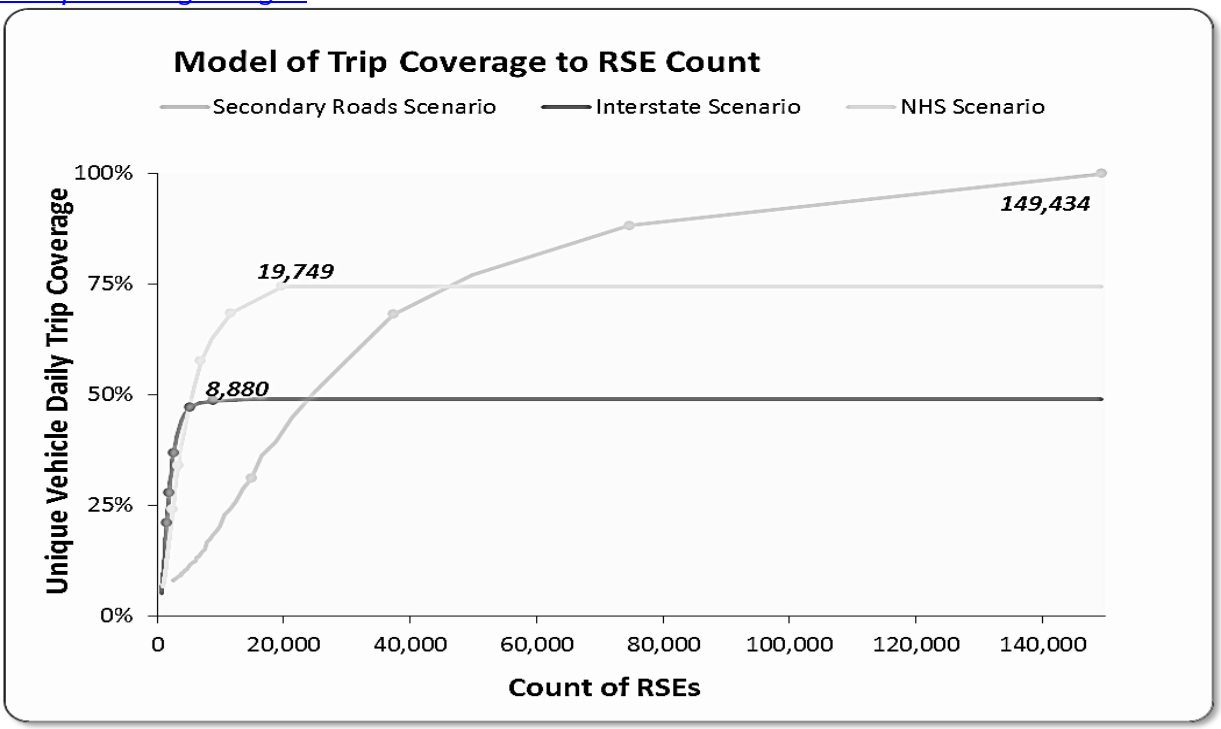

Figure VII-1 Coverage of RSE by Road Type

b) Assumptions

The agency applied the assumptions used in the CDDS model to estimate communication costs. These comprehensive assumptions included the length of initial new certificate deployment period, the certificate download size and frequency at the full system deployment, the potential device misbehavior rate, and the potential size of a certificate revocation list. The cost model also considered the costs that relate to the three communication technologies used in the Hybrid approach: cellular data rate, cellular component cost in the vehicles, Wi-Fi component costs, satellite data rate, and satellite radio cost. It is also necessary to consider the cost of road side units for the DSRC-exclusive approach system. The agency notes that while not included in these estimates, there is potential for road side unit costs to not be borne solely by a V2V system. Road side units may also be deployed in accordance with guidance from the Federal Highway Administration (FHWA) as signaling and related traffic control equipment undergoes normal upgrades. Overall, unless otherwise stated, all cost calculations have been made with the assumptions found in Table VII-7 and are estimated for over a 40 year timeframe. Additional details on the communication cost assumptions can be found the Chapter VII of the PRIA. The agency requests comment on these assumptions.

Table VII-7 Cost Assumptions by Communication Options

Cost Factors	Component	Hybrid	DSRC
Certificate			

	Certificate Option	3000 per bundle	3000 per bundle
	Certificate Phase-In Period	3 years	3 years
	Certificate Download Frequency at Full Deployment	Every 3 years	Every 3 years
Misbehavior			
	Misbehavior Rate	0.10%	0.10%
	CRL Type	Satellite/Incremental	Incremental
Communication Technology			
Cellular	Cellular Data Price	$4.00 / GB	NA
	Cellular Component Cost Per Vehicle	$10.00	NA
	Fraction of Data Shifted from Cellular	67%	NA
Wi-Fi	Wi-Fi Component Cost per Vehicle	$2.00	NA
Satellite	Satellite Data Price	$1.60 /GB	NA
	Satellite Component Cost per Vehicle	$6.00	NA
Three Above Combined	Annual Technology Component Replacement Rate	2%	NA
RSE	RSE Component per Vehicle	NA	Included in the DSRC radios
	# Nationwide RSEs	NA	19,750
	RSE Structure Supporting Cost	NA	$8,839
	RSE Replacement Cost	NA	$22,719
	RSE Installation Phase-in	16 Year	NA
	RSE Life	NA	15 years

c) Hybrid Option Costs

The agency estimates the annual overall costs for the Hybrid communication option would range from approximately $148 million in Year 1 to approximately $490 million at Year 40. On a per vehicle basis, this equates to $9.18 in Year 1 to $25.47 after 40 years. The detailed estimated annual communication costs are shown in Table VII-8. The cost increase over time represents the increases in certificate distributions and SCMS communications as fleet penetration increases.

It is important to note the table reflects zero satellite and cellular data costs for the first three years. This zero cost results from the assumption that vehicles will be pre-loaded with three years of security certificates, reflecting that communication between vehicles and SCMS will be very limited during this time period. In addition, the acknowledged certificate revocations lists would be transmitted to vehicles during this time but, overall, the estimated misbehavior rate of 0.1 percent, combined with an anticipated, small revocation list size, would not have a substantive impact on communication costs.

Table VII-8 Estimated Annual Communication Costs and Per Vehicle Costs - Hybrid

	Calendar			Data Cost			Cost Per
Year	Year	RSE	OBE	Satellite	Cellular	Total	Vehicle
1	2021	$0	$148,624,200	$0	$0	$148,624,200	$9.18
2	2022	$0	$213,159,926	$0	$0	$213,159,926	$13.05
3	2023	$0	$309,000,919	$0	$0	$309,000,919	$18.80
4	2024	$0	$316,361,705	$14,502	$5,964,604	$322,340,811	$19.50
5	2025	$0	$324,585,446	$20,225	$7,771,778	$332,377,450	$19.94
6	2026	$0	$331,663,749	$26,516	$9,558,220	$341,248,485	$20.37
7	2027	$0	$339,583,781	$33,316	$11,326,199	$350,943,297	$20.79
8	2028	$0	$347,798,557	$41,044	$13,073,502	$360,913,103	$21.19
9	2029	$0	$355,008,739	$49,204	$14,787,665	$369,845,609	$21.59
10	2030	$0	$363,357,905	$57,691	$16,463,486	$379,879,082	$21.96
11	2031	$0	$370,982,194	$66,319	$18,080,731	$389,129,243	$22.31
12	2032	$0	$378,019,671	$74,932	$19,626,112	$397,720,714	$22.65
13	2033	$0	$384,620,645	$83,389	$21,090,223	$405,794,257	$22.97
14	2034	$0	$392,045,404	$91,615	$22,473,154	$414,610,174	$23.24
15	2035	$0	$399,021,900	$99,529	$23,771,089	$422,892,517	$23.49
16	2036	$0	$405,714,525	$107,044	$24,979,082	$430,800,651	$23.72
17	2037	$0	$412,479,551	$114,107	$26,095,952	$438,689,610	$23.92
18	2038	$0	$418,390,535	$120,627	$27,113,321	$445,624,483	$24.10
19	2039	$0	$424,344,445	$126,553	$28,030,229	$452,501,226	$24.25
20	2040	$0	$430,726,546	$131,916	$28,854,679	$459,713,141	$24.36
21	2041	$0	$437,935,982	$136,760	$29,599,075	$467,671,817	$24.43
22	2042	$0	$429,324,211	$140,688	$30,178,332	$459,643,231	$24.77
23	2043	$0	$432,732,888	$144,189	$30,688,025	$463,565,102	$24.84
24	2044	$0	$435,960,956	$147,346	$31,140,495	$467,248,797	$24.91
25	2045	$0	$439,237,664	$150,263	$31,551,344	$470,939,271	$24.96
26	2046	$0	$442,230,479	$153,002	$31,929,276	$474,312,757	$25.00
27	2047	$0	$445,334,157	$155,668	$32,285,302	$477,775,127	$25.04
28	2048	$0	$448,190,015	$158,253	$32,619,841	$480,968,109	$25.08
29	2049	$0	$450,983,531	$160,763	$32,934,626	$484,078,920	$25.11
30	2050	$0	$453,904,155	$163,206	$33,232,654	$487,300,015	$25.13
31	2051	$0	$454,730,556	$165,503	$33,494,491	$488,390,550	$25.19
32	2052	$0	$455,469,747	$167,722	$33,728,697	$489,366,166	$25.24
33	2053	$0	$456,124,543	$169,851	$33,936,162	$490,230,556	$25.28
34	2054	$0	$456,712,926	$171,880	$34,122,586	$491,007,391	$25.32
35	2055	$0	$457,234,600	$173,792	$34,287,873	$491,696,266	$25.36
36	2056	$0	$457,690,833	$175,587	$34,432,426	$492,298,846	$25.39
37	2057	$0	$458,084,204	$177,260	$34,557,062	$492,818,527	$25.42
38	2058	$0	$458,395,516	$178,752	$34,655,698	$493,229,966	$25.44
39	2059	$0	$458,655,327	$180,143	$34,738,017	$493,573,487	$25.46
40	2060	$0	$458,874,218	$181,461	$34,807,370	$493,863,049	$25.47

d) DSRC Option Costs

Table VII-9 summarizes the estimated annual communication costs for the DSRC exclusive approach. Estimates for this option show a range of $0 at Year 1 increasing to an approximate $177 million annual average by Year 40. When viewed from a per vehicle basis,

the costs range from $0 in the first year to approximately $9 annual average in the out years. An important note with this communication option is the need to include road side unit replacement based on the assumed 15 year life of span of this equipment, Years 19 and 34 reflect the annual cost of replacing this equipment.

Table VII-9 Estimated Annual Communication Costs and Per Vehicle Costs - DSRC

	Calendar			**Data Cost**			**Cost Per**
Year	Year	RSE	OBE	Satellite	Cellular	Total	Vehicle
1	2021	$0	$0	$0	$0	$0	$0.00
2	2022	$0	$0	$0	$0	$0	$0.00
3	2023	$0	$0	$0	$0	$0	$0.00
4	2024	$186,090,367	$0	$0	$0	$186,090,367	$11.26
5	2025	$85,882,056	$0	$0	$0	$85,882,056	$5.15
6	2026	$95,733,225	$0	$0	$0	$95,733,225	$5.72
7	2027	$105,584,395	$0	$0	$0	$105,584,395	$6.25
8	2028	$115,435,565	$0	$0	$0	$115,435,565	$6.78
9	2029	$125,286,734	$0	$0	$0	$125,286,734	$7.31
10	2030	$135,137,904	$0	$0	$0	$135,137,904	$7.81
11	2031	$144,989,074	$0	$0	$0	$144,989,074	$8.31
12	2032	$154,840,243	$0	$0	$0	$154,840,243	$8.82
13	2033	$164,691,413	$0	$0	$0	$164,691,413	$9.32
14	2034	$174,542,583	$0	$0	$0	$174,542,583	$9.78
15	2035	$184,393,752	$0	$0	$0	$184,393,752	$10.24
16	2036	$168,543,441	$0	$0	$0	$168,543,441	$9.28
17	2037	$147,767,545	$0	$0	$0	$147,767,545	$8.06
18	2038	$147,767,545	$0	$0	$0	$147,767,545	$7.99
19	2039	$252,465,284	$0	$0	$0	$252,465,284	$13.53
20	2040	$177,681,184	$0	$0	$0	$177,681,184	$9.42
21	2041	$177,681,184	$0	$0	$0	$177,681,184	$9.28
22	2042	$177,681,184	$0	$0	$0	$177,681,184	$9.57
23	2043	$177,681,184	$0	$0	$0	$177,681,184	$9.52
24	2044	$177,681,184	$0	$0	$0	$177,681,184	$9.47
25	2045	$177,681,184	$0	$0	$0	$177,681,184	$9.42
26	2046	$177,681,184	$0	$0	$0	$177,681,184	$9.37
27	2047	$177,681,184	$0	$0	$0	$177,681,184	$9.31
28	2048	$177,681,184	$0	$0	$0	$177,681,184	$9.26
29	2049	$177,681,184	$0	$0	$0	$177,681,184	$9.22
30	2050	$177,681,184	$0	$0	$0	$177,681,184	$9.16
31	2051	$162,724,365	$0	$0	$0	$162,724,365	$8.39
32	2052	$147,767,545	$0	$0	$0	$147,767,545	$7.62
33	2053	$147,767,545	$0	$0	$0	$147,767,545	$7.62
34	2054	$252,465,284	$0	$0	$0	$252,465,284	$13.02
35	2055	$177,681,184	$0	$0	$0	$177,681,184	$9.16
36	2056	$177,681,184	$0	$0	$0	$177,681,184	$9.16
37	2057	$177,681,184	$0	$0	$0	$177,681,184	$9.16
38	2058	$177,681,184	$0	$0	$0	$177,681,184	$9.16
39	2059	$177,681,184	$0	$0	$0	$177,681,184	$9.16
40	2060	$177,681,184	$0	$0	$0	$177,681,184	$9.16

e) Communication Cost Summary

Comparing the two communication options evaluated in this proposal yields a sharp cost difference between the Hybrid and DSRC option, a difference of approximately $325 million annually at full deployment. Exploiting the "free" usage of the allocated DSRC spectrum appears to provide clear advantages to consumers and the overall system sustainability. Challenges deploying the approach, however, are in the physical placement of the road side units across the nation in a timely manner. Leveraging the existing cellular and satellite network poses a clear advantage to accelerating deployment in the fleet.

f) Included SCMS Costs

The agency developed cost estimates for a potential SCMS based on additional research and modeling conducted by BAH, like the CDDS model used for communication cost estimation. The agency determined that it was appropriate to make some minor adjustments to the cost model based on updated information obtained between development of the original model and in preparation for this proposal. More specifically, the agency updated the model with changes to project salaries, compensation costs, and by including costs needed for establishing the SCMS (Year 0).

Salaries were revised using the most current data from Occupational Employment Statistics (OES) [357] published by the Bureau of Labor Statistics (BLS) May 2014. In addition, the agency mapped new/revised BLS job categories to those originally used by BAH. Compensation costs in the BAH model were revised to align with newer information indicating that the average hourly wages for all workers in private industry is $21.94 and the average total benefit is $9.71, where the total benefits are 44.3 percent of the wages.[358] The 44.3 percentage is significantly higher than the 25 percent used in the SCMS cost model and the agency believed it was appropriate to revised these values to accurate reflect compensation values. Finally, including Year 0 costs for the SCMS added $20.8 million as a one-time cost. The Year 0 costs include the design of the SCMS facilities, land preparation, power source redundancy, power line installation, and other facility characteristics that are necessary, and in some cases unique, for a successful SCMS operation. This new, added cost was amortized over 20 years which the agency believes is reasonable considering the long term commitment associated with SCMS development and operation.

To estimate the annual total costs for the entire SCMS, the agency first examined the costs for each of the 10 component functions of the SCMS. For each function, the costs

---

[357] MSA_M2014 File as May 2014, www.bls.gov/oes

[358] Based on the News Release on, EMPLOYER COSTS FOR EMPLOYEE COMPENSATION, March 2015 (2015 USDL-15-1132)Table 5 (page 10), released June 10, 2015, http://www.bls.gov/news.release/pdf/ecec.pdf

comprised five expenditure categories: Hardware Purchase, Software Purchase, Software Operation and Maintenance (Q&M), Initial Facility Costs, Annual Facility Costs, and Full Time Equivalent (FTE) Costs. The SCMS model identified several locations that could be used to establish an SCMS as a way to develop facility cost averages. The averages are based on six geographically and demographically varying areas: Metro DC, Richland, WA, Denver, CO, Chicago, IL, San Antonio, TX, and Gastonia, NC. The key cost components evaluated are labor costs, energy costs, land cost, and monthly rent.

Table VII-10 and Table VII-11 show the estimated SCMS costs by specific SCMS function, the total costs, and the per vehicle cost. Any equipment related costs are adjusted for learning. As shown, the total estimated SCMS costs range from $39.1 million in the first year to $160.1 million in year 40 with per vehicle cost ranging from $2.42 to $8.29. The agency requests comment on its assumptions concerning potential SCMS costs. In particular, how would different approaches to the design of the SCMS affect the costs of operating the system? In addition, how would the costs of the SCMS be passed along to consumers?

Table VII-10 SCMS Costs by Function

Year	Calendar Year	PCA	RA	LA	MA	LOP	ECA
1	2021	$4,708,025	$10,358,634	$987,277	$3,679,694	$2,332,410	$4,381,260
2	2022	$4,672,050	$10,270,907	$988,020	$3,658,706	$2,311,587	$4,343,622
3	2023	$4,677,281	$10,274,580	$990,346	$3,658,847	$2,312,044	$4,343,622
4	2024	$4,687,633	$10,281,935	$995,076	$3,659,125	$2,312,536	$4,343,622
5	2025	$6,728,645	$13,103,893	$1,740,502	$3,889,204	$2,771,798	$4,781,464
6	2026	$4,724,254	$10,308,046	$1,011,781	$3,660,108	$2,313,639	$4,343,622
7	2027	$4,744,931	$10,322,789	$1,021,213	$3,660,663	$2,314,203	$4,343,622
8	2028	$4,765,448	$10,337,418	$1,030,571	$3,661,213	$2,314,761	$4,343,622
9	2029	$4,785,584	$10,351,775	$1,039,756	$3,661,753	$2,315,308	$4,343,622
10	2030	$10,510,180	$16,401,748	$4,799,128	$4,179,494	$3,682,299	$4,781,464
11	2031	$9,308,218	$14,856,461	$9,073,569	$5,441,652	$4,543,859	$4,343,622
12	2032	$9,327,079	$14,869,909	$9,082,173	$5,442,159	$4,544,359	$4,343,622
13	2033	$9,345,391	$14,882,966	$9,090,526	$5,442,650	$4,544,835	$4,343,622
14	2034	$9,363,032	$14,895,544	$9,098,573	$5,443,123	$4,545,288	$4,343,622
15	2035	$14,419,003	$20,996,845	$12,930,027	$5,772,704	$5,912,422	$4,781,464
16	2036	$9,395,586	$14,918,755	$9,113,422	$5,443,997	$4,546,114	$4,343,622
17	2037	$9,410,421	$14,929,333	$9,120,189	$5,444,395	$4,546,484	$4,343,622
18	2038	$9,424,185	$14,939,146	$9,126,467	$5,444,764	$4,546,824	$4,343,622
19	2039	$9,436,904	$14,948,215	$9,132,269	$5,445,106	$4,547,132	$4,343,622
20	2040	$18,633,720	$24,737,954	$15,746,265	$6,126,542	$7,214,409	$4,781,464
21	2041	$13,918,676	$19,420,803	$13,587,376	$7,223,691	$6,773,241	$4,343,622
22	2042	$13,927,310	$19,426,959	$13,591,314	$7,223,922	$6,773,441	$4,343,622
23	2043	$13,935,979	$19,433,140	$13,595,268	$7,224,155	$6,773,625	$4,343,622
24	2044	$13,943,871	$19,438,767	$13,598,868	$7,224,367	$6,773,790	$4,343,622
25	2045	$22,174,444	$29,152,824	$20,355,009	$7,633,697	$9,489,116	$4,781,464
26	2046	$13,955,521	$19,447,074	$13,604,182	$7,224,679	$6,774,061	$4,343,622
27	2047	$13,960,466	$19,450,599	$13,606,438	$7,224,812	$6,774,181	$4,343,622
28	2048	$13,964,937	$19,453,788	$13,608,477	$7,224,932	$6,774,292	$4,343,622
29	2049	$13,969,051	$19,456,721	$13,610,354	$7,225,042	$6,774,396	$4,343,622

30	2050	$26,815,885	$33,350,158	$23,655,970	$8,045,813	$11,171,981	$4,781,464
31	2051	$18,425,034	$23,909,622	$18,057,646	$9,002,835	$8,999,434	$4,343,622
32	2052	$18,428,332	$23,911,973	$18,059,151	$9,002,923	$8,999,513	$4,343,622
33	2053	$18,431,447	$23,914,194	$18,060,572	$9,003,007	$8,999,585	$4,343,622
34	2054	$18,434,213	$23,916,166	$18,061,833	$9,003,081	$8,999,649	$4,343,622
35	2055	$28,781,702	$35,756,214	$26,844,673	$9,423,600	$12,687,495	$4,781,464
36	2056	$18,438,804	$23,919,440	$18,063,928	$9,003,204	$8,999,755	$4,343,622
37	2057	$18,440,716	$23,920,803	$18,064,800	$9,003,256	$8,999,799	$4,343,622
38	2058	$18,442,316	$23,921,944	$18,065,529	$9,003,299	$8,999,834	$4,343,622
39	2059	$18,443,789	$23,922,994	$18,066,201	$9,003,338	$8,999,864	$4,343,622
40	2060	$31,518,164	$38,029,601	$28,307,710	$9,825,764	$13,480,752	$4,781,464

Table VII-11 Continued SCMS Costs by Function

Year	Calendar Year	Intermediate CA	Root CA	DCM	Manager	Total Costs	Total per Vehicle
1	2021	$4,317,570	$1,723,817	$4,378,553	$2,233,628	$39,100,867	$2.42
2	2022	$4,279,932	$1,717,795	$4,340,915	$2,231,119	$38,814,652	$2.38
3	2023	$4,279,932	$1,717,795	$4,340,915	$2,231,119	$38,826,479	$2.36
4	2024	$4,279,932	$1,717,795	$4,340,915	$2,231,119	$38,849,687	$2.35
5	2025	$4,718,684	$1,808,090	$4,760,710	$2,292,279	$46,595,268	$2.80
6	2026	$4,279,932	$1,717,795	$4,340,915	$2,231,119	$38,931,210	$2.32
7	2027	$4,279,932	$1,717,795	$4,340,915	$2,231,119	$38,977,180	$2.31
8	2028	$4,279,932	$1,717,795	$4,340,915	$2,231,119	$39,022,793	$2.29
9	2029	$4,279,932	$1,717,795	$4,340,915	$2,231,119	$39,067,558	$2.28
10	2030	$5,968,049	$1,808,090	$4,760,710	$2,557,780	$59,448,941	$3.44
11	2031	$8,455,524	$1,717,795	$4,340,915	$3,382,829	$65,464,444	$3.75
12	2032	$8,455,524	$1,717,795	$4,340,915	$3,382,829	$65,506,362	$3.73
13	2033	$8,455,524	$1,717,795	$4,340,915	$3,382,829	$65,547,052	$3.71
14	2034	$8,455,524	$1,717,795	$4,340,915	$3,382,829	$65,586,244	$3.68
15	2035	$10,890,222	$1,808,090	$4,760,710	$3,511,964	$85,783,450	$4.77
16	2036	$8,455,524	$1,717,795	$4,340,915	$3,382,829	$65,658,556	$3.62
17	2037	$8,455,524	$1,717,795	$4,340,915	$3,382,829	$65,691,506	$3.58
18	2038	$8,455,524	$1,717,795	$4,340,915	$3,382,829	$65,722,070	$3.55
19	2039	$8,455,524	$1,717,795	$4,340,915	$3,382,829	$65,750,310	$3.52
20	2040	$12,177,224	$1,808,090	$4,760,710	$3,774,067	$99,760,445	$5.29
21	2041	$12,631,117	$1,717,795	$4,340,915	$4,517,339	$88,474,574	$4.62
22	2042	$12,631,117	$1,717,795	$4,340,915	$4,517,339	$88,493,733	$4.77
23	2043	$12,631,117	$1,717,795	$4,340,915	$4,517,339	$88,512,955	$4.74
24	2044	$12,631,117	$1,717,795	$4,340,915	$4,517,339	$88,530,450	$4.72
25	2045	$17,513,413	$1,808,090	$4,760,710	$4,691,868	$122,360,635	$6.48
26	2046	$12,631,117	$1,717,795	$4,340,915	$4,517,339	$88,556,305	$4.67
27	2047	$12,631,117	$1,717,795	$4,340,915	$4,517,339	$88,567,283	$4.64
28	2048	$12,631,117	$1,717,795	$4,340,915	$4,517,339	$88,577,214	$4.62
29	2049	$12,631,117	$1,717,795	$4,340,915	$4,517,339	$88,586,351	$4.59
30	2050	$19,214,431	$1,808,090	$4,760,710	$4,691,868	$138,296,371	$7.13
31	2051	$16,806,710	$1,717,795	$4,340,915	$4,517,339	$110,120,950	$5.68
32	2052	$16,806,710	$1,717,795	$4,340,915	$4,517,339	$110,128,271	$5.68
33	2053	$16,806,710	$1,717,795	$4,340,915	$4,517,339	$110,135,185	$5.68
34	2054	$16,806,710	$1,717,795	$4,340,915	$4,517,339	$110,141,322	$5.68
35	2055	$23,459,123	$1,808,090	$4,760,710	$4,692,002	$152,995,074	$7.89

36	2056	$16,806,710	$1,717,795	$4,340,915	$4,517,339	$110,151,511	$5.68
37	2057	$16,806,710	$1,717,795	$4,340,915	$4,517,339	$110,155,754	$5.68
38	2058	$16,806,710	$1,717,795	$4,340,915	$4,517,339	$110,159,302	$5.68
39	2059	$16,806,710	$1,717,795	$4,340,915	$4,517,339	$110,162,566	$5.68
40	2060	$23,459,123	$1,808,090	$4,760,710	$4,692,026	$160,663,404	$8.29

3. Fuel Economy Impact

In addition to the cost of V2V equipment itself, other potential costs include the potential for new equipment on vehicles to increase vehicle weight. The agency expects increased weight of V2V equipment will have a small impact on the fuel economy of the individual vehicles. Over the lifetime of these vehicles, this impact on fuel economy will create a cost for society.

Potential fuel economy impacts can be evaluated in terms of annual impacts and the lifetime fuel economy impacts for a specified MY vehicle (MY fuel impact). The annual fuel impact represents the additional fuel costs from all V2V-equipped vehicles for that year. The MY fuel impact represents the additional fuel costs for a life of a MY vehicle and should be discounted.

As described in previous sections, V2V components include DSRC radios and relevant parts/materials (e.g., antenna, installation material, HSM etc.) and OBE for cellular, Wi-Fi and satellite. A variance depending on the potential implementation is related to the one or two DSRC radio communication approach. Therefore, for the Hybrid option, the total additional total weight would be 3.21 pounds which came from one-radio and relevant parts/materials (3.06 pounds) and satellite radios (0.15 pounds). Weight from cellular and Wi-Fi are negligible. For the DSRC option, the total additional weight would be 3.38 pounds based the used of two DSRC radios and relevant parts/materials.

The impact of added weight on both annual and MY fuel economic is a function of vehicle volumes, vehicle miles traveled, survival probability (i.e., the percentage of the vehicle fleet that will not be scrapped due to an accident), the price of gasoline, and the change in vehicle fuel economy (i.e., change in miles per gallon) due to the added weight. Details on the estimating vehicle volumes, miles traveled, and survivability can be found in Chapter VII of the PRIA.

a) Annual Fuel Economy Impact

Table VII-12 shows the annual fuel economy impact for both one-radio with the Hybrid option and two radios with the DSRC option. Note that the weight difference between the two-radio system and the one-radio system is 0.17 pound. This small weight difference resulted in no discernable difference between these two technology approaches. To be consistent with the measure used for other cost items, the "per vehicle" cost was estimated to be the cost per a new vehicle. As shown, the proposed rule would increase the current total annual fuel consumption by 1.10 million gallons in 2021 to 30.51 million gallons in 2060. The corresponding annual cost for these additional fuels was estimated to be $3.08 to $135.16 million, annually. These amounts were translated into $0.19 to $6.97 per new vehicle sold.

Table VII-12 Annual Fuel Economy Impact*

Year	Calendar Year	Fuel Price	Additional Galleons (Million)	Total Fuel Economy (Million $)	Per Vehicle Cost ($)
1	2021	$2.80	1.10	$3.08	$0.19
2	2022	$2.86	2.69	$7.69	$0.47
3	2023	$2.91	4.70	$13.68	$0.83
4	2024	$2.95	6.58	$19.41	$1.17
5	2025	$2.99	8.34	$24.94	$1.50
6	2026	$3.02	10.02	$30.26	$1.81
7	2027	$3.06	11.66	$35.68	$2.11
8	2028	$3.08	13.19	$40.63	$2.39
9	2029	$3.11	14.62	$45.47	$2.65
10	2030	$3.14	16.01	$50.27	$2.91
11	2031	$3.18	17.32	$55.08	$3.16
12	2032	$3.22	18.52	$59.63	$3.40
13	2033	$3.26	19.69	$64.19	$3.63
14	2034	$3.35	20.73	$69.45	$3.89
15	2035	$3.38	21.76	$73.55	$4.09
16	2036	$3.43	22.68	$77.79	$4.28
17	2037	$3.47	23.50	$81.55	$4.45
18	2038	$3.51	24.28	$85.22	$4.61
19	2039	$3.58	24.99	$89.46	$4.79
20	2040	$3.66	25.64	$93.84	$4.97
21	2041	$3.64	26.27	$95.62	$5.00
22	2042	$3.68	26.70	$98.26	$5.29
23	2043	$3.72	27.11	$100.85	$5.40
24	2044	$3.76	27.46	$103.25	$5.50
25	2045	$3.80	27.83	$105.75	$5.60
26	2046	$3.84	28.11	$107.94	$5.69
27	2047	$3.88	28.44	$110.35	$5.78
28	2048	$3.93	28.71	$112.83	$5.88
29	2049	$3.97	28.91	$114.77	$5.95
30	2050	$4.01	29.21	$117.13	$6.04
31	2051	$4.06	29.43	$119.49	$6.16
32	2052	$4.10	29.65	$121.57	$6.27
33	2053	$4.14	29.82	$123.45	$6.37
34	2054	$4.18	29.97	$125.27	$6.46
35	2055	$4.22	30.10	$127.02	$6.55
36	2056	$4.27	30.20	$128.95	$6.65
37	2057	$4.31	30.33	$130.72	$6.74
38	2058	$4.35	30.41	$132.28	$6.82
39	2059	$4.39	30.47	$133.76	$6.90
40	2060	$4.43	30.51	$135.16	$6.97

*for both one-radio and two-radios approaches

b) MY Fuel Economy Impact

MY fuel cost (i.e., lifetime fuel economy cost) is the cost of additional gasoline used over the vehicle's life and is estimated on a per vehicle basis. The fuel economy cost for a specific MY vehicle is derived by applying the specific MY fuel economy cost per vehicle to every vehicle. The cost is accrued throughout the vehicle's life and is discounted to reflect its present value (in 2014 dollars) using 3% and 7% discount rates. The MY fuel economy impact also is a function of mileage, survival probability (i.e., the percentage of the vehicle fleet that will not be scrapped due to an accident), the price of gasoline, the change in vehicle fuel economy due to the added weight, and the discount rate chosen to express lifetime impacts in their present value. Additional details on the deriving the MY fuel economy impact can be found in Chapter 7 of the PRIA.

Table VII-13 shows the MY fuel economy impacts at both 3 and 7 percent discount rates. As shown, at a 3 percent discount rate, the MY fuel economy impact of V2V related equipment is estimated to be $32.75 million at MY 2021 and gradually increasing to $104.73 million for MY 2050 vehicles. The cost per vehicle is estimated to be $2.02 for MY 2021 and $5.40 for MY 2050 vehicles. The increase in fuel cost in the future, especially after the third year when the full adoption of DSRC radios starts, is primarily due to projected higher fuel prices and vehicle sales, both of which can vary. The cost per vehicle for a particular MY vehicle is calculated by dividing the total fuel cost for that MY by the total vehicle sales of that MY vehicle. For the first two years, due to the proposed phased in implementation, the cost per vehicle is smaller than the cost per affected vehicle since cost per vehicle as defined is the average cost over all new vehicles.

At a 7 percent discount rate, the MY fuel economy impact is estimated to be $25.03 for million MY 2021 and $80.52 million for MY 2050 vehicles. The cost per vehicle for these two MY vehicles would be $1.55 and $4.15 for MY 202 and MY 2050 vehicles, respectively.

Table VII-13 MY Fuel Economy Impact* by Discount Rate

Year	Model Year	Gallons per Vehicle	Total Gallons (Million)	MY Fuel Economy Impact (Million $)		Per Vehicle Cost	
				@3%	@7%	@3%	@7%
1	2021	0.83	13.38	$32.75	$25.03	$2.02	$1.55
2	2022	1.22	19.88	$49.33	$37.71	$3.02	$2.31
3	2023	1.58	26.01	$65.34	$49.96	$3.97	$3.04
4	2024	1.54	25.52	$64.90	$49.62	$3.93	$3.00
5	2025	1.49	24.80	$63.85	$48.81	$3.83	$2.93
6	2026	1.50	25.07	$65.31	$49.92	$3.90	$2.98
7	2027	1.50	25.39	$66.95	$51.17	$3.97	$3.03
8	2028	1.51	25.74	$68.69	$52.50	$4.03	$3.08
9	2029	1.52	26.03	$70.32	$53.74	$4.11	$3.14
10	2030	1.53	26.42	$72.30	$55.27	$4.18	$3.19
11	2031	1.53	26.77	$74.21	$56.74	$4.26	$3.25
12	2032	1.54	27.06	$76.00	$58.14	$4.33	$3.31
13	2033	1.55	27.34	$77.77	$59.52	$4.40	$3.37
14	2034	1.55	27.71	$79.86	$61.15	$4.48	$3.43
15	2035	1.56	28.07	$81.82	$62.67	$4.55	$3.48
16	2036	1.56	28.40	$83.76	$64.18	$4.61	$3.53
17	2037	1.57	28.77	$85.80	$65.76	$4.68	$3.59
18	2038	1.57	29.09	$87.73	$67.25	$4.74	$3.64
19	2039	1.58	29.45	$89.80	$68.86	$4.81	$3.69
20	2040	1.58	29.87	$92.00	$70.56	$4.88	$3.74
21	2041	1.58	30.30	$94.14	$72.18	$4.92	$3.77
22	2042	1.59	29.53	$92.69	$71.07	$4.99	$3.83
23	2043	1.59	29.69	$94.15	$72.20	$5.05	$3.87
24	2044	1.59	29.85	$95.63	$73.36	$5.10	$3.91
25	2045	1.59	30.03	$97.17	$74.56	$5.15	$3.95
26	2046	1.59	30.19	$98.66	$75.72	$5.20	$3.99
27	2047	1.59	30.37	$100.21	$76.94	$5.25	$4.03
28	2048	1.59	30.53	$101.73	$78.14	$5.30	$4.07
29	2049	1.59	30.69	$103.20	$79.30	$5.35	$4.11
30	2050	1.59	30.87	$104.73	$80.52	$5.40	$4.15

4. Overall Annual Costs

a) Total Annual Costs

The annual costs represent the total annual capital investment and fuel economy impact from all V2V-equipped vehicles per year. The costs comprise four major categories: (1) vehicle technology (i.e., DSRC radios and app), (2) SCMS, (3) equipment and communication network in support of vehicles-to-SCMS communication (i.e., Communication), and (4) fuel economy impact due to the increased weight from the in-vehicle equipment in (1) and (3).

Table VII-14 presents the total annual costs and cost per vehicle. The total annual costs would range from $2.2 (the lower bound for 2021) to $5.0 billion (not shown, upper bound for 2024). The cost per new vehicle would range from $135 to $301 (lower bound for 2021 and upper bound for 2024). The lower and upper bounds represent the two technology implementation approaches (one-radio and two-radios) that the agency believes can meet the proposed rule and the security and privacy specifications.

Table VII-14 Total Annual Costs and Cost Per Vehicle (2014 $)

Year	Calendar Year	Annual Cost (Million $)		Annual Cost per Vehicle	
		Low	High	Low	High
1	2021	$2,192	$2,864	$135.38	$176.89
5	2025	$3,701	$4,803	$222.02	$288.13
10	2030	$3,649	$4,692	$210.94	$271.22
15	2035	$3,717	$4,757	$206.52	$264.26
20	2040	$3,831	$4,844	$203.01	$256.71
25	2045	$3,796	$4,764	$201.14	$252.49
30	2050	$3,858	$4,818	$198.97	$248.50
35	2055	$3,832	$4,766	$197.65	$245.80
40	2060	$3,804	$4,717	$196.20	$243.27

b) Total Annual Costs By Cost Category

Table VII-15 to Table VII-18 lists the total annual costs separately for the four cost categories. As shown, the majority of costs came from vehicle technology costs. The annual vehicle technology costs ranged from $2.0 to $4.9 billion (in 2023, not shown) and the per vehicle cost ranged from $124 to $298.

The SCMS costs included the costs for the establishment, operation, and maintenance of the system that covered the expenditure on human resources, equipment, facilities, energy, etc. The total annual SCMS costs would range from $39 to $161 million. This is equivalent to $2 to $8 per vehicle.

The communication costs included the costs for equipment and communication network that are needed in support of the vehicle-to-SCMS communication. The annual communication

costs would range up to $494 million. The communication cost per vehicle would be up to $26 per vehicle.

The fuel economy impact was based on the added weight of 3.38 pounds for the two-radio technology approach and 3.21 pounds for the one-radio approach. Due to the insignificant weight difference between these two approaches, the estimated fuel economy impacts are identical for these approaches when factoring rounding errors. Therefore, the fuel economy impact as shown applies to both approaches. The annual fuel economy impact would range from $3 to 135 million. This equates to up to $7 per vehicle.

Table VII-15 Total Annual Vehicle Technology Costs (2014 $ and Vehicles in Millions)

Year	Calendar Year	Total Costs (Million $)		Cost Per Vehicle	
		Low	High	Low	High
1	2021	$2,001	$2,822	$123.59	$174.29
5	2025	$3,297	$4,646	$197.79	$278.68
10	2030	$3,160	$4,447	$182.63	$257.06
15	2035	$3,135	$4,413	$174.17	$245.17
20	2040	$3,178	$4,473	$168.39	$237.03
25	2045	$3,096	$4,359	$164.09	$230.98
30	2050	$3,115	$4,385	$160.67	$226.16
35	2055	$3,061	$4,308	$157.85	$222.19
40	2060	$3,015	$4,243	$155.47	$218.85

Table VII-16 Total Annual SCMS Costs* (2014 $ and Vehicles in Millions)

Year	Calendar Year	Total Costs (Million $)	Cost Per Vehicle
1	2021	$39	$2.42
5	2025	$47	$2.80
10	2030	$59	$3.44
15	2035	$86	$4.77
20	2040	$100	$5.29
25	2045	$122	$6.48
30	2050	$138	$7.13
35	2055	$153	$7.89
40	2060	$161	$8.29

* not impacted by technology approach

Table VII-17 Total Annual Communication Costs (2014 $ and Vehicles in Millions)

Year	Calendar Year	Total Costs (Million $)		Cost Per Vehicle	
		Low	High	Low	High
1	2021	$0	$1,486	$0.00	$9.18
5	2025	$85	$3,324	$5.15	$19.94
10	2030	$135	$3,799	$7.81	$21.96
15	2035	$185	$4,229	$10.24	$23.49
20	2040	$178	$4,597	$9.42	$24.36

25	2045	$178	$4,709	$9.42	$24.96
30	2050	$178	$4,873	$9.16	$25.13
35	2055	$178	$4,917	$9.16	$25.36
40	2060	$178	$4,939	$9.16	$25.47

Table VII-18 Total Annual Fuel Economy Impact*Costs (2014 $ and Vehicles in Millions)

Year	Calendar Year	Fuel Consumption (Million Gallons)	Fuel Costs (Million $)	Cost Per Vehicle
1	2021	1.10	$3.08	$0.19
5	2025	8.34	$24.94	$1.50
10	2030	16.01	$50.27	$2.91
15	2035	21.76	$73.55	$4.09
20	2040	25.64	$93.84	$4.97
25	2045	27.83	$105.75	$5.60
30	2050	29.21	$117.13	$6.04
35	2055	30.10	$127.02	$6.55
40	2060	30.51	$135.16	$6.97

*cost equal for both two technology implementation approaches due to insignificant weight difference

5. Overall Model Year (MY) Costs

The primary difference between the annual and MY costs is the fuel economy impact. The PRIA assumes that vehicle technology, SCMS, and communication costs would be paid by vehicle owners when their vehicles were purchased. Thus, these three costs are identical between the annual and MY costs. In annual costs, the fuel economy impact measures the additional fuel costs for all V2V-equipped MY vehicles in a specific calendar year. For estimating the MY costs, the fuel economy impact measures the incremental lifetime fuel impact for a specific MY vehicles and were discounted at a 3 and 7 percent rate to reflect their present value.

Table VII-19 and Table VII-20 shows the MY costs at a 3 percent and 7 percent discount rate, respectively. At a 3 percent discount rate, the MY costs would range from $2.22 (lower bound at Year 1) to $5.03 billion (upper bound at Year 4, not shown). The cost per vehicle would range from $137.21 to $304.06. The lower bound of the costs represents the MY costs for the one-radio approach and the higher bound represents the cost for the two-radio approach.

At a 7 percent discount rate, the MY costs would range from $2.21 (lower bound at Year 1) to $5.01 billion (upper bound at Year 4, not shown). The MY cost per vehicle would range from $136.73 to $303.14.

Table VII-19 Total MY Costs and Cost Per Vehicle @3 Percent

Year	Model Year	Total MY Costs (Million $)		MY Cost per Vehicle	
		Low	High	Low	High
1	2021	$2,221	$2,894	$137.21	$178.72
5	2025	$3,740	$4,842	$224.36	$290.46

10	2030	$3,671	$4,714	$212.21	$272.49
15	2035	$3,726	$4,765	$206.98	$264.72
20	2040	$3,829	$4,842	$202.92	$256.61
25	2045	$3,787	$4,756	$200.68	$252.03
30	2050	$3,846	$4,806	$198.33	$247.86

Table VII-20 Total MY Costs and Cost Per Vehicle @7 Percent

Year	Calendar Year	Total MY Costs (Million $)		MY Cost per Vehicle	
		Low	High	Low	High
1	2021	$2,214	$2,886	$136.73	$178.25
5	2025	$3,725	$4,827	$223.45	$289.56
10	2030	$3,654	$4,697	$211.22	$271.51
15	2035	$3,706	$4,746	$205.92	$263.66
20	2040	$3,808	$4,821	$201.78	$255.47
25	2045	$3,764	$4,733	$199.49	$250.83
30	2050	$3,821	$4,782	$197.09	$246.61

The agency seeks comment on all aspects of the cost estimates developed for this proposal. This includes all cost assumptions, estimated component costs, communication costs including other potential options the agency did not evaluate, and views on potential SCMS costs. Please provide any supporting data for the comments. If necessary, the agency has processes and procedures for submitting confidential business information.

C. Non-Quantified Costs

The agency identified four major non-quantified costs that could be related to the deployment of V2V devices. These include the potential health costs due to a potential increase in electromagnetic hypersensitivity (EHS, i.e., human radiation exposure to wireless communications discussed in Section IV.E) potential loss of perceived privacy, the opportunity costs of alternative uses for the spectrum, and possibly increased litigation costs. The agency requests comment on these costs, particularly whether there exist ways to quantify any of these costs.

1. Health Insurance Costs Relating to EHS

Many commenters (mostly individual citizens) commented on the potential relationship of DSRC radio technology and electromagnetic field exposure hypersensitivity, raising concerns regarding the potential for a V2V mandate to increase electromagnetic beyond today's levels. The agency takes these concerns very seriously. The agency since has conducted a literature review and other research (on-going) to better understand electromagnetic radiation and its relationship to the symptoms of EHS. As we understand that the expertise of our sister agencies such as the Federal Communications Commission (FCC) and the Food and Drug Administration (FDA), among others, have been involved with electromagnetic fields, in parallel with the pervasiveness of cellular phone deployment in the United States and globally.

The FDA found that most studies conducted to date show no connection between certain health problems and exposure to radiofrequency fields via cell phone use and that attempts to replicate and confirm the few studies that did show a connection have failed.[359] Furthermore, V2V devices would operate at distances significantly further than the distance between a portable cellular phone to its operator, where the device is generally carried on a person or pressed directly to the ear. Therefore, the EHS effects are expected to be lower for V2V than cell phones; the agency does not quantify the health costs relating to EHS. Nevertheless, the agency acknowledges that research is still ongoing and, as technology evolves; wireless communications will most likely continue to increase. We will continue to monitor the progress of this issue and closely follow the efforts of the Radiofrequency Interagency Work Group (RFIAWG) which may yield any potential future guidance for wireless device deployment and usage.

2. Perceived Privacy Loss

One intangible outcome of the proposed rule is a perceived potential for loss of privacy. Individuals may perceive the V2V system as eroding their personal privacy and view this as a considerable negative consequence. Also, several surveys showed that individual attitudes towards information security seems inconsistent with their behavior on protection of their information.[360,361] Acquisti, et al. stated that identifying the consequence of a privacy incident is difficult enough, and quantifying these consequences is remarkably complex.[362] Furthermore, there are few studies on the economic costs for privacy and even less for quantifying the economic costs for perceived privacy loss. Given the great uncertainties for valuing the perceived loss of privacy, this analysis does not quantify this cost.

To ease the privacy concerns and mitigate possible privacy loss, the agency is committed to regulating V2V communications in a manner that both protects individuals and promotes this important safety technology. NHTSA has worked closely with experts and our industry research partners (CAMP and the VIIC) to build privacy protections into the design and deployment of V2V communications that help guard against risks to individual privacy.

The agency has conducted a thorough privacy impact assessment as required by the Consolidated Appropriations Act, 2005, Pub. L. 108-447. This Act requires that Federal

---

[359] Radiation-Emitting Products, "Current Research Results," http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/HomeBusinessandEntertainment/CellPhones/ucm116335.htm, last accessed: June 3, 2015.

[360] Acquisti, Alessandro (2004), Privacy Attitudes and Privacy Behavior, Losses, Gains, and Hyperbolic Discounting (Preliminary draft)

[361] Acquisti, Alessandro (2002). Protecting privacy with economics: Economic incentives for preventing technologies in ubiquitous computing environments. In workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing – UBICOMP'02

[362] Acquisti, A., Friedman, A., Telang, R., "Is there a Cost to Privacy Breaches? An Event Study", Twenty Seventh International Conference on Information System, Milwaukee 2006 (pre-proceeding draft version)

agencies conduct privacy impact assessments (PIAs) of proposed regulatory activities involving collections or systems of information in electronic form with the potential to impact individual privacy. A PIA documents the flow of information and information requirements within a system by detailing how and why information is transmitted, collected, stored and shared to: 1) ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of the proposed data transactions; and iii) examine and evaluate protections and alternative processes for handling data to mitigate potential privacy risks.

3. Opportunity Costs of Spectrum for Other Uses

a) Overview

Our analysis shows that this rule will generate significant net benefits due to improved safety, decreased loss of life, reduced property damage, and other impacts. While requiring this technology has costs, the analysis here shows that the benefits of this rule well justify those costs.

As discussed in greater detail elsewhere in this notice, the FCC designated the 5.9 GHz band (i.e., 5850 – 5925 MHz) for ITS radio services and adopted open license to both public safety and non-public safety use of this band with the priority for public safety communications in 2003. Within the 5.9 GHz band, the FCC has designated Channel 172 (i.e., 5.855-5.865 GHz, a 10 MHz band) exclusively for "vehicle-to-vehicle communication for crash avoidance and mitigation, and safety of life and property applications."

Given the FCC's decision about how to allocate Channel 172, this rule results in the use of that particular radio spectrum for vehicle-to-vehicle communication even though that resource could potentially have alternative uses for society, including alternative safety applications. The FCC, not NHTSA or DOT, has the authority to determine the commercial use of spectrum. However, NHTSA understands the scarcity of spectrum and in the interests of providing a complete analysis of the costs and benefits of this rule seeks comment on the potential costs associated with the lost opportunity to exploit the spectrum at issue for other uses.

The FCC, as part of its own ongoing rulemaking proceeding, is considering whether to allow "Unlicensed National Information Infrastructure" (UNII) devices (that provide short-range, high-speed, unlicensed wireless connections for, among other applications, Wi-Fi-enabled radio local area networks, cordless telephones, and fixed outdoor broadband transceivers used by wireless Internet service providers) to operate in the same frequencies of the spectrum as V2V.

Opening any spectrum band to sharing could result in many more devices transmitting and receiving information on the same or similar frequencies. Depending on the technology, band, and uses at issue, such sharing can work well or can lead to harmful interference among those devices. Recognizing the scarcity of spectrum, in December 2015 and January 2016, the DOT, FCC, and the Department of Commerce sent joint letters to members of the U.S. Senate Committee on Commerce, Science, and Transportation, stating a shared "commitment to finding

the best method to develop, successfully test, and deploy advanced automotive safety systems while working to meet existing and future spectrum demands," and announcing an interagency, multi-phased testing regime that will be used to "provide reliable, real-world data on the performance of unlicensed devices that are designed to avoid interfering with DSRC operation in the 5.9 GHz band."[363] The results of this test will inform FCC on potential sharing solutions, if any, between proposed Unlicensed National Information Infrastructure (U-NII) devices and DSRC operations in the 5.850-5.925 GHz (U-NII-4) band.

The results of the interagency tests will also be utilized to inform NHTSA's proceeding as it progresses towards aproceeding prior to any final rulemaking on V2V. As noted in the joint DOT-FCC-Commerce letter that responds to a Congressional letter dated September 9, 2015, it is "imperative – to ensure the future automotive safety and efficiency of the traveling public – that all three phases of the FCC test plan be completed before reaching any conclusions as to whether [non-DSRC] unlicensed devices can safely operate in the 5.9 GHz band.." without interfering with DSRC operation.

DOT believes that any estimate of the opportunity cost of this NPRM should be made in the context of the FCC's existing policies and authorities. Put another way, in identifying and valuing other opportunities that might be precluded or degraded by this NPRM, DOT is considering those opportunities consistent with the FCC's designation of spectrum. However, in assessing the benefits in the context of the current FCC designation on which this rule focuses, we invite and will consider comments on opportunity costs associated with broader uses of spectrum beyond the current FCC designation.

In addition, we provide a further discussion of other potential benefits of DSRC beyond the two safety applications quantified in the economic analysis for this NPRM. Those additional benefits include potential safety, congestion, environmental, UAS and Smart City benefits.

b) Benefits of DSRC

We first provide a further explanation of the potential additional safety benefits of DSRC beyond the two intersection safety applications quantified in the economic analysis for this NPRM.

The primary benefit of the proposed rule is improved automobile safety. Section VII.D discusses this benefit at length. DOT also wishes to present a broader discussion of the benefits not measured in the Primary Regulatory Impact Analysis and seek comment on the resulting estimate. To arrive at this estimate, we have taken existing research that quantified motor vehicle crashes as costing society over $242 billion in economic impacts in 2010 and caused societal harm of over $836 billion through fatalities, injuries and property damage. Adjusting the

[363] See letter in NHTSA Docket No. NHTSA-2016-0126

societal harm estimate to reflect the increase in traffic fatalities and CPI in 2015, we arrive at a value of $966 billion. Recognizing previous research has indicated that V2V could potentially avoid or mitigate 80% of unimpaired crashes, we have conservatively calculated scenarios where V2V is phased in linearly, reaching maximum crash reduction benefits of 5, 10, and 15% by 2035.

Table VII-21 Summary of Estimated Present Value of Benefits of V2V communication for this NPRM

Societal Harm ($M)	Percentage of crashes prevented	2018 PV at 3% discount rate ($M)	2018 PV at 7% discount rate ($M)
$966,000	5.0%	$603,620	$288,480
$966,000	10.0%	$1,207,230	$576,950
$966,000	15.0%	$1,810,850	$865,430

A more conservative approach to calculating total benefit of the rule could be considering a function of the number of lives that would be saved by V2V communication, multiplied by the economic value of a life. A number of values have been used for the economic value of a life;, we compute our sensitivity analysis using values of $5-$13.4M. Table VII-22 below presents different estimates for the 2018 value of the benefit of the rule through 2050.

Table VII-22 Summary of Estimated Present Value of Benefits of V2V communication for this NPRM

Value of a life ($M)	Percentage of fatalities prevented	fatalities prevented	2018 PV at 3% discount rate ($M)	2018 PV at 7% discount rate ($M)
$ 5.4	1.0%	350.92	$ 38,636	$ 23,965
$ 13.4	1.0%	350.92	$ 95,874	$ 59,468
$ 5.4	5.0%	1754.6	$ 193,181	$ 119,824
$ 13.4	5.0%	1754.6	$ 479,373	$ 297,341
$ 5.4	10.0%	3509.2	$ 386,360	$ 239,648
$ 13.4	10.0%	3509.2	$ 958,747	$ 594,683

c) Other Benefits of DSRC Communication

The benefits shown above offset the costs, including opportunity costs, of this proposed rule. Moreover, the beneficial uses of spectrum for vehicle-to-vehicle communications could well increase in the future. Over the last five years, the USDOT has sponsored the Connected Vehicle Program under Intelligent Transportation Systems Research. This program has identified more than fifty potential connected vehicle applications concepts, many of which have already been prototyped and demonstrated. As a part of this process, the component application development programs have also conducted assessments to measure safety, mobility, and environmental impacts. Field demonstrations have been supplemented by estimation of difficult-to-observe impacts and potential future impacts from broader application deployment using a

range of analytical methods. The USDOT has published documentation from the more advanced application development efforts, including concepts of operations, system requirements, design documents, algorithms, functional descriptions, characterization test results, field test evaluation results and estimation of benefits associated with these prototypes. In total, the USDOT has identified fifty-three connected vehicle applications that will depend on effective vehicle communication. These fifty-three applications include thirteen safety applications that address vehicle occupant and pedestrian safety through communication with other vehicles as well as roadside infrastructure. They also include fifteen applications that address environmental quality and resource consumption, and many more that address congestion, mobility, and data gathering.

d) Opportunity Costs of Precluding Alternative Uses

Decisions regarding whether to allow additional uses of spectrum than those currently authorized by the FCC for the ITS band are not within the scope of DOT's or NHTSA's authority. Comments on the value of these uses will, however, be accepted. Such comments should consider that the interagency spectrum sharing tests are not yet complete, and it will be impossible to fully measure such benefits until the feasibility of sharing is determined. If such sharing is possible, those benefits will likely decrease opportunity costs associated with mandating V2V communications. Nothing in this rulemaking would preclude the FCC, in conjunction with DOT and NTIA, from authorizing appropriate sharing at some future date.

The chart below is a generic calculation of the spectrum opportunity cost, based on preclusion of alternative uses for the spectrum. This estimate might overstate the value of opportunity cost if sharing is determined to be possible. We use estimated Wi-Fi values from 2013 and earlier reports to estimate the economic value of one MHz of spectrum. To do this, we begin by extracting data from the largest and most recent study of spectrum values from TAS, making several adjustments based on our analysis.[364] To calculate a net present value as of 2016, we treat the annual economic value of the spectrum beginning in 2018 and until 2050, meaning that it will generate the same value for each year in the future. There are two assumptions

[364] Assessment of the Economic Value of Unlicensed Spectrum in the United States, Final Report, February 2014, Telecom Advisory Services, LLC http://www.wififorward.org/wp-content/uploads/2014/01/Value-of-Unlicensed-Spectrum-to-the-US-Economy-Full-Report.pdf (last accessed Dec 8, 2016). We first remove RFID retail because it is a very different technology from Wi-Fi and it operates at very low frequency bands (13.56, 4.33, and 902-928 MHz (i.e., all operate at less than 1 GHz). Second, Table C includes $34.885B of producer surplus associated with Wi-Fi only tablets estimated as the difference between the retail price and manufacturing costs for a weighted average of tablet suppliers. In practice, consumers pay above manufacturing costs for marketing, brand, and other amenities, making this an overestimate. As a rough adjustment, we cut this number in half to $17.44B. Adding all spectrum values from Table C of the TAS report except for RFID retail yields a total value for unlicensed Wi-Fi spectrum of $110 billion. Based on the CEA report, there are a total of 638 MHz of spectrum available for unlicensed Wi-Fi use. This includes 83 MHz in the 2.4 GHz band and 555 MHz in the 5.1-5.8 GHz band. Dividing the TAS estimate of Wi-Fi value by the total bandwidth gives an estimate of $172.4 million per each MHz of spectrum.

implicit in this approach: (1) The spectrum continues to generate value into the future and (2) the value of the spectrum does not change from year to year (i.e., the growth rate is zero).[365]

The estimated present value of each additional MHz up to 2050 ranges between $1.9B and $3.4B based on whether a 7 or a 3 percent discount rate is used, respectively.[366]

We seek comment on whether these per-MHz figures are reasonable, including comment on the detailed analysis in footnote 3, as well as any alternative methodologies.

Table VII-23 Summary of Estimated Present Value of Spectrum

Approach	Value (Billions of $)	MHz	Billions of $/MHz	PV to 2050, 2018 Implementation, 3% discount rate (Billions of $/MHz)	PV to 2050, 2018 Implementation, 7% discount rate (Billions of $/MHz)
Estimated Value of Wi-Fi	110	638	0.2	3.4	1.9

Other ways to estimate the opportunity cost of spectrum may be feasible, including using auction values for spectrum licenses. A method like this would require estimates of the ratio between auction value and annual consumer surplus. A method like that would generate far higher values than the table above because it uses licensed rather than unlicensed spectrum as a benchmark - making it yield an estimate that cannot be directly used to assess the value of unlicensed spectrum. Other considerations when using the estimates above to value the spectrum in question include:

The value of spectrum is highly situational and the historic spectrum value might not be a valid indication of the spectrum of the future. Spectrum value differs with respect to variables including, but not limited to, frequencies, size of the block or segment, international harmonization, geographic location, the timing of the release of new batches of spectrum, and the extent to which use is shared or exclusive. Frequencies might be the most significant factor to determine the value since different frequencies have different characteristics that make useful for different applications. The most useful bands of frequencies may be auctioned out and developed early. The spectrum values for these frequencies may have very different characteristics from the 5.9 GHz band and their value may exceed the value of the 5.9 GHz.

---

[365] Other researchers including Bazelon and McHenry (2015) use a similar approach. Bazelon and McHentry (2015) paper is available here: http://www.brattle.com/system/publications/pdfs/000/005/168/original/Mobile_Broadband_Spectrum_-_A_Valuable_Resource_for_the_American_Economy_Bazelon_McHenry_051115.pdf (last accessed Dec 8, 2016)

[366] We use 3 and 7 percent discount rates to be consistent with OMB guidelines, available here (Step 7, p. 11): https://www.whitehouse.gov/sites/default/files/omb/inforeg/regpol/circular-a-4_regulatory-impact-analysis-a-primer.pdf (last accessed Dec 8, 2016)

The cost of delivering information over spectrum varies and is a function of the range in which it operates. Higher frequency spectrums like 5.9 GHz broadcast over much shorter distances than lower frequency spectrums and thus require the interaction of interoperable devices over these short distances to transmit and receive messages in order for applications to activate.

Existing market values do not reflect the progressive increase of the economic value of spectrum over time (i.e., time-dependent value).

The above estimates yield per-MHz figures for the gross opportunity cost that would result if spectrum in these bands were monopolized. However, the actual opportunity cost associated with spectrum that would result from mandating V2V in the way prescribed in this NPRM is represented by foregone alternative uses of that spectrum, which would be more limited.

It is possible that all spectrum within the relevant 75 MHz will ultimately be used for vehicle-to-vehicle communications given the substantial safety benefits of that technology. It is, however, likely that not all spectrum within the relevant 75 MHz will be de facto or de jure used exclusively for the specific safety applications envisioned by this rule, i.e., those based on transmission of the Basic Safety Message. In particular, we propose to require BSM transmissions on a single 10 MHz channel. Multiplying this 10 MHz by the per-MHz values derived above yields an opportunity cost of $19-$34 billion. We seek comment on the best framework to appropriately consider the opportunity costs of this proposed rule across the band, taking into account varying assumptions about spectrum usage. DOT expects to include an estimate of the opportunity cost of spectrum as part of its RIA in a final rule.

4. Increased Litigation Costs

The agency recognizes the possibility of higher litigation costs due to the cooperative nature of the V2V environment. However, the agency reiterates that driving tasks are drivers' responsibilities. The at-fault driver in a crash will bear the economic burden and this will not be altered in the V2V environment. Furthermore, V2V technology is expected to help avoid crashes and thus reduce the overall burden imposed on legal systems and traffic courts.

D. Estimated Benefits

1. Assumptions and Overview

In order to estimate the benefits of this rule, the agency made several key assumptions. The agency applied the same assumptions for adoption and vehicle fleet penetration rates as for estimating both the costs and benefits of this proposed rule, as shown in Table VII-24 and Table VII-25.

Table VII-24 V2V Technology Adoption Rates in Percent

	Model Year

	2021	2022	2023	2024	2025	2026	2027	2028
DSRC %	50	75	100	100	100	100	100	100
Applications %*	0	5	10	25	40	65	90	100

*as percent of DSRC-equipped vehicles

Table VII-25 V2V Technology Fleet Penetration

Year	Calendar	With DSRC Radios		With Apps	
	Year	Number of Vehicles (Million)	Percent	Number of Vehicles (Million)	Percent
1	2021	8.1	3.3%	0.0	0.0%
5	2025	68.13	27.4%	6.3	5.2%
10	2030	144.3	55.8%	87.2	33.7%
15	2035	208.4	77.6%	163.7	61.0%
20	2040	253.0	90.8%	226.1	81.2%
25	2045	276.6	96.2%	265.3	92.3%
30	2050	291.3	98.6%	286.9	96.8%
35	2055	300.6	99.7%	298.1	98.9%
40	2060	305.2	100.0%	304.6	99.8%

The agency estimated the potential benefits of the proposed rule based upon a scenario where two safety applications, IMA and LTA, are voluntarily adopted by industry following a DSRC-mandate. The agency focused on these potential safety applications because we have sufficient data and because they can be effectively enabled only by V2V. IMA warns drivers of vehicles approaching from a lateral direction at an intersection, while LTA warns drivers of vehicles approaching from the opposite direction when attempting a left turn at an intersection. The agency notes that this may not be the scenario that actually occurs following a DSRC-mandate; manufacturers may choose to offer other safety applications that use V2V technology beyond these two and may offer those technologies or IMA and LTA in a time frame different from what is considered for purposes of analysis. In addition, manufacturers may also offer various other technologies that use DSRC, such as V2I or V2P technologies. These other technologies may offer benefits of a different amount than those calculated for IMA and LTA and they may accrue over a different timeframe. The agency requests comment on these assumptions.

Overall, three major factors influence the potential benefits of a V2V implementation: the size of the crash population, the safety application effectiveness, and vehicle communication rates. The undiscounted annual benefits thus are the product of these three factors and can be expressed mathematically by the following generic formula:

$$B_i = P * E * C_i$$

Where, B_i = Annual benefits (or MY benefits) of the proposed rule at year i,

P = Target population (crashes, fatalities, injuries, or PDOVs),

E = Effectiveness of apps (i.e., IMA or LTA), and

C_i = communication rate at year i.

a) Target Population (P)

The target population (P) includes crashes, fatalities, injuries, and PDOVs. As described in Section II.A, the Safety Need, this proposed rule is estimated to affect potentially 3.4 million light-vehicle-to-light-vehicle crashes. This potential population excludes other crashes scenarios. More specifically, single-vehicle crashes were excluded based on the V2V's inherent cooperative operation, with two vehicles communicating with each to potentially issue a warning before a crash. Crashes with four or more vehicles were not included because the agency does not have data to estimate how effective the safety warning applications would be as these crashes might involve complex interactions among vehicles. Crashes involving pedestrians and pedal-cyclists were also excluded since these crashes might need the communication between vehicles and persons. Crashes involving motorcycles were excluded because the agency has not conducted any V2V research on motorcycles. Finally, crashes involving at least one heavy vehicle[367] are excluded since the agency is only evaluating light vehicle crashes at this time.

Figure VII-2 depicts how the agency determined the potential target population for both the IMA and LTA safety warning applications. In addition, the figure also includes the corresponding monetized values at each "stage" of filtering for the potential target population. As indicated, the end result is an estimated 1.06 million crashes that could be addressed by the IMA and LTA safety warning applications, making up approximately 19 percent of the total police-reported crashes. These crashes resulted in 2,372 fatalities and 0.69 million MAIS 1-5 injuries and damaged 1.29 million vehicles. Together, these crashes cost society $121 billion, annually. Separately, IMA crashes resulted in 1,824 fatalities and 0.47 million MAIS 1-5 injuries and damaged 0.97 million vehicles. The IMA crashes cost society $84 billion, annually. When compared to IMA, LTA has a smaller number of target crashes. LTA crashes resulted in 548 fatalities and 0.22 million injuries (MAIS 1-5) and damaged 0.32 million vehicles. The IMA crashes cost society $36 billion, annually.

[367] Heavy vehicles include trucks and buses with a GVWR greater than 10,000 pounds.

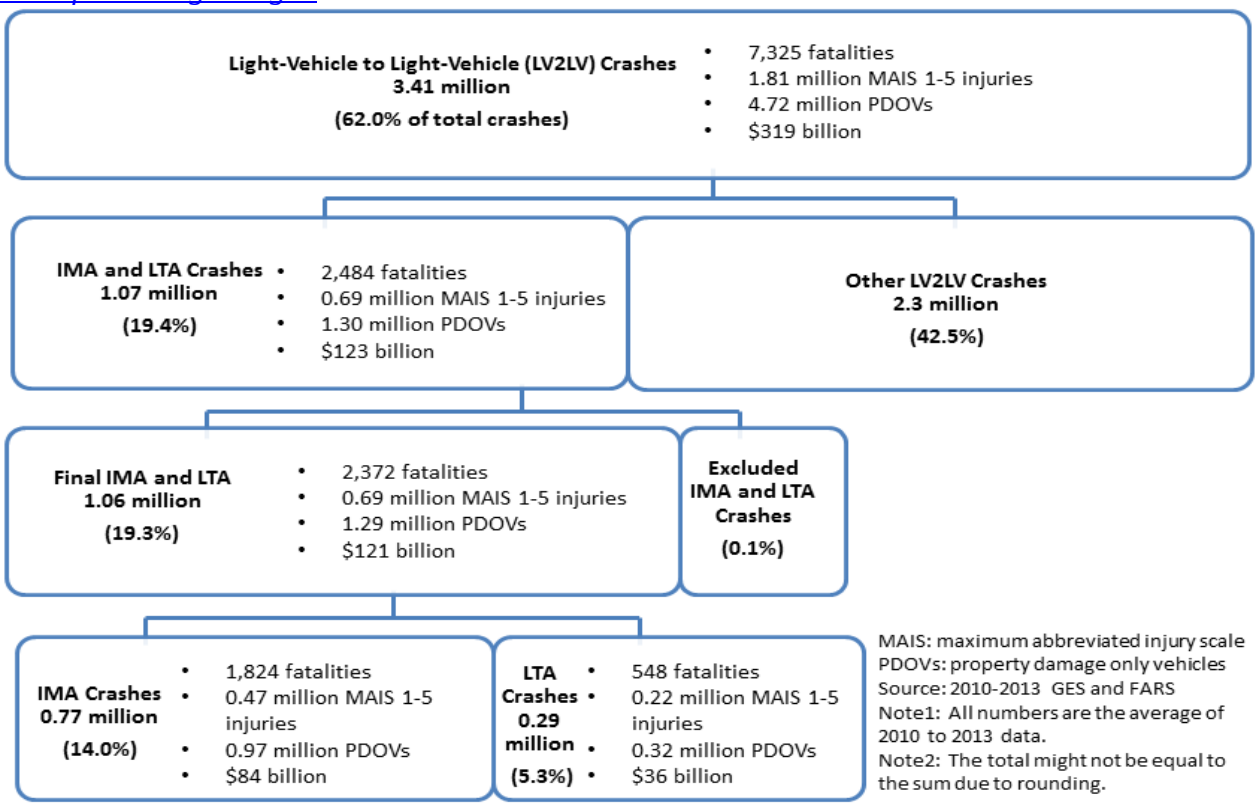

Figure VII-2 Annual LV2LV Crash Population Breakdown

The target populations used for this analysis were retrieved from the 2010-2013 FARS and GES. FARS is a census of fatalities that occurred in fatal crashes on public roadways. FARS was used to derive the incidence of fatal target crashes and associated fatalities. GES is a sampling system of all police-reported crashes. GES was used to derive the MAIS 1+ injuries in non-fatal target crashes and PDOVs. The agency utilized multiple years of crash data to limit variations of crashes and provide the best possible estimate for projecting potential benefits.

The variables used to define the target crashes include vehicle forms submitted, vehicle body type, crash type, the first harmful event, relation to roadway, roadway alignment, roadway condition, rollover type, jackknife status, driver contributing factor, and vehicle contributing factor. Of these variables, the driver contributing and vehicle contributing factors were used to refine the target population. The driver contribution factor specifies whether driver's alertness contributed to the crashes. The vehicle contributing factor identifies whether vehicle's component failure or defect contributed to the crashes. Crashes where incapacitated or drowsy drivers were involved and where vehicle mechanical failures such as brake systems, tires, steering, and transmissions were cited as contributing factors were excluded.

b) Effectiveness (E)

The agency applied effectiveness rates for IMA and LTA. The effectiveness rate estimates are derived using the Safety Impact Methodology (SIM) tool developed by the Department of Transportation's Volpe Center, specifically for estimating the effectiveness of V2V technology. In order to obtain a crash warning using V2V technology, two V2V-equipped vehicles need to interact during a potential crash situation – if a V2V-equipped vehicle interacts with a non-V2V-equipped vehicle in a potential crash situation, no warning is to be expected, because the non-equipped vehicle would produce no BSM for the equipped vehicle to recognize and respond to. To be able to estimate the effectiveness of advanced crash avoidance technology such as V2V, NHTSA developed a methodology that uses available data and computer simulation,[368] extending current estimation capabilities and enabling V2V technology to be "exposed" to more conflict situations to make up for and potential lack of crashes in the real-world crash databases. The methodology and simulation tool allows the agency to better comprehend the crash avoidance potential and the performance criteria of the V2V technology prior to the technology's actual deployment. Extensive details on how the agency estimates effectiveness of potential V2V safety applications can be found in Chapter 4 of the PRIA and Chapter XII.B.1 of the V2V Readiness Report.

Table VII-26 shows the effectiveness of IMA and LTA used for the benefit estimates in this proposal. As shown, IMA is estimated to prevent 43-56 percent of intersection related crashes and LTA would prevent 37 - 63 percent of crashes where a left turn is being attempted across oncoming traffic.

Table VII-26 Effectiveness of IMA and LTA Safety Applications

Apps	Low	High
IMA	43%	56%
LTA	37%	63%

These estimates are adjusted slightly from the effectiveness estimates used in the V2V Readiness Report to reflect the latest crash data available to the agency. There are no changes in methodology for developing the effectiveness estimate from that used in the V2V Readiness Report. In the Readiness Report, the agency estimated values of 41-55 percent for IMA and 36 - 62 percent for LTA, differences of only one to two percent at either end of the ranges. The differences originate in the minor adjustment in the injury probability curves for IMA and overall the newer crash data yielded a different crash scenario distribution. In order to account for potential uncertainty in these effectiveness rates, the agency included lower effectiveness rates in the uncertainty analysis for this rule. The agency requests additional information concerning the potential effectiveness of these two applications.

[368] For an overview of this methodology, see "Implementation of the Safety Impact Methodology Tool" DRAFT located in Docket NHTSA-2016-0126.

c) Communication Rate ($C_{i)}$

The communication rate (C_i) used the generic benefit formula above, represents the potential probability of a crash in which the vehicles involved are both DSRC-equipped light vehicles utilizing the safety applications IMA and LTA. To derive this probability, the agency first developed a projection of the number of vehicles that would be equipped by leveraging the technology adoption rates used for estimating the proposed rule costs. As discussed in the estimated cost section, the proposed rule would require that all applicable vehicles are equipped allowing for a market-driven adoption for safety applications. The proposed requirement for DSRC radio adoption schedule is a three year phase-in: 50 percent of the first MY vehicles, 75 percent of the second MY vehicles and 100 percent of the third MY vehicles. For benefits estimation, the agency applied these proposed, required adoption rates to estimated, future vehicle sales yielding the potential vehicles that could be equipped with DSRC devices in the overall vehicle fleet.

The agency believes a similar, market-driven approach could take hold for V2V technology once the equipment becomes widely available and consumers recognize the potential benefits.

The agency believes that IMA and LTA could be adopted as standard equipment on a schedule similar to the "combined" schedules for the FCW and LDW displayed in the NCAP data. Based on broad collection of implementation information such as, the ITS study, NCAP data, agency meetings with manufacturers, announcements on V2V implementation from vehicle industry, and the cost consideration; the agency established the a safety application adoption trend of 0% for the first MY vehicles that have DSRC radios, 5%, 10%, 25%, 40%, 65%, 90%, and 100% for each following MY vehicles, respectively.

The agency believes that this adoption rate is reasonable. We note that the pattern is similar to those shown in the NCAP data; with slow initial rate spanning approximately two years and then increasing year over year at a rate that would reach full adoption in the eighth year of the implementation of the DSRC technology. Under this adoption scenario, the benefits estimates assume IMA and LTA would not be deployed in the first year. In the second year, with the required 75 percent DSRC installation rate and the five percent safety application adoption among the DSRC-equipped vehicles, five percent of the total new vehicles (= 0.05 * 0.75) are expected to have the two safety applications. In the third year, 10 percent of the new vehicles (= 0.1 * 1.00) would have the apps, and so on so forth. Overall, the benefits (and costs) of the proposed rule were estimated based on this specific technology adoption scenario, as shown in Table VII-27.

Table VII-27 V2V Technology Adoption Scenario for Cost and Benefit Estimates

Year (MY)	**1 (2021)**	**2 (2022)**	**3 (2023)**	**4 (2024)**	**5 (2025)**	**6 (2026)**	**7 (2027)**	**8 (2028)**
DSRC	50%	75%	100%	100%	100%	100%	100%	100%
Apps*	0%	5%	10%	25%	40%	65%	90%	100%

Apps Actual**	0%	4%	10%	25%	40%	65%	90%	100%

*IMA and LTA of DSRC-equipped new vehicles
**of all new vehicles

Table VII-28 shows the communication rates from 2021 to 2060 by vehicle type (i.e., PCs, LTVs, and PCs and LTVs combined) separately for IMA and LTA. As expected, the communication rates would be relatively small in the first few years and accelerate faster when time progresses.

The overall communication with vehicles that had the apps would be rare in the first three years as measured by those rates for IMA. The rate would reach over 50 percent (51.41%) in 2034, the 14th year of the implementation of the proposed rule. In 2039, 5 years later, the rate would reach 75 percent. In 2044, the communication rate would reach over 90 percent.

For LTA, the communication rates would be smaller than the general communication rates. In 2022, for example, the contributable rate for LTA with vehicles equipped with the apps is about 0.02 percent, 50 percent of the overall communication rate. However, the ratio would increase over time and narrow the difference between these two rates. In 2034, the rate for LTA would be 41.36 percent, 80.5 percent of the overall communicating rate.

Table VII-28 Light Vehicle Fleet Communication Rates

Year	Calendar Year	IMA			LTA		
		PCs	LTVs	Combined	PCs	LTVs	Combined
1	2021	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
2	2022	0.02%	0.02%	0.04%	0.01%	0.01%	0.02%
3	2023	0.13%	0.13%	0.26%	0.07%	0.07%	0.14%
4	2024	0.52%	0.50%	1.02%	0.28%	0.27%	0.55%
5	2025	1.32%	1.26%	2.58%	0.73%	0.70%	1.43%
6	2026	2.77%	2.64%	5.41%	1.61%	1.54%	3.15%
7	2027	4.94%	4.71%	9.65%	3.06%	2.92%	5.98%
8	2028	7.55%	7.19%	14.74%	4.96%	4.72%	9.68%
9	2029	10.40%	9.88%	20.28%	7.17%	6.81%	13.98%
10	2030	13.45%	12.76%	26.21%	9.63%	9.14%	18.77%
11	2031	16.63%	15.77%	32.40%	12.33%	11.69%	24.02%
12	2032	19.90%	18.84%	38.74%	15.20%	14.39%	29.59%
13	2033	23.19%	21.92%	45.11%	18.20%	17.20%	35.40%
14	2034	26.46%	24.95%	51.41%	21.29%	20.07%	41.36%
15	2035	29.65%	27.87%	57.52%	24.41%	22.95%	47.36%
16	2036	32.69%	30.62%	63.31%	27.50%	25.75%	53.25%
17	2037	35.53%	33.16%	68.69%	30.48%	28.45%	58.93%
18	2038	38.12%	35.46%	73.58%	33.31%	30.98%	64.29%
19	2039	40.40%	37.47%	77.87%	35.92%	33.32%	69.24%
20	2040	42.36%	39.21%	81.57%	38.29%	35.45%	73.74%
21	2041	43.99%	40.69%	84.68%	40.38%	37.36%	77.74%
22	2042	45.18%	42.03%	87.21%	42.06%	39.12%	81.18%
23	2043	46.11%	43.17%	89.28%	43.46%	40.69%	84.15%
24	2044	46.81%	44.17%	90.98%	44.59%	42.07%	86.66%
25	2045	47.33%	45.04%	92.37%	45.47%	43.27%	88.74%
26	2046	47.72%	45.83%	93.55%	46.16%	44.33%	90.49%
27	2047	48.04%	46.56%	94.60%	46.71%	45.28%	91.99%
28	2048	48.29%	47.25%	95.54%	47.14%	46.13%	93.27%
29	2049	48.49%	47.90%	96.39%	47.49%	46.91%	94.40%
30	2050	48.65%	48.50%	97.15%	47.77%	47.61%	95.38%
31	2051	48.75%	49.02%	97.77%	47.97%	48.24%	96.21%
32	2052	48.81%	49.50%	98.31%	48.14%	48.82%	96.96%
33	2053	48.82%	49.93%	98.75%	48.25%	49.34%	97.59%
34	2054	48.81%	50.31%	99.12%	48.33%	49.81%	98.14%
35	2055	48.78%	50.65%	99.43%	48.37%	50.23%	98.60%
36	2056	48.73%	50.96%	99.69%	48.39%	50.60%	98.99%
37	2057	48.65%	51.22%	99.87%	48.37%	50.93%	99.30%
38	2058	48.54%	51.41%	99.95%	48.33%	51.19%	99.52%
39	2059	48.43%	51.56%	99.99%	48.29%	51.41%	99.70%
40	2060	48.33%	51.67%	100.00%	48.25%	51.57%	99.82%

d) Adoption Rate of IMA and LTA

Since the agency is not mandating any applications, we next made an assumption concerning at what rate IMA and LTA could be adopted voluntarily by industry. We contracted with the Intelligent Transportation Society of America (ITS America, or ITS) to conduct a study to better understand the utilization of DSRC among stakeholders and to investigate potential safety application deployment and product development.[369] As part of the effort, ITS identified an array of V2V and vehicle-to-infrastructure (V2I) apps and interviewed 42 stakeholders specifically about these apps' development and deployment. The stakeholders interviewed included chipset manufacturers, mobile device manufacturers, infrastructure industrial equipment makers, vehicle original equipment manufacturers (OEMs), and academia. Based on the interview results, ITS America concluded that about 91 apps (including both V2V and V2I) would likely to be deployed within 5 years of a DSRC mandate. IMA and LTA were rated among the highest priority apps among all the interviewees.

The ITS study confirmed many aspects of the agency's proposed requirements and assumptions regarding potential V2V deployment including the proposed implementation timing. However, the study was not able to predict clearly a safety application adoption trend after an initial deployment. To fill this gap and establish a potential trend, the agency examined the adoption patterns of the three crash avoiding warning systems reported as part of regular data submissions associated with the agency's New Car Assessment Program (NCAP). The crash avoiding warning systems are blind spot detection (BSD), forward collision warning (FCW), and Lane Departure Warning (LDW). We note that only FCW and LDW are currently reported on NHTSA's Safer Car technologies as being "Recommended Technologies," while BSD is reported to NHTSA for research purposes but not, at this time, presented to the public.

Table VII-29 lists the adoption rates for these systems that were offered as standard equipment and the combined adoption rates for the technologies offered as standard or optional. As shown, the rate of the standard equipment is relatively low, although it increases gradually. In contrast, the rate for the optional equipment (based on the combined rates) was much higher and the pace of the offering these features increased faster. These warning technologies are projected to reach the full combined deployment around 2021 based on a curve linear regression model resulting in an estimated full deployment spanning ten years. This projected rate is absent any sort of formal regulation beyond the inclusion in the agency's NCAP ratings program.

Table VII-29 Reported Adoption Rates by Vehicle Manufacturers (percent)

Year	BSD		FCW		LDW	
	Standard	Combined*	Standard	Combined*	Standard	Combined*

[369] Impact of Light Vehicle Rule on Consumer/Aftermarket Adoption- Dedicated Short Range Communications Market Study, Intelligent Transportation Society of America, FHWA-JPO-17-487, available at http://ntl.bts.gov/lib/60000/60500/60535/FHWA-JPO-17-487_Final_.pdf (last accessed Dec 12, 2016)

2011	0.3	11.9	0.0	11.4	0.0	2.5
2012	1.0	30.0	0.0	11.4	0.0	5.9
2013	1.3	30.4	0.8	21.0	0.0	17.4
2014	0.1	27.0	2.6	22.1	0.2	15.8
2015	0.6	45.7	5.6	57.3	2.5	52.7

*standard equipment and optional equipment combined.

The agency believes a similar, market-driven approach could take hold for V2V technology once the equipment becomes widely available and consumers recognize the potential benefits. The agency believes that IMA and LTA could be adopted as standard equipment on a schedule similar to the "combined" schedules for the FCW and LDW displayed in the NCAP data.

Based on broad collection of implementation information such as, the ITS study, NCAP data, agency meetings with manufacturers, announcements on V2V implementation from vehicle industry, and the cost consideration; the agency established the a safety application adoption trend of 0% for the first MY vehicles that have DSRC radios, 5%, 10%, 25%, 40%, 65%, 90%, and 100% for each following MY vehicles, respectively. The agency notes that the pattern is similar to those shown in the NCAP data; with slow initial rate spanning approximately two years and then increasing year over year at a rate that would reach full adoption in the eighth year of the implementation of the DSRC technology. Under this adoption scenario, IMA and LTA would not be deployed in the first year. In the second year, with the required 75 percent DSRC installation rate and the five percent safety application adoption among the DSRC-equipped vehicles, five percent of the total new vehicles (= 0.05 * 0.75) are expected to have the two safety applications. In the third year, 10 percent of the new vehicles (= 0.1 * 1.00) would have the apps, and so on so forth. Overall, the benefits (and costs) of the proposed rule were estimated based on this specific technology adoption scenario, as shown in Table VII-27. However, in order to test the significant uncertainty in this assumption, we included adoption rate as one of the variables in our uncertainty analysis.

The agency, though, requests comment on these assumption. Do commenters have more concrete data concerning the potential or likely adoption rate of these applications? Are there any other technologies that have been voluntarily introduced into the fleet that the agency should consider when projecting the potential adoption rate of IMA and LTA?

2. Injury and Property Damage Benefits

a) Annual Injury and Property Damage Benefits

(1) Maximum Annual Benefits

The maximum annual benefits represent the crashes, fatalities, injuries, and property damage vehicles (PDOVs) that can be reduced annually after the *full adoption* of DSRC and safety related applications.[370] Once fully deployed, the agency estimates the proposed rule would:

- Prevent 439,000 to 615,000 crashes annually
- equivalent to 13 to 18 percent of multiple light-vehicle crashes
- Save 987 to 1,366 lives
- Reduce 305,000 to 418,000 MAIS 1-5 injuries,[371] and
- Eliminate 537,000 to 746,000 property damage only vehicles (PDOVs)

(2) Annual Benefits

The annual benefits are summarized every five years from 2021 to 2060 in Table VII-30. As shown, the proposed rule would not yield benefits in Year 1 due to the zero percent safety application adoption rates for new vehicles in that year. However, the agency estimates that five years after a final rule is issued, Year 5 (2025), 10,094 to 13,763 annual vehicle crashes would potentially be prevented, saving 23 to 31 lives and preventing 6,946 to 9,197 MAIS 1-5 injuries. Moreover, the agency estimates this proposed rule has the potential to prevent 12,496 to 16,949 damaged vehicles.

As the fleet penetration increases, the proposed rule could prevent 107,120 to 147,615 crashes, save 244 to 332 lives, and reduce 73,983 to 99,254 MAIS 1-5 injuries by Year 10, a more than ten-fold increase from Year 5.

After 20 years, the agency estimates about 80 percent of the maximum benefits will be achievable. The yields an estimated to 349,914 to 487,561 crashes prevented, 789 to 1,089 lives save, and the reduction of 242,589 to 329,909 MAIS 1-5 injuries.

Table VII-30 Summary of Annual Benefits of the Proposed Rule (Undiscounted)

	Calendar	Crashes	Fatalities	MAIS 1-5 Injuries	PDOVs

[370] Would occur 43 years after the first implementation

[371] MAIS (Maximum Abbreviated Injury Scale) represents the maximum injury severity of an occupant at an Abbreviated Injury Scale (AIS) level. AIS ranks individual injuries by body region on a scale of 1 to 6: 1=minor, 2=moderate, 3=serious, 4=severe, 5=critical, and 6=maximum (untreatable).

Year	Year	Low	High	Low	High	Low	High	Low	High
1	2021	0	0	0	0	0	0	0	0
5	2025	10,094	13,763	23	31	6,946	9,197	12,496	16,949
10	2030	107,120	147,615	244	332	73,983	99,254	131,946	180,693
15	2035	241,740	335,287	547	751	167,329	226,278	296,835	408,920
20	2040	349,914	487,561	789	1,087	242,589	329,909	428,697	593,093
25	2045	401,894	561,737	904	1,249	278,926	380,771	491,628	682,127
30	2050	424,901	594,569	955	1,321	295,009	403,284	519,483	721,535
35	2055	435,932	610,326	980	1,355	302,723	414,094	532,831	740,437
40	2060	439,138	615,028	987	1,365	304,986	417,366	536,657	745,996

b) Lifetime Injury and Property Damage Benefits by Vehicle Model Year

The lifetime benefits for a MY vehicle (also MY Benefits), as described earlier, represent the total benefits that would be accrued through the life of a vehicle. The MY benefits represent the total benefits that would be accrued though the life of a vehicle. The lifetime benefits can occur at any time during the in-use life of a vehicle and are required to be discounted to reflect their present values (2014 dollars). The discounting procedures for future benefits and costs in regulatory analyses are based on the guidelines published in OMB Circular A-4 and OMB Circular A-94 Revised.

The agency's analysis for determining lifetime benefits uses two approaches. One approach is a so-called "free rider" approach and the other is the "no free-rider" approach, where the primary difference is the treatment on the distribution of benefits from crashes involving different MY vehicles.

The "free-rider approach" is based on the notion that the lifetime benefits of a specific MY vehicle should correspond to the investment up to that specific MY of vehicles and that benefits should be credited to the later MY vehicles. For example, if benefits are from a crash that involved a MY 2021 vehicle and a MY 2030 vehicle, under this approach, all benefits would be credited to the MY 2030 vehicle. The MY 2021 vehicle would not receive any benefits because the benefits would not be realized until the investment on the MY 2030 vehicles is made. In contrast, the "no free-rider" approach is based on the notion that benefits should be shared among all vehicles since the future investment will continue because of the proposed rule. With the same case above, the no free-rider approach allows both MY 2021 and MY 2030 vehicles to share a portion of the benefits. Additional details on the methodology and derivation of benefits of these two approaches can be found in Chapter V of the PRIA prepared in support of this proposal.

(1) Injury and Property Damage Benefits by Model Year and Approach

Table VII-31 and Table VII-32 show the MY specific injury and property damage benefits (i.e., the lifetime benefits for a specific MY vehicle) for the "free rider approach" for the

3 and 7 percent discount, respectively. In parallel, Table VII-33 and Table VII-34 show the benefits for the "no free-rider" approach also at a 3 and 7 percent discount rate, respectively.

The analysis estimates the lifetime benefits only for MYs 2021 to 2050 vehicles. For 2050 MY vehicles, its lifetime benefits would be realized from year 2040 to year 2086. As described in the annual benefit section, the annual benefits would be stabilized at the maximum level around year 2062. Furthermore, after MY 2050, vehicle sales were assumed to at the MY 2050 level. Therefore, the lifetime benefits for vehicles newer than MY 2050 would be stabilized at the MY 2050 level.

Table VII-31 MY Benefits for Light Vehicles Free-Rider Approach @3 Percent Discount

	Model	Crash Prevented		Fatalities Eliminated		MAIS 1-5 Injuries		PDOVs	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2021	0	0	0	0	0	0	0	0
2	2022	271	369	1	1	187	246	336	455
3	2023	1,821	2,484	4	6	1,254	1,660	2,255	3,059
4	2024	8,138	11,116	19	25	5,604	7,436	10,066	13,675
5	2025	20,094	27,510	46	62	13,847	18,427	24,828	33,799
6	2026	45,766	62,828	104	142	31,567	42,151	56,477	77,072
7	2027	86,774	119,428	198	269	59,905	80,243	106,948	146,292
8	2028	125,283	172,790	285	389	86,552	116,237	154,257	211,408
9	2029	151,801	209,713	345	471	104,932	141,211	186,755	256,340
10	2030	175,685	243,053	398	545	121,501	163,794	215,991	296,855
11	2031	196,823	272,641	446	611	136,178	183,866	241,830	332,755
12	2032	215,458	298,792	488	669	149,129	201,633	264,580	364,439
13	2033	231,828	321,830	524	720	160,518	217,309	284,539	392,308
14	2034	247,041	343,282	558	767	171,108	231,922	303,068	418,229
15	2035	260,349	362,101	588	809	180,382	244,762	319,252	440,931
16	2036	271,907	378,496	614	845	188,445	255,966	333,289	460,676
17	2037	282,112	393,009	636	877	195,570	265,900	345,664	478,129
18	2038	290,458	404,930	655	903	201,406	274,078	355,763	492,430
19	2039	297,903	415,591	671	926	206,617	281,402	364,761	505,202
20	2040	305,087	425,875	687	948	211,645	288,466	373,446	517,525
21	2041	312,804	436,885	704	972	217,039	296,015	382,788	530,741
22	2042	305,604	427,030	688	950	212,077	289,414	373,891	518,632
23	2043	308,426	431,146	694	959	214,065	292,270	377,270	523,513
24	2044	310,949	434,815	699	967	215,841	294,812	380,294	527,871
25	2045	313,325	438,253	705	974	217,510	297,187	383,150	531,965
26	2046	315,443	441,309	709	981	218,996	299,295	385,700	535,611
27	2047	317,611	444,417	714	987	220,514	301,432	388,318	539,332
28	2048	319,665	447,353	719	994	221,951	303,447	390,802	542,853
29	2049	321,616	450,138	723	1,000	223,315	305,356	393,165	546,196
30	2050	323,726	453,138	728	1,006	224,788	307,409	395,724	549,803

Table VII-32 MY Benefits for Light Vehicles Free-Rider Approach @7 Percent Discount

	Model	Crash Prevented		Fatalities Eliminated		MAIS 1-5 Injuries		PDOVs	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2021	0	0	0	0	0	0	0	0
2	2022	256	348	1	1	176	232	317	429
3	2023	1,703	2,322	4	5	1,172	1,552	2,109	2,860
4	2024	7,517	10,264	17	23	5,175	6,865	9,300	12,630
5	2025	18,321	25,071	42	57	12,623	16,789	22,643	30,811
6	2026	41,157	56,470	94	128	28,383	37,874	50,801	69,294
7	2027	77,149	106,128	176	239	53,251	71,286	95,110	130,038
8	2028	110,525	152,362	251	343	76,343	102,466	136,116	186,464
9	2029	133,399	184,211	303	414	92,198	124,008	164,150	225,223
10	2030	154,035	213,015	349	478	106,513	143,518	189,411	260,228
11	2031	172,397	238,716	391	535	119,263	160,954	211,857	291,412
12	2032	188,544	261,378	427	585	130,486	176,350	231,570	318,868
13	2033	202,920	281,609	459	630	140,486	190,116	249,097	343,341
14	2034	216,257	300,416	489	672	149,771	202,927	265,341	366,065
15	2035	227,911	316,898	515	708	157,892	214,173	279,513	385,947
16	2036	238,068	331,308	537	740	164,978	224,022	291,846	403,300
17	2037	247,120	344,183	558	768	171,299	232,835	302,824	418,783
18	2038	254,424	354,622	574	791	176,407	239,999	311,659	431,301
19	2039	260,956	363,981	588	811	180,980	246,431	319,551	442,510
20	2040	267,247	372,995	602	831	185,384	252,625	327,152	453,305
21	2041	273,843	382,418	617	851	189,997	259,091	335,132	464,608
22	2042	267,553	373,820	602	832	185,665	253,336	327,356	454,035
23	2043	270,054	377,472	608	839	187,427	255,872	330,347	458,363
24	2044	272,178	380,572	612	846	188,924	258,023	332,888	462,038
25	2045	274,288	383,630	617	853	190,407	260,137	335,424	465,677
26	2046	276,078	386,219	621	858	191,664	261,926	337,576	468,762
27	2047	278,074	389,079	625	864	193,061	263,891	339,986	472,186
28	2048	279,772	391,511	629	870	194,250	265,562	342,038	475,099
29	2049	281,380	393,809	633	875	195,374	267,140	343,983	477,855
30	2050	283,192	396,388	637	880	196,640	268,906	346,180	480,956

Table VII-33 MY Benefits for Light Vehicles No Free-Rider Approach @3 Percent Discount

	Model	Crash Prevented		Fatalities Eliminated		MAIS 1-5 Injuries		PDOVs	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2021	0	0	0	0	0	0	0	0
2	2022	4,006	5,506	9	12	2,764	3,697	4,941	6,750
3	2023	12,297	16,917	28	38	8,488	11,363	15,159	20,727
4	2024	34,161	47,041	78	106	23,588	31,616	42,093	57,606
5	2025	59,813	82,461	136	186	41,316	55,459	73,659	100,913
6	2026	104,216	143,863	237	323	72,020	96,827	128,262	175,926
7	2027	153,676	212,415	349	477	106,247	143,074	189,014	259,566
8	2028	180,917	250,375	410	562	125,133	168,761	222,387	305,740
9	2029	190,032	263,281	430	590	131,488	177,573	233,465	321,299
10	2030	199,389	276,526	451	619	138,010	186,614	244,840	337,269
11	2031	207,808	288,476	470	645	143,885	194,784	255,061	351,656
12	2032	215,391	299,268	487	669	149,181	202,173	264,254	364,628
13	2033	222,098	308,843	502	690	153,870	208,741	272,371	376,118
14	2034	228,851	318,485	517	711	158,591	215,353	280,546	387,688
15	2035	234,712	326,883	530	729	162,695	221,125	287,627	397,746
16	2036	239,796	334,194	541	745	166,258	226,159	293,758	406,483
17	2037	244,444	340,890	551	760	169,518	230,774	299,356	414,478
18	2038	248,150	346,265	559	771	172,124	234,492	303,807	420,872
19	2039	251,493	351,122	566	782	174,475	237,855	307,817	426,644
20	2040	254,958	356,134	574	792	176,909	241,317	311,982	432,615
21	2041	258,973	361,900	583	805	179,722	245,284	316,828	439,511
22	2042	251,474	351,552	566	782	174,540	238,321	307,596	426,854
23	2043	252,797	353,515	569	786	175,478	239,695	309,167	429,160
24	2044	254,138	355,482	572	790	176,425	241,064	310,767	431,486
25	2045	255,409	357,336	574	794	177,320	242,350	312,289	433,684
26	2046	256,606	359,072	577	798	178,162	243,551	313,725	435,749
27	2047	257,844	360,856	580	802	179,030	244,781	315,217	437,879
28	2048	258,876	362,342	582	805	179,754	245,805	316,460	439,653
29	2049	259,929	363,853	584	808	180,492	246,844	317,732	441,462
30	2050	261,241	365,723	587	812	181,408	248,125	319,322	443,708

Table VII-34 MY Benefits for Light Vehicles No Free-Rider Approach @7 Percent Discount

	Model	Crash Prevented		Fatalities Eliminated		MAIS 1-5 Injuries		PDOVs	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2021	0	0	0	0	0	0	0	0
2	2022	3,026	4,154	7	9	2,087	2,787	3,735	5,096
3	2023	9,423	12,946	21	29	6,501	8,689	11,624	15,874
4	2024	26,555	36,520	60	82	18,328	24,527	32,742	44,755
5	2025	46,855	64,517	107	145	32,352	43,361	57,736	79,010
6	2026	82,119	113,231	187	255	56,727	76,161	101,122	138,557
7	2027	121,940	168,381	277	378	84,277	113,350	150,052	205,873
8	2028	144,104	199,249	327	447	99,640	134,231	177,213	243,433
9	2029	152,069	210,514	345	472	105,191	141,918	186,899	257,022
10	2030	160,196	222,006	363	497	110,854	149,758	196,784	270,886
11	2031	167,621	232,533	379	521	116,033	156,950	205,804	283,568
12	2032	174,185	241,865	394	541	120,615	163,337	213,764	294,792
13	2033	180,128	250,340	407	559	124,769	169,145	220,962	304,969
14	2034	186,049	258,785	420	578	128,907	174,934	228,133	315,108
15	2035	191,219	266,186	432	594	132,525	180,018	234,382	323,976
16	2036	195,680	272,596	441	608	135,651	184,430	239,763	331,640
17	2037	199,807	278,538	450	621	138,545	188,523	244,737	338,737
18	2038	202,975	283,135	457	631	140,773	191,705	248,540	344,204
19	2039	205,888	287,369	464	640	142,823	194,636	252,034	349,234
20	2040	208,845	291,652	470	649	144,901	197,597	255,587	354,333
21	2041	212,188	296,460	478	660	147,244	200,908	259,617	360,079
22	2042	205,999	287,930	464	640	142,969	195,173	251,993	349,638
23	2043	207,175	289,675	466	644	143,803	196,394	253,389	351,688
24	2044	208,251	291,263	468	647	144,564	197,502	254,669	353,558
25	2045	209,421	292,967	471	651	145,388	198,684	256,071	355,582
26	2046	210,280	294,224	473	654	145,994	199,557	257,098	357,069
27	2047	211,429	295,876	475	657	146,799	200,694	258,483	359,043
28	2048	212,258	297,073	477	660	147,381	201,521	259,481	360,471
29	2049	213,224	298,458	479	663	148,057	202,472	260,648	362,129
30	2050	214,216	299,875	481	666	148,751	203,445	261,848	363,829

(2) Summary of Injury and Property Damage Benefits by Model Year

Under both approaches, the MY benefits were derived by dividing the annual benefits among all involved MY vehicles according to their survived volume and vehicle miles traveled. Afterwards, the annual benefits for that specific MY vehicles were discounted by multiplying them with an appropriate discounting factor. Finally, we summed the annual discounted benefits of that MY vehicles over their operational lifespan to derive the MY benefits. These benefits were discounted at a 3 percent and 7 percent discount rate to represent their present value. Table VII-35 and Table VII-36 presents the discounted MY benefits from MY 2021 to MY 2050

vehicles for every five MYs. As shown, the first MY vehicles (i.e., MY 2021) would not accrue benefits due to the adoption scenario used in the PRIA. At a three percent discount rate, the 5th applicable MY vehicles (MY 2025) would prevent 20,094 to 82,481 crashes, save 46 to 186 lives, and reduce 13,847 to 55459 MAIS 1-5 injuries. At this discount, the MY 2025 would also eliminate 24,828 to 100,913 PDOVs. The 30th MY vehicles (MY 2050) would prevent 261,241 to 453,138 crashes, save 587 to 1,006 lives, reduce 181,408 to 307,409 injuries, and eliminate up to 549,803 PDOVs.

At a seven percent discount rate, MY 2025 vehicles would prevent 18,321 to 65,517 crashes, save 42 to 145 lives, reduce 12,623 to 43,361 MAIS 1-5 injuries and eliminate 22,643 to 79,010 PDOVs. The MY 2050 vehicles would prevent 214,216 to 396,388 crashes, save 481 to 880 lives, reduce 148,741 to 268,906 MAIS 1-5 injuries, and eliminate up to 480,956 PDOVs.

Table VII-35 Summary of MY Injury and Property Damage Benefits (@3% Discount)

	Model	Crashes		Fatalities		MAIS 1-5 Injuries		PDOVs	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2021	0	0	0	0	0	0	0	0
5	2025	20,094	82,461	46	186	13,847	55,459	24,828	100,913
10	2030	175,685	276,526	398	619	121,501	186,614	215,991	337,269
15	2035	234,712	362,101	530	809	162,695	244,762	287,627	440,931
20	2040	254,958	425,875	574	948	176,909	288,466	311,982	517,525
25	2045	255,409	438,253	574	974	177,320	297,187	312,289	531,965
30	2050	261,241	453,138	587	1,006	181,408	307,409	319,322	549,803

Table VII-36 Summary of MY Injury and Property Damage Benefits (@7% Discount)

	Model	Crashes		Fatalities		MAIS 1-5 Injuries		PDOVs	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2021	0	0	0	0	0	0	0	0
5	2025	18,321	64,517	42	145	12,623	43,361	22,643	79,010
10	2030	154,035	222,006	349	497	106,513	149,758	189,411	270,886
15	2035	191,219	316,898	432	708	132,525	214,173	234,382	385,947
20	2040	208,845	372,995	470	831	144,901	252,625	255,587	453,305
25	2045	209,421	383,630	471	853	145,388	260,137	256,071	465,677
30	2050	214,216	396,388	481	880	148,751	268,906	261,848	480,956

Note that the range of benefits is due to the use of a range of effectiveness rates and the two MY benefit estimating approaches. The two benefit approaches, labeled as "free-rider" and "no free-rider" approaches, deployed a different treatment on the distribution of benefits from crashes involving different MY vehicles.

3. Monetized Benefits

The agency developed the monetized benefits by applying the comprehensive cost for a fatality to the total equivalent lives saved (i.e., fatal equivalents) in accordance with Department of Transportation 2015 guidance.[372]. The guidance requires the identified nonfatal MAIS injuries and PDOVs to be expressed in terms of fatalities. This is done by comparing the comprehensive cost of preventing nonfatal injuries to that of preventing a fatality. Comprehensive costs include economic costs and the value of quality life (QALYs). Economic costs reflect the tangible costs of reducing fatalities and injuries which includes savings from medical care, emergency services, insurance administration, workplace costs, legal costs, congestion and property damage, as well as lost productivity. The QALY captures the intangible value of lost quality-of-life that results from potential fatalities and injuries.

Table VII-37 shows the comprehensive values and the relative fatality ratios for MAIS injuries and PDOVs that were used to derived the fatal equivalents.[373] As shown, the comprehensive cost of preventing a fatality is currently valued at $9.7 million. A MAIS 5 injury, for example, is 0.6136 fatal equivalents. Thus, monetized benefits can be derived by multiplying $9.7 million by the derived fatal equivalents.

Table VII-37 also shows the unit costs for congestion and property damage. These two costs are considered to be part of the comprehensive costs. The congestion and property damage costs are provided now for later use when calculating the net costs of the proposed rule. The net costs are defined as the total vehicle costs minus the savings from reducing property damage and crash related congestion.

Table VII-37 Unit Congestion, Property Damage, and Comprehensive Cost (2014 $)

Injury Category	Congestion	Property Damage	Comprehensive Cost	Relative Fatality Ratio
PDOVs	$2,280	$3,908	$6,591	0.0007
MAIS 0	$1,535	$2,923	$4,753	0.0005
MAIS 1	$1,545	$8,641	$47,144	0.0049
MAIS 2	$1,572	$9,239	$449,239	0.0463
MAIS 3	$1,615	$17,400	$1,065,032	0.1097
MAIS 4	$1,638	$17,727	$2,612,382	0.2690

[372] "Guidance on the Treatment of the Economic Value of a Statistical Life (VSL) in U.S. Department of Transportation Analyses" February 28, 2013, https://www.transportation.gov/sites/dot.dev/files/docs/DOT%202013%20Signed%20VSL%20Memo.pdf (last accessed Dec 8, 2106)

[373] Revise to 2014 $ from the unit costs published in this report, Blincoe, L. J., Miller, T. R., Zaloshnja, E., & Lawrence, B. A. (2015, May). The economic and societal impact of motor vehicle crashes, 2010. (Revised) (Report No. DOT HS 812 013). Washington, DC: National Highway Traffic Safety Administration

MAIS 5	$1,657	$16,385	$5,958,375	0.6136
Fatality	$6,200	$12,172	$9,710,659	1.0000

a) Monetized Annual Benefits

Table VII-38 provides the undiscounted annual fatal equivalents, monetized benefits, and property damage and congestion savings of the proposed rule from the year 2021 to 2060. As shown, by Year 5 the proposed rule is estimated to save 129 to 169 fatal equivalents totaling approximately $1.3 to $1.6 billion annually. Approximately 12 percent of the monetized savings, $176 to $237 million, are from the estimated reduction of property damage and congestion. By the year 2060, with V2V fully deployed, the proposed rule is estimated to save approximately 5,631 to 7,613 fatal equivalents annually. Finally, the total associated monetized annual savings would range from $54.7 to $73.9 billion. Of these savings, $7.7 to $10.6 billion is estimated to be property damage and congestion savings.

b) Maximum Monetized Annual Benefit

The proposed rule would save a maximum of $54.7 to $74.0 billion annually after the full adoption of DSRC radios and the two safety apps. Of these amounts, $7.7 to $10.6 billion are the potential savings from reducing crash related congestion and vehicle property damage.

Table VII-38 Annual Monetized Benefits (Undiscounted, 2014 $ in Millions)

	Calendar	Fatal Equivalents		Total Monetized Benefits		Property Damage and Congestion	
Year	Year	Low	High	Low	High	Low	High
1	2021	0.00	0.00	$0.00	$0.00	$0.00	$0.00
2	2022	1.98	2.57	$19.18	$24.99	$2.69	$3.60
3	2023	12.98	16.97	$126.05	$164.75	$17.67	$23.75
4	2024	50.94	66.58	$494.62	$646.51	$69.35	$93.20
5	2025	129.38	169.32	$1,256.34	$1,644.21	$176.14	$237.00
6	2026	273.40	358.63	$2,654.86	$3,482.52	$372.24	$501.88
7	2027	492.69	648.24	$4,784.30	$6,294.87	$670.88	$906.96
8	2028	760.14	1,003.08	$7,381.47	$9,740.54	$1,035.15	$1,403.08
9	2029	1,055.03	1,395.74	$10,245.07	$13,553.52	$1,436.84	$1,951.93
10	2030	1,373.29	1,820.47	$13,335.53	$17,677.94	$1,870.39	$2,545.51
11	2031	1,708.97	2,269.74	$16,595.21	$22,040.63	$2,327.71	$3,173.24
12	2032	2,055.46	2,734.45	$19,959.89	$26,553.31	$2,799.80	$3,822.44
13	2033	2,406.57	3,206.42	$23,369.32	$31,136.42	$3,278.19	$4,481.66
14	2034	2,756.78	3,678.26	$26,770.14	$35,718.29	$3,755.42	$5,140.59
15	2035	3,099.49	4,141.07	$30,098.04	$40,212.46	$4,222.44	$5,786.78
16	2036	3,427.08	4,584.47	$33,279.20	$44,518.16	$4,668.90	$6,405.77
17	2037	3,734.36	5,001.37	$36,263.04	$48,566.54	$5,087.70	$6,987.66
18	2038	4,016.39	5,384.96	$39,001.73	$52,291.53	$5,472.13	$7,522.96
19	2039	4,267.25	5,727.35	$41,437.81	$55,616.35	$5,814.11	$8,000.63
20	2040	4,486.82	6,028.11	$43,569.99	$58,536.92	$6,113.46	$8,420.10
21	2041	4,674.40	6,286.06	$45,391.52	$61,041.76	$6,369.24	$8,779.76
22	2042	4,829.59	6,500.30	$46,898.45	$63,122.18	$6,580.86	$9,078.39
23	2043	4,958.71	6,679.27	$48,152.35	$64,860.05	$6,756.97	$9,327.77
24	2044	5,065.75	6,827.92	$49,191.70	$66,303.56	$6,902.96	$9,534.88
25	2045	5,153.64	6,950.12	$50,045.25	$67,490.21	$7,022.85	$9,705.13
26	2046	5,228.04	7,053.49	$50,767.72	$68,493.96	$7,124.33	$9,849.14
27	2047	5,293.45	7,144.11	$51,402.88	$69,373.99	$7,213.54	$9,975.43
28	2048	5,351.13	7,223.76	$51,963.02	$70,147.39	$7,292.20	$10,086.44
29	2049	5,402.91	7,295.12	$52,465.83	$70,840.43	$7,362.81	$10,185.94
30	2050	5,448.79	7,358.22	$52,911.30	$71,453.12	$7,425.36	$10,273.91
31	2051	5,486.64	7,410.41	$53,278.83	$71,959.96	$7,476.97	$10,346.67
32	2052	5,519.98	7,456.51	$53,602.60	$72,407.63	$7,522.44	$10,410.92
33	2053	5,547.41	7,494.52	$53,868.95	$72,776.73	$7,559.85	$10,463.88
34	2054	5,570.75	7,526.96	$54,095.66	$73,091.76	$7,591.69	$10,509.08
35	2055	5,590.30	7,554.13	$54,285.50	$73,355.51	$7,618.36	$10,546.93
36	2056	5,606.76	7,577.01	$54,445.28	$73,577.69	$7,640.80	$10,578.80
37	2057	5,618.70	7,593.79	$54,561.30	$73,740.69	$7,657.10	$10,602.17
38	2058	5,625.16	7,603.20	$54,623.95	$73,832.03	$7,665.92	$10,615.22
39	2059	5,629.36	7,609.56	$54,664.73	$73,893.77	$7,671.66	$10,624.03
40	2060	5,631.45	7,612.92	$54,685.04	$73,926.44	$7,674.53	$10,628.67

c) Monetized Benefits by Vehicle Model Year

The range of the monetized benefits by vehicle model year (I.e., the lifetime benefits of a MY vehicles) represents the estimates from both the "free-rider" and "no free-rider" approaches. The lower bound of the range represents the low estimate from the "free-rider" approach and upper bound represents the high estimate of "no free-rider" approach. For each approach, the low and high estimates correspond to the low and high app effectiveness, respectively. Table VII-39 and

Table VII-40 show the monetized MY benefits at a 3 percent and 7 percent discount rate, respectively.

As shown, at a three percent discount rate, MY 2022 vehicles would save 3 to 68 fatal equivalent and $33.8 to $659.0 million over their lifespan. MY 2050 vehicles would save a total 3,350 to 5,608 fatal equivalents and $32.5 to $54.5 billion. The property damage and congestion savings would range from $4.7 to $94.9 million for MY 2022 vehicles and $4.6 to $7.8 billion for 2050 MY vehicles.

At a seven percent discount rate, the MY 2022 vehicles would save 3 to 51 fatal equivalents and $31.8 to $497.0 million over their lifespan. MY 2050 vehicles would save a total 2,747 to 4,906 fatal equivalents and $26.7 to $47.6 billion. Of these monetized savings, the property damage and congestion savings are estimated to be $4.5 to $71.6 million for MY 2022 vehicles and $3.7 to $6.8 billion for 2050 MY vehicles.

Table VII-39 Monetized MY Benefits @3 Percent Discount (2014 $ in Millions)

	Model	Fatal Equivalents		Total Monetized Benefits		Property Damage and Congestion	
Year	Year	Low	High	Low	High	Low	High
1	2021	0.00	0.00	$0.00	$0.00	$0.00	$0.00
2	2022	3.48	67.86	$33.79	$658.99	$4.74	$94.91
3	2023	23.35	208.55	$226.72	$2,025.12	$31.79	$291.65
4	2024	104.31	580.04	$1,012.92	$5,632.53	$142.02	$811.11
5	2025	257.57	1,017.05	$2,501.20	$9,876.22	$350.72	$1,422.05
6	2026	586.69	1,774.90	$5,697.12	$17,235.41	$798.94	$2,481.38
7	2027	1,112.42	2,621.45	$10,802.30	$25,455.98	$1,515.02	$3,664.44
8	2028	1,606.16	3,090.78	$15,596.91	$30,013.55	$2,187.63	$4,320.00
9	2029	1,946.18	3,250.93	$18,898.69	$31,568.66	$2,650.90	$4,543.36
10	2030	2,252.45	3,415.26	$21,872.79	$33,164.45	$3,068.24	$4,772.57
11	2031	2,523.52	3,563.63	$24,505.02	$34,605.22	$3,437.64	$4,979.46
12	2032	2,761.74	3,697.69	$26,818.31	$35,906.98	$3,762.58	$5,166.34
13	2033	2,847.78	3,975.69	$27,653.77	$38,606.57	$3,879.91	$5,555.21
14	2034	2,934.41	4,241.63	$28,495.06	$41,189.00	$3,998.06	$5,926.26
15	2035	3,009.61	4,475.08	$29,225.26	$43,456.01	$4,100.63	$6,251.90
16	2036	3,074.84	4,678.59	$29,858.67	$45,432.21	$4,189.61	$6,535.69
17	2037	3,134.46	4,858.86	$30,437.71	$47,182.69	$4,270.96	$6,787.01
18	2038	3,182.03	5,007.07	$30,899.56	$48,621.96	$4,335.86	$6,993.56
19	2039	3,224.93	5,139.68	$31,316.16	$49,909.68	$4,394.41	$7,178.33
20	2040	3,269.38	5,267.60	$31,747.87	$51,151.88	$4,455.07	$7,356.56
21	2041	3,320.90	5,404.46	$32,248.10	$52,480.81	$4,525.34	$7,547.30
22	2042	3,224.76	5,283.11	$31,314.49	$51,302.48	$4,394.39	$7,377.52
23	2043	3,241.75	5,334.51	$31,479.52	$51,801.61	$4,417.60	$7,449.02
24	2044	3,258.96	5,380.31	$31,646.62	$52,246.36	$4,441.10	$7,512.74
25	2045	3,275.27	5,423.17	$31,805.05	$52,662.57	$4,463.36	$7,572.40
26	2046	3,290.63	5,461.25	$31,954.16	$53,032.36	$4,484.32	$7,625.42
27	2047	3,306.52	5,499.93	$32,108.44	$53,407.94	$4,505.99	$7,679.31
28	2048	3,319.75	5,536.44	$32,236.99	$53,762.45	$4,524.05	$7,730.18
29	2049	3,333.27	5,571.05	$32,368.22	$54,098.58	$4,542.49	$7,778.42
30	2050	3,350.10	5,608.31	$32,531.65	$54,460.39	$4,565.44	$7,830.37

Table VII-40 Monetized MY Benefits @7 Percent Discount (2014 $ in Millions)

	Model	Fatal Equivalents		Total Monetized Benefits		Property Damage and Congestion	
Year	Year	Low	High	Low	High	Low	High
1	2021	0.00	0.00	$0.00	$0.00	$0.00	$0.00
2	2022	3.28	51.18	$31.80	$497.03	$4.46	$71.59
3	2023	21.83	159.55	$212.00	$1,549.29	$29.72	$223.15
4	2024	96.35	450.18	$935.65	$4,371.50	$131.19	$629.59
5	2025	234.85	795.52	$2,280.53	$7,725.00	$319.78	$1,112.43
6	2026	527.59	1,396.62	$5,123.26	$13,562.13	$718.45	$1,952.75
7	2027	989.03	2,077.54	$9,604.09	$20,174.30	$1,346.94	$2,904.40
8	2028	1,416.94	2,459.15	$13,759.41	$23,879.93	$1,929.87	$3,437.45
9	2029	1,710.25	2,598.90	$16,607.61	$25,236.98	$2,329.50	$3,632.38
10	2030	1,974.86	2,741.45	$19,177.23	$26,621.24	$2,690.07	$3,831.23
11	2031	2,149.18	2,947.24	$20,869.91	$28,619.59	$2,927.85	$4,119.15
12	2032	2,233.37	3,227.88	$21,687.48	$31,344.84	$3,042.66	$4,510.89
13	2033	2,309.61	3,478.57	$22,427.83	$33,779.21	$3,146.63	$4,860.73
14	2034	2,385.57	3,711.72	$23,165.40	$36,043.23	$3,250.21	$5,186.03
15	2035	2,451.89	3,916.19	$23,809.50	$38,028.75	$3,340.68	$5,471.24
16	2036	2,509.12	4,095.07	$24,365.23	$39,765.77	$3,418.75	$5,720.68
17	2037	2,562.08	4,254.99	$24,879.46	$41,318.79	$3,490.99	$5,943.64
18	2038	2,602.73	4,384.79	$25,274.25	$42,579.22	$3,546.47	$6,124.52
19	2039	2,640.12	4,501.23	$25,637.28	$43,709.92	$3,597.49	$6,286.75
20	2040	2,678.06	4,613.37	$26,005.75	$44,798.85	$3,649.27	$6,442.98
21	2041	2,720.95	4,730.53	$26,422.20	$45,936.55	$3,707.77	$6,606.25
22	2042	2,641.60	4,624.69	$25,651.68	$44,908.74	$3,599.70	$6,458.14
23	2043	2,656.70	4,670.32	$25,798.30	$45,351.86	$3,620.32	$6,521.61
24	2044	2,670.51	4,709.04	$25,932.43	$45,727.85	$3,639.18	$6,575.46
25	2045	2,685.53	4,747.17	$26,078.29	$46,098.16	$3,659.68	$6,628.54
26	2046	2,696.56	4,779.45	$26,185.33	$46,411.61	$3,674.73	$6,673.47
27	2047	2,711.29	4,815.03	$26,328.44	$46,757.14	$3,694.84	$6,723.04
28	2048	2,721.94	4,845.29	$26,431.78	$47,050.95	$3,709.36	$6,765.20
29	2049	2,734.33	4,873.87	$26,552.13	$47,328.48	$3,726.26	$6,805.02
30	2050	2,747.06	4,905.91	$26,675.71	$47,639.58	$3,743.62	$6,849.69

The agency seeks comment on all aspects of the monetized benefits developed for this proposal. More specifically, the assumptions used for the benefits calculations which are the basis the estimates. Please provide any supporting data for the comments. If necessary, the agency has processes and procedures for submitting confidential business information.

4. Non-Quantified Benefits

As discussed above, the agency has only quantified potential benefits of this rule derived from the assumed adoption of IMA and LTA. Although this assumption allows the agency to provide a reasonable quantification of the potential benefits of this rulemaking, it does not account for many other potential benefits of V2V. The non-quantified benefits of the proposed rule can come from several sources: (1) the effects of enhancing vehicle-resident safety systems, (2) the incremental benefits over the current vehicle-resident safety systems, (3) the potential impact of the next generation V2V apps that would actively assist drivers to avoid crashes rather than simply issuing warnings, (4) the impact of enabling wide range deployment of V2P and V2I apps, and (5) the effects of adding V2V sensor input to other sensors utilized for automation. The agency does not quantify the potential impacts of these sources primarily due to lack of data (e.g., effectiveness of the apps, incremental effective rate of the V2V apps over the vehicle-resident systems, etc.) that can be used to discern these benefits.

a) The Effect for Enhancing Vehicle-Resident Safety Systems

For vehicles equipped with current on-board sensors, V2V can offer a fundamentally different, but complementary, source of information that can significantly enhance the reliability and accuracy of the information available. Instead of relying on each vehicle to sense its surroundings on its own, V2V enables surrounding vehicles to help each other by reporting safety information to each other. V2V communication can also detect threat vehicles that are not in the sensors' field of view, and can use a V2V signal to validate a return from a vehicle-based sensor. This added capability can potentially lead to improved warning timing and a reduction in the number of false warnings, thereby adding confidence to the overall safety system, and increasing consumer satisfaction and acceptance. The vehicle-resident FCW, LCM/BSW systems can be improved by BSMs. However, the agency could not quantify the benefit due to lack of the measurement of how BSM can improve the vehicle-resident systems.

b) Incremental Benefits of the V2V Apps

Due to the sensing advantage of the V2V apps, the agency believes that these apps also have some incremental benefits over the vehicle-resident version of the systems. For example, V2V-based FCW and LCM might perform better than the vehicle-resident systems. However, benefits from these apps could accrue if they add a marginal effectiveness to the existing in-vehicle systems, or if they enable the installation of these apps in vehicles that do not voluntarily have these systems. This later effect would occur due to the significant marginal cost reduction for these apps that would result from V2V. However, we do not have sufficient data to determine the marginal effectiveness of V2V for these apps and the added installation rates. Therefore, we did not quantify this type of benefits.

c) Potential Impact of Next Generation V2V Apps

The agency believes that the V2V apps will be evolved as did the vehicle-resident systems. The next generation V2V apps, we envision, can also actively assist drivers to avoid crashes as did the vehicle-resident crash avoidance systems (such as advance brake assist). Furthermore, the new apps might be applicable to motorcycle crashes. V2V could increase the adoption of these apps to lower incremental cost.

d) The Impact of Enabling V2P and V2I Apps

The V2V also is the foundation for the deployment V2P and V2I apps. For V2P, pedestrians can carry devices (such as mobile phones) with a V2V chip that can send out a safety signal to V2V devices in the vehicles and vice versa. Both the driver and the pedestrian could be warned if a possible conflict arises. Specifically, V2P can protect pedestrians in crosswalk and improve mobility. However, there are many issues to be resolved concerning V2P apps. The agency is developing a research plan that will investigate issues relating to V2P communication, safety applications, and human factors, and among other things.

The same communications technology that supports V2V apps could also enable a broader set of safety and mobility applications when combined with compatible roadway infrastructure. The potential V2I apps have been identified included: Red Light Violation Warning, Curve Speed Warning, Stop Sign Gap Assist, Reduced Speed Zone Warning, Spot Weather Information Warning, Stop Sign Violation Warning, Railroad Crossing Violation Warning, and Oversize Vehicle Warning.[374] These V2I apps can mitigate congestion and facilitate green transportation choices, thus reducing the energy consumptions and environmental impacts.

e) The Effects of Paving the Way for Automation

We believe that V2X technology may be necessary to realize the full potential of vehicle automation (e.g., self-driving vehicles), as such communication would provide a vehicle with the highest level of awareness of its surroundings, which is likely necessary in situations where the driver cedes all control of safety-critical functions and relies on the vehicle to monitor roadway and driving conditions.

E. Breakeven Analysis

The agency conducted a breakeven analysis of the proposed rule's estimated costs and benefits. The analysis is used to determine when the cumulative estimated benefits will recoup

[374] The Connected Vehicle Core System Architecture, See www.its.dot.gov/research/systems_engineering.htm (last accessed Jan. 9, 2014).

the investment made up to that year. In essence, this analysis determines the year that the total investment of the proposed rule will be paid back through the total realized benefits of the proposed rule. The total investment of the proposed rule for a year is the cumulative annual costs from the first year of implementation up to that year. Similarly, the total realized benefits would be the cumulative monetized annual benefits from the first year of implementation up to that year. All annual costs and monetized benefits used in this analysis are discounted back to 2021, the projected first year of implementation of the proposed rule. In determining the potential breakeven point, the agency needed to develop the undiscounted annual net benefits yielding the values shown in Table VII-41. As shown, undiscounted, the proposed rule would accrue a positive annual benefit around 2026 and 2027.

Table VII-41 Annual Net Benefits (Undiscounted, 2014 $ in Millions)

	Calendar	Total Monetized Benefits		Annual Costs		Annual Net Benefits	
Year	Year	Low	High	Low	High	Low	High
1	2021	$0	$0	$2,192	$2,864	-$2,864	-$2,192
2	2022	$19	$25	$3,011	$3,926	-$3,907	-$2,986
3	2023	$126	$165	$3,832	$4,946	-$4,820	-$3,668
4	2024	$495	$647	$3,741	$4,981	-$4,486	-$3,095
5	2025	$1,256	$1,644	$3,701	$4,803	-$3,547	-$2,057
6	2026	$2,655	$3,483	$3,655	$4,735	-$2,080	-$173
7	2027	$4,784	$6,295	$3,640	$4,705	$79	$2,655
8	2028	$7,381	$9,741	$3,634	$4,690	$2,692	$6,106
9	2029	$10,245	$13,554	$3,622	$4,668	$5,577	$9,931
10	2030	$13,336	$17,678	$3,649	$4,692	$8,643	$14,029
11	2031	$16,595	$22,041	$3,659	$4,699	$11,896	$18,381
12	2032	$19,960	$26,553	$3,662	$4,699	$15,261	$22,891
13	2033	$23,369	$31,136	$3,665	$4,699	$18,670	$27,471
14	2034	$26,770	$35,718	$3,682	$4,719	$22,051	$32,036
15	2035	$30,098	$40,212	$3,717	$4,757	$25,341	$36,495
16	2036	$33,279	$44,518	$3,713	$4,731	$28,548	$40,805
17	2037	$36,263	$48,567	$3,734	$4,726	$31,537	$44,833
18	2038	$39,002	$52,292	$3,749	$4,736	$34,266	$48,543
19	2039	$41,438	$55,616	$3,769	$4,858	$36,580	$51,847
20	2040	$43,570	$58,537	$3,831	$4,844	$38,726	$54,706
21	2041	$45,392	$61,042	$3,856	$4,872	$40,519	$57,186
22	2042	$46,898	$63,122	$3,737	$4,715	$42,183	$59,385
23	2043	$48,152	$64,860	$3,744	$4,719	$43,434	$61,116
24	2044	$49,192	$66,304	$3,752	$4,723	$44,469	$62,552
25	2045	$50,045	$67,490	$3,796	$4,764	$45,281	$63,695
26	2046	$50,768	$68,494	$3,770	$4,736	$46,032	$64,724
27	2047	$51,403	$69,374	$3,780	$4,745	$46,658	$65,594
28	2048	$51,963	$70,147	$3,789	$4,752	$47,211	$66,359
29	2049	$52,466	$70,840	$3,797	$4,759	$47,707	$67,043
30	2050	$52,911	$71,453	$3,858	$4,818	$48,093	$67,595

31	2051	$53,279	$71,960	$3,822	$4,761	$48,518	$68,138
32	2052	$53,603	$72,408	$3,813	$4,732	$48,870	$68,594
33	2053	$53,869	$72,777	$3,805	$4,719	$49,150	$68,972
34	2054	$54,096	$73,092	$3,797	$4,810	$49,285	$69,295
35	2055	$54,285	$73,356	$3,832	$4,766	$49,520	$69,523
36	2056	$54,445	$73,578	$3,782	$4,711	$49,734	$69,795
37	2057	$54,561	$73,741	$3,775	$4,700	$49,862	$69,966
38	2058	$54,624	$73,832	$3,768	$4,688	$49,936	$70,064
39	2059	$54,665	$73,894	$3,761	$4,677	$49,987	$70,133
40	2060	$54,685	$73,926	$3,804	$4,717	$49,968	$70,122

Table VII-42 and Table VII-43 show the discounted cumulative annual benefits, cumulative annual costs, cumulative annual net benefits, and breakeven year at a 3 and 7 percent rate, respectively. As shown, the proposed rule would be expected to break even between 2029 and 2031 for a 3 percent discount rate and 2030 to 2032 for a 7 percent discount rate.

Table VII-42 Breakeven Analysis (@3 Percent, 2014 $ in Millions)

Year	Calendar Year	Cumulative Monetized Benefits		Total Cumulative Annual Costs		Cumulative Net Benefits		Breakeven Year	
		Low	High	Low	High	Low	High	Low	High
1	2021	$0	$0	$2,160	$2,822	-$2,822	-$2,160	*	*
2	2022	$18	$24	$5,040	$6,578	-$6,559	-$5,016	*	*
3	2023	$135	$177	$8,600	$11,172	-$11,036	-$8,423	*	*
4	2024	$581	$760	$11,973	$15,663	-$15,081	-$11,213	*	*
5	2025	$1,681	$2,199	$15,213	$19,868	-$18,186	-$13,014	*	*
6	2026	$3,938	$5,160	$18,320	$23,892	-$19,954	-$13,161	*	*
7	2027	$7,886	$10,354	$21,324	$27,775	-$19,889	-$10,970	*	*
8	2028	$13,800	$18,158	$24,236	$31,533	-$17,732	-$6,078	*	*
9	2029	$21,769	$28,700	$27,053	$35,164	-$13,395	$1,647	*	2029
10	2030	$31,840	$42,050	$29,809	$38,707	-$6,867	$12,241	*	2030
11	2031	$44,007	$58,211	$32,492	$42,152	$1,855	$25,719	2031	2031
12	2032	$58,215	$77,111	$35,099	$45,497	$12,718	$42,013	2032	2032
13	2033	$74,365	$98,630	$37,632	$48,744	$25,621	$60,998	2033	2033
14	2034	$92,328	$122,597	$40,102	$51,911	$40,417	$82,494	2034	2034
15	2035	$111,934	$148,791	$42,524	$55,009	$56,925	$106,267	2035	2035
16	2036	$132,980	$176,944	$44,872	$58,001	$74,979	$132,072	2036	2036
17	2037	$155,245	$206,764	$47,165	$60,903	$94,342	$159,599	2037	2037
18	2038	$178,494	$237,935	$49,400	$63,726	$114,768	$188,536	2038	2038
19	2039	$202,478	$270,126	$51,581	$66,537	$135,941	$218,545	2039	2039
20	2040	$226,960	$303,018	$53,734	$69,259	$157,701	$249,284	2040	2040
21	2041	$251,726	$336,322	$55,837	$71,918	$179,808	$280,485	2041	2041
22	2042	$276,568	$369,758	$57,817	$74,415	$202,153	$311,941	2042	2042
23	2043	$301,328	$403,109	$59,742	$76,841	$224,486	$343,367	2043	2043
24	2044	$325,889	$436,214	$61,616	$79,200	$246,690	$374,599	2044	2044
25	2045	$350,146	$468,927	$63,455	$81,509	$268,637	$405,472	2045	2045

26	2046	$374,038	$501,160	$65,229	$83,738	$290,300	$435,931	2046	2046
27	2047	$397,524	$532,857	$66,956	$85,906	$311,618	$465,901	2047	2047
28	2048	$420,574	$563,975	$68,637	$88,014	$332,561	$495,337	2048	2048
29	2049	$443,171	$594,486	$70,273	$90,063	$353,108	$524,213	2049	2049
30	2050	$465,294	$624,360	$71,886	$92,078	$373,216	$552,474	2050	2050
31	2051	$486,919	$653,569	$73,437	$94,010	$392,909	$580,132	2051	2051
32	2052	$508,044	$682,104	$74,940	$95,875	$412,169	$607,165	2052	2052
33	2053	$528,654	$709,949	$76,396	$97,681	$430,974	$633,553	2053	2053
34	2054	$548,751	$737,102	$77,806	$99,468	$449,283	$659,296	2054	2054
35	2055	$568,332	$763,562	$79,189	$101,187	$467,145	$684,373	2055	2055
36	2056	$587,399	$789,329	$80,513	$102,837	$484,562	$708,816	2056	2056
37	2057	$605,949	$814,401	$81,797	$104,435	$501,515	$732,604	2057	2057
38	2058	$623,981	$838,772	$83,040	$105,982	$517,999	$755,732	2058	2058
39	2059	$641,501	$862,455	$84,246	$107,481	$534,020	$778,210	2059	2059
40	2060	$658,513	$885,454	$85,429	$108,949	$549,565	$800,025	2060	2060

*not breakeven

Table VII-43 Breakeven Analysis (@7 Percent, 2014 $ in Millions)

Year	Calendar Year	Cumulative Monetized Benefits		Total Cumulative Annual Costs		Cumulative Net Benefits		Breakeven Year	
	Year	Low	High	Low	High	Low	High	Low	High
1	2021	$0	$0	$2,119	$2,768	-$2,768	-$2,119	*	*
2	2022	$17	$23	$4,840	$6,316	-$6,299	-$4,817	*	*
3	2023	$124	$162	$8,076	$10,492	-$10,369	-$7,914	*	*
4	2024	$514	$672	$11,028	$14,423	-$13,909	-$10,356	*	*
5	2025	$1,441	$1,884	$13,757	$17,965	-$16,524	-$11,873	*	*
6	2026	$3,271	$4,285	$16,277	$21,228	-$17,958	-$11,992	*	*
7	2027	$6,353	$8,340	$18,622	$24,260	-$17,907	-$10,282	*	*
8	2028	$10,796	$14,204	$20,810	$27,083	-$16,287	-$6,606	*	*
9	2029	$16,560	$21,829	$22,847	$29,709	-$13,149	-$1,018	*	*
10	2030	$23,572	$31,124	$24,766	$32,176	-$8,604	$6,358	*	2030
11	2031	$31,727	$41,955	$26,564	$34,485	-$2,759	$15,391	*	2031
12	2032	$40,894	$54,151	$28,246	$36,643	$4,251	$25,905	2032	2032
13	2033	$50,925	$67,515	$29,819	$38,660	$12,264	$37,695	2033	2033
14	2034	$61,665	$81,845	$31,297	$40,554	$21,111	$50,548	2034	2034
15	2035	$72,949	$96,920	$32,690	$42,337	$30,612	$64,230	2035	2035
16	2036	$84,610	$112,520	$33,991	$43,995	$40,615	$78,528	2036	2036
17	2037	$96,486	$128,425	$35,214	$45,542	$50,943	$93,211	2037	2037
18	2038	$108,420	$144,426	$36,361	$46,992	$61,429	$108,065	2038	2038
19	2039	$120,271	$160,333	$37,439	$48,381	$71,891	$122,893	2039	2039
20	2040	$131,918	$175,980	$38,463	$49,676	$82,242	$137,516	2040	2040
21	2041	$143,257	$191,228	$39,427	$50,893	$92,364	$151,801	2041	2041
22	2042	$154,207	$205,967	$40,299	$51,994	$102,214	$165,668	2042	2042
23	2043	$164,714	$220,119	$41,116	$53,023	$111,691	$179,003	2043	2043
24	2044	$174,744	$233,639	$41,881	$53,986	$120,758	$191,757	2044	2044
25	2045	$184,283	$246,502	$42,605	$54,894	$129,388	$203,898	2045	2045
26	2046	$193,325	$258,701	$43,276	$55,738	$137,587	$215,425	2046	2046
27	2047	$201,883	$270,252	$43,905	$56,528	$145,355	$226,346	2047	2047
28	2048	$209,969	$281,167	$44,495	$57,267	$152,701	$236,672	2048	2048
29	2049	$217,597	$291,467	$45,047	$57,959	$159,638	$246,420	2049	2049
30	2050	$224,788	$301,177	$45,571	$58,614	$166,174	$255,606	2050	2050
31	2051	$231,554	$310,316	$46,057	$59,219	$172,336	$264,260	2051	2051
32	2052	$237,917	$318,911	$46,509	$59,780	$178,136	$272,402	2052	2052
33	2053	$243,891	$326,982	$46,931	$60,304	$183,587	$280,051	2053	2053
34	2054	$249,501	$334,562	$47,325	$60,803	$188,698	$287,236	2054	2054
35	2055	$254,761	$341,670	$47,697	$61,264	$193,497	$293,973	2055	2055
36	2056	$259,688	$348,329	$48,039	$61,691	$197,997	$300,290	2056	2056
37	2057	$264,304	$354,567	$48,358	$62,088	$202,216	$306,209	2057	2057
38	2058	$268,625	$360,407	$48,656	$62,459	$206,166	$311,751	2058	2058
39	2059	$272,665	$365,868	$48,934	$62,805	$209,860	$316,934	2059	2059
40	2060	$276,443	$370,976	$49,197	$63,131	$213,313	$321,779	2060	2060

*not breakeven

Table VII-44 summarizes the breakeven year for the proposed rule based on the estimated costs and monetized benefits.

Table VII-44 Summary of the Breakeven Year of the proposed rule

Discount Rate	Year
At 3 Percent	2029 to 2031
At 7 Percent	2030 to 2032

F. Cost Effectiveness and Positive Net Benefits Analysis

1. Cost Effectiveness

The cost-effectiveness analysis identifies the model year the agency estimates the net cost per fatal equivalent is no greater than the $9.7 million comprehensive cost of a fatality, indicating the point at which cost of the propose rule is lower than a fatal equivalent. For this analysis, the agency defines the net cost as the difference between a given MY cost and the congestion benefits and PDO savings (i.e., the lifetime savings of these two categories for a given vehicle MY).

For each discount rate, the range of fatal equivalents covers those from the two benefits estimating approaches discussed previously Section VII.D: free-rider and no free-rider. The low fatal equivalent numbers represent the low benefit estimates from the free-rider approach and the high estimates represent the higher benefit estimates from the no free-rider approach. Additionally, the cost-related low and high values represent the two potential cost estimates that result from utilizing a one-radio or two-radio approach to DSRC implementation approach.[375]

The agency utilizes the net cost per equivalent life saved to determine the cost-effectiveness for a given vehicle MY. The net cost defined in this analysis is the difference between the MY costs and the savings from reducing property damage and congestion. As described in Section VII.D.3, fatal equivalents are derived by translating the MAIS 1-5 injuries saved and the PDOVs prevented into fatalities using the calculated relative fatality ratios found in Table VII-37.

[375] The one-DSRC radio consists of one DSRC radio in vehicle paring with a hybrid (WiFi/Cellular/Satellite) vehicle-to-SCMS communication. The two DSRC radios in vehicle are paring with DSRC vehicle-to-SCMS communication.

Table VII-45 and Table VII-46 present the factors used when determine cost-effectiveness, the net cost per fatal equivalent discounted at 3 percent and 7 percent, respectively, and when the agency estimates the proposed rule would become cost-effective. As shown in the tables, the agency estimates the proposed rule would become cost effective in MY 2024 to MY 2026 regardless of the discount rate. Note that the negative MY net cost shown in the tables means that the MY benefits outweigh its costs.

Table VII-45 Cost-Effectiveness Analysis (@3 Percent, 2014 $ in Millions)

	Model	Fatal Equivalents		MY Net Costs		Net Cost per Fatal Equivalent		Cost-Effective	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2021	0.00	0.00	$2,221.39	$2,893.52	$2,221.39	$2,893.52	*	*
2	2022	3.48	67.86	$2,958.11	$3,963.34	$43.59	$1,138.99	*	*
3	2023	23.35	208.55	$3,592.36	$4,965.74	$17.23	$212.68	*	*
4	2024	104.31	580.04	$2,975.53	$4,884.16	$5.13	$46.82	2024	*
5	2025	257.57	1,017.05	$2,317.96	$4,491.28	$2.28	$17.44	2025	*
6	2026	586.69	1,774.90	$1,208.85	$3,970.64	$0.68	$6.77	2026	2026
7	2027	1,112.42	2,621.45	$7.03	$3,221.61	$0.00	$2.90	2027	2027
8	2028	1,606.16	3,090.78	-$657.77	$2,530.40	-$0.21	$1.58	2028	2028
9	2029	1,946.18	3,250.93	-$896.40	$2,042.34	-$0.28	$1.05	2029	2029
10	2030	2,252.45	3,415.26	-$1,101.36	$1,645.84	-$0.32	$0.73	2030	2030
11	2031	2,523.52	3,563.63	-$1,301.00	$1,280.31	-$0.37	$0.51	2031	2031
12	2032	2,761.74	3,697.69	-$1,487.91	$952.38	-$0.40	$0.34	2032	2032
13	2033	2,847.78	3,975.69	-$1,876.58	$833.11	-$0.47	$0.29	2033	2033
14	2034	2,934.41	4,241.63	-$2,233.79	$731.05	-$0.53	$0.25	2034	2034
15	2035	3,009.61	4,475.08	-$2,526.26	$664.36	-$0.56	$0.22	2035	2035
16	2036	3,074.84	4,678.59	-$2,816.23	$547.13	-$0.60	$0.18	2036	2036
17	2037	3,134.46	4,858.86	-$3,048.91	$459.30	-$0.63	$0.15	2037	2037
18	2038	3,182.03	5,007.07	-$3,242.04	$402.76	-$0.65	$0.13	2038	2038
19	2039	3,224.93	5,139.68	-$3,409.01	$463.44	-$0.66	$0.14	2039	2039
20	2040	3,269.38	5,267.60	-$3,527.55	$387.12	-$0.67	$0.12	2040	2040
21	2041	3,320.90	5,404.46	-$3,692.67	$345.44	-$0.68	$0.10	2041	2041
22	2042	3,224.76	5,283.11	-$3,646.00	$315.00	-$0.69	$0.10	2042	2042
23	2043	3,241.75	5,334.51	-$3,711.27	$294.44	-$0.70	$0.09	2043	2043
24	2044	3,258.96	5,380.31	-$3,768.41	$274.41	-$0.70	$0.08	2044	2044
25	2045	3,275.27	5,423.17	-$3,785.48	$292.50	-$0.70	$0.09	2045	2045
26	2046	3,290.63	5,461.25	-$3,865.08	$242.56	-$0.71	$0.07	2046	2046
27	2047	3,306.52	5,499.93	-$3,909.53	$228.66	-$0.71	$0.07	2047	2047
28	2048	3,319.75	5,536.44	-$3,952.52	$216.58	-$0.71	$0.07	2048	2048
29	2049	3,333.27	5,571.05	-$3,992.64	$204.60	-$0.72	$0.06	2049	2049
30	2050	3,350.10	5,608.31	-$3,984.67	$240.58	-$0.71	$0.07	2050	2050

* The proposed rule would not be cost effective for the MY vehicles since the net cost per fatal equivalent is greater than $9.7M in 2014 dollars.

Table VII-46 Cost-Effectiveness Analysis (@7 Percent, 2014 $ in Millions)

	Model	Fatal Equivalents		MY Net Costs		Net Cost per Fatal Equivalent		Cost-Effective	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2021	0.00	0.00	$2,213.68	$2,885.80	$2,213.68	$2,885.80	*	*
2	2022	3.28	51.18	$2,969.81	$3,952.00	$58.02	$1,206.56	*	*
3	2023	21.83	159.55	$3,645.47	$4,952.42	$22.85	$226.83	*	*
4	2024	96.35	450.18	$3,141.76	$4,879.71	$6.98	$50.64	2024	*
5	2025	234.85	795.52	$2,612.54	$4,507.19	$3.28	$19.19	2025	*
6	2026	527.59	1,396.62	$1,722.09	$4,035.73	$1.23	$7.65	2026	2026
7	2027	989.03	2,077.54	$751.28	$3,373.91	$0.36	$3.41	2027	2027
8	2028	1,416.94	2,459.15	$208.58	$2,771.96	$0.08	$1.96	2028	2028
9	2029	1,710.25	2,598.90	-$2.00	$2,347.17	$0.00	$1.37	2029	2029
10	2030	1,974.86	2,741.45	-$177.05	$2,006.97	-$0.06	$1.02	2030	2030
11	2031	2,149.18	2,947.24	-$458.15	$1,772.63	-$0.16	$0.82	2031	2031
12	2032	2,233.37	3,227.88	-$850.33	$1,654.44	-$0.26	$0.74	2032	2032
13	2033	2,309.61	3,478.57	-$1,200.35	$1,548.14	-$0.35	$0.67	2033	2033
14	2034	2,385.57	3,711.72	-$1,512.27	$1,460.19	-$0.41	$0.61	2034	2034
15	2035	2,451.89	3,916.19	-$1,764.75	$1,405.16	-$0.45	$0.57	2035	2035
16	2036	2,509.12	4,095.07	-$2,020.80	$1,298.41	-$0.49	$0.52	2036	2036
17	2037	2,562.08	4,254.99	-$2,225.59	$1,219.23	-$0.52	$0.48	2037	2037
18	2038	2,602.73	4,384.79	-$2,393.47	$1,171.68	-$0.55	$0.45	2038	2038
19	2039	2,640.12	4,501.23	-$2,538.36	$1,239.43	-$0.56	$0.47	2039	2039
20	2040	2,678.06	4,613.37	-$2,635.41	$1,171.48	-$0.57	$0.44	2040	2040
21	2041	2,720.95	4,730.53	-$2,773.58	$1,141.05	-$0.59	$0.42	2041	2041
22	2042	2,641.60	4,624.69	-$2,748.24	$1,088.07	-$0.59	$0.41	2042	2042
23	2043	2,656.70	4,670.32	-$2,805.80	$1,069.77	-$0.60	$0.40	2043	2043
24	2044	2,670.51	4,709.04	-$2,853.41	$1,054.05	-$0.61	$0.39	2044	2044
25	2045	2,685.53	4,747.17	-$2,864.22	$1,073.57	-$0.60	$0.40	2045	2045
26	2046	2,696.56	4,779.45	-$2,936.06	$1,029.21	-$0.61	$0.38	2046	2046
27	2047	2,711.29	4,815.03	-$2,976.53	$1,016.55	-$0.62	$0.37	2047	2047
28	2048	2,721.94	4,845.29	-$3,011.12	$1,007.69	-$0.62	$0.37	2048	2048
29	2049	2,734.33	4,873.87	-$3,043.14	$996.93	-$0.62	$0.36	2049	2049
30	2050	2,747.06	4,905.91	-$3,028.20	$1,038.18	-$0.62	$0.38	2050	2050

* The proposed rule would not be cost effective for the MY vehicles since the net cost per fatal equivalent is greater than $9.7M in 2014 dollars

2. Lifetime Net Benefits for a Specified Model Year

The lifetime net benefits for a specified MY vehicle (i.e., MY net benefits) is the difference between the monetized MY benefits and the corresponding MY costs. Table VII-47 and Table VII-48 show the MY net benefits at a 3 and 7 percent discount rate, respectively. As shown, for both discount rates, MY 2024 to MY 2026 vehicles would accrue positive lifetime net benefits. (Due to rounding errors, discrepancy existed between the monetized MY benefits that were deriving directly by multiplying $9.7 million by fatal equivalents and those reported in the tables below.)

Table VII-47 MY Net Benefits (@3 Percent, 2014 $ in Millions)

Year	Model Year	Monetized MY Benefits		MY Costs		MY Net Benefits	
		Low	High	Low	High	Low	High
1	2021	$0.00	$0.00	$2,221.39	$2,893.52	-$2,893.52	-$2,221.39
2	2022	$33.79	$658.99	$3,053.02	$3,968.08	-$3,934.29	-$2,394.03
3	2023	$226.72	$2,025.12	$3,884.01	$4,997.52	-$4,770.80	-$1,858.89
4	2024	$1,012.92	$5,632.53	$3,786.63	$5,026.18	-$4,013.26	$1,845.90
5	2025	$2,501.20	$9,876.22	$3,740.01	$4,842.01	-$2,340.81	$6,136.21
6	2026	$5,697.12	$17,235.41	$3,690.23	$4,769.58	$927.54	$13,545.18
7	2027	$10,802.30	$25,455.98	$3,671.47	$4,736.63	$6,065.67	$21,784.52
8	2028	$15,596.91	$30,013.55	$3,662.23	$4,718.02	$10,878.89	$26,351.32
9	2029	$18,898.69	$31,568.66	$3,646.96	$4,693.24	$14,205.45	$27,921.70
10	2030	$21,872.79	$33,164.45	$3,671.21	$4,714.08	$17,158.71	$29,493.24
11	2031	$24,505.02	$34,605.22	$3,678.46	$4,717.95	$19,787.07	$30,926.76
12	2032	$26,818.31	$35,906.98	$3,678.43	$4,714.96	$22,103.36	$32,228.55
13	2033	$27,653.77	$38,606.57	$3,678.63	$4,713.02	$22,940.75	$34,927.94
14	2034	$28,495.06	$41,189.00	$3,692.47	$4,729.11	$23,765.95	$37,496.53
15	2035	$29,225.26	$43,456.01	$3,725.64	$4,764.99	$24,460.27	$39,730.37
16	2036	$29,858.67	$45,432.21	$3,719.46	$4,736.74	$25,121.92	$41,712.75
17	2037	$30,437.71	$47,182.69	$3,738.10	$4,730.26	$25,707.44	$43,444.60
18	2038	$30,899.56	$48,621.96	$3,751.52	$4,738.62	$26,160.94	$44,870.43
19	2039	$31,316.16	$49,909.68	$3,769.32	$4,857.85	$26,458.31	$46,140.36
20	2040	$31,747.87	$51,151.88	$3,829.01	$4,842.19	$26,905.68	$47,322.87
21	2041	$32,248.10	$52,480.81	$3,854.63	$4,870.78	$27,377.32	$48,626.18
22	2042	$31,314.49	$51,302.48	$3,731.52	$4,709.39	$26,605.10	$47,570.96
23	2043	$31,479.52	$51,801.61	$3,737.75	$4,712.04	$26,767.49	$48,063.86
24	2044	$31,646.62	$52,246.36	$3,744.33	$4,715.51	$26,931.12	$48,502.03
25	2045	$31,805.05	$52,662.57	$3,786.93	$4,755.86	$27,049.18	$48,875.65
26	2046	$31,954.16	$53,032.36	$3,760.35	$4,726.88	$27,227.28	$49,272.01
27	2047	$32,108.44	$53,407.94	$3,769.78	$4,734.65	$27,373.79	$49,638.16
28	2048	$32,236.99	$53,762.45	$3,777.66	$4,740.64	$27,496.35	$49,984.79
29	2049	$32,368.22	$54,098.58	$3,785.78	$4,747.09	$27,621.14	$50,312.80
30	2050	$32,531.65	$54,460.39	$3,845.70	$4,806.01	$27,725.64	$50,614.69

Table VII-48 MY Net Benefits (@7 Percent, 2014 $ in Millions)

Year	Model Year	Monetized MY Benefits		Vehicle Costs		MY Net Benefits	
		Low	High	Low	High	Low	High
1	2021	$0.00	$0.00	$2,213.68	$2,885.80	-$2,885.80	-$2,213.68
2	2022	$31.80	$497.03	$3,041.41	$3,956.46	-$3,924.66	-$2,544.37
3	2023	$212.00	$1,549.29	$3,868.62	$4,982.14	-$4,770.14	-$2,319.34
4	2024	$935.65	$4,371.50	$3,771.35	$5,010.90	-$4,075.25	$600.15
5	2025	$2,280.53	$7,725.00	$3,724.97	$4,826.97	-$2,546.44	$4,000.03
6	2026	$5,123.26	$13,562.13	$3,674.84	$4,754.19	$369.08	$9,887.29
7	2027	$9,604.09	$20,174.30	$3,655.69	$4,720.85	$4,883.24	$16,518.61
8	2028	$13,759.41	$23,879.93	$3,646.03	$4,701.83	$9,057.59	$20,233.89
9	2029	$16,607.61	$25,236.98	$3,630.38	$4,676.66	$11,930.95	$21,606.59
10	2030	$19,177.23	$26,621.24	$3,654.18	$4,697.04	$14,480.18	$22,967.06
11	2031	$20,869.91	$28,619.59	$3,661.00	$4,700.48	$16,169.42	$24,958.59
12	2032	$21,687.48	$31,344.84	$3,660.57	$4,697.09	$16,990.38	$27,684.27
13	2033	$22,427.83	$33,779.21	$3,660.38	$4,694.77	$17,733.06	$30,118.83
14	2034	$23,165.40	$36,043.23	$3,673.77	$4,710.41	$18,455.00	$32,369.46
15	2035	$23,809.50	$38,028.75	$3,706.49	$4,745.84	$19,063.67	$34,322.26
16	2036	$24,365.23	$39,765.77	$3,699.88	$4,717.16	$19,648.07	$36,065.89
17	2037	$24,879.46	$41,318.79	$3,718.05	$4,710.22	$20,169.24	$37,600.74
18	2038	$25,274.25	$42,579.22	$3,731.05	$4,718.15	$20,556.11	$38,848.18
19	2039	$25,637.28	$43,709.92	$3,748.39	$4,836.91	$20,800.36	$39,961.54
20	2040	$26,005.75	$44,798.85	$3,807.57	$4,820.75	$21,185.00	$40,991.28
21	2041	$26,422.20	$45,936.55	$3,832.67	$4,848.82	$21,573.37	$42,103.88
22	2042	$25,651.68	$44,908.74	$3,709.90	$4,687.77	$20,963.91	$41,198.84
23	2043	$25,798.30	$45,351.86	$3,715.80	$4,690.09	$21,108.20	$41,636.06
24	2044	$25,932.43	$45,727.85	$3,722.05	$4,693.23	$21,239.19	$42,005.80
25	2045	$26,078.29	$46,098.16	$3,764.31	$4,733.25	$21,345.04	$42,333.85
26	2046	$26,185.33	$46,411.61	$3,737.41	$4,703.94	$21,481.39	$42,674.20
27	2047	$26,328.44	$46,757.14	$3,746.51	$4,711.38	$21,617.06	$43,010.63
28	2048	$26,431.78	$47,050.95	$3,754.07	$4,717.05	$21,714.73	$43,296.87
29	2049	$26,552.13	$47,328.48	$3,761.88	$4,723.19	$21,828.94	$43,566.60
30	2050	$26,675.71	$47,639.58	$3,821.49	$4,781.80	$21,893.91	$43,818.10

3. Summary

Table VII-49 summarizes the MY vehicles that would be cost-effective.

Table VII-49 Summary of the MY Would Be Cost-Effective and Have Positive Net Benefits

Discount Rate	Cost-Effective	Net Benefits
At 3 Percent	2024 to 2026	2024 to 2026
At 7 Percent	2024 to 2026	2024 to 2026

G. Uncertainty Analysis

In order to account for the inherent uncertainty in the assumptions underlying this cost-benefit analysis, the agency also conducted extensive uncertainty analysis to illustrate the variation in the rule's benefits and costs associated with different assumptions about the future number of accidents that could be prevented, the assumed adoption rates and estimated effectiveness of the two safety applications, and our assumptions about the costs of providing V2V communications capability. This analysis showed that the proposed rule would reach its breakeven year between 2030 and 2032 with 90 percent certainty, with even the most conservative scenario showing that the breakeven year would be five to six years later than the previously estimated years (2029-2032). Considering these same sources of uncertainty in the cost-effectiveness and net benefits analyses showed that the proposed rule would become cost-effective and would accrue positive net benefits between MY 2024 and MY 2027 with 90 percent certainty. This indicates that it is very likely to become cost-effectiveness at most one MY later than estimated in the primary analysis, and that even under the most conservative scenario, this would occur two to three model years later than the initial estimate of 2024-2026.

H. Estimated Costs and Benefits of V2V Alternatives

In the interest of ensuring the agency's proposed approach regulating V2V technology is both fully informed and backed by a comprehensive regulatory analysis, the agency considered two potential alternative approaches for V2V deployment. The first alternative evaluated explores the concept of a potential mandate going beyond V2V communications enabling equipment (radio), which is the preferred alternative, by including a mandate for two safety warning applications: intersection movement assist (IMA) and left turn across path (LTA). The other alternative is an if-equipped rulemaking that would allow V2V communication with requirements as specified in the proposed rule. These two alternatives represent a significant range of potential agency actions beyond the baseline and the proposal.

Of these two alternatives, the first one would ensure the deployment of apps and thus can achieve anticipated benefits. The second alternative (i.e., if-equipped), on the other hand, faces much greater uncertainty regarding the V2V technology adoption than does the proposed rule. Based on the estimated costs of V2V communications and SCMS and the interoperability nature of the V2V communication, the agency believes that the second alternative is unlikely to lead to meaningful deployment of V2V communications. Consequently, the "second alternative would delay potentially for a significant period of time the anticipated benefits of V2V. Furthermore, it is possible that this delay could mean that the designated spectrum for V2V safety applications would be lost. Due to this, as well as to the significant uncertainty surrounding the technology adoption, this alternative was not selected and the agency does not examine the costs and benefits for this alternative.

The agency only examined the costs and benefits of the first alternative. The following describes the alternative proposal and the cost and benefit estimates of this alternative. The process for estimating the benefits and costs of the alternative is the same as is described in Section VII.A above and in the PRIA.

Details of the alternative analyzed include:

- the same phase-in requirements for DSRC equipment in new vehicles as the proposal, 50%-75%-100% three-year phase-in
- a 4 year mandatory phase-for the IMA and LTA safety applications. The phase-in evaluated assumes 0% in the first year, 50% in the second year, 75% in the third year, and 100% implementation by the fourth, final phase-in year.

The alternative approach does allow one additional year of lead time (represented by the first year being zero percent), providing additional flexibility for manufacturers and developers. The staggered approach could help fulfill the agency's interest in moving forward with equipment deployment, speeding the number of units in the fleet transmitting basic safety messages, while allowing more time for the more challenging and resource-intensive safety application development and production implementation. Overall, the agency analysis of this alternative approach assumes a much more aggressive safety application adoption rate, a result of mandating as compared to the "free market" approach taken in the preferred alternative.

In terms of benefits, mandating safety applications in addition to V2V devices would accrue more annual benefits sooner than the preferred alternative would accrue. Once fully deployed, the maximum annual benefits for the "plus applications" alternative are identical to those of the preferred alternative, but those maximum annual benefits would be achieved four years sooner.

When evaluating the costs for this alternative, the agency estimates there would be little change in overall cost from that for the preferred alternative. This lack of cost difference results from the relatively low incremental (piece) costs for safety applications as compared to DSRC radios – as noted, we estimate that applications would cost less than 0.1 percent of the cost of DSRC radios. While this low cost gives us some confidence that manufacturers could realistically undertake to develop such applications and begin deploying them in the field once DSRC is mandated, it does not mean, however, that the agency believes that V2V safety applications could reasonably be mandated, consistent with the Safety Act criteria, without significant additional research to establish practicable and objective test procedures ensuring consistent performance across the fleet.

As a result of the accelerated benefit accrual and flat costs, the "plus applications" alternative would reach the breakeven year between 2027 and 2030, two years sooner than the preferred alternative. The agency estimates the "plus applications" alternative would be cost-effective and accrue positive net benefits between MY 2022 and 2024, also two MYs ahead of the preferred alternative. Table VII-50 compares these visually.

Table VII-50 Comparison of Breakeven and Cost-Effective Measures

	"Plus Applications" Alternative	**Preferred Alternative**
Breakeven (CY)	2027 to 2030	2029 to 2032
Cost-Effective (MY)	2022 to 2024	2024 to 2026
Positive Net Benefits (MY)	2022 to 2024	2024 to 2026

Although mandating safety applications like IMA and LTA along with the V2V communication capability (i.e., DSRC) would result in significant safety benefits sooner, the agency is not proposing to mandate these applications as part of this proposal, because the agency currently does not have sufficient data to proceed with a mandate at this time. As explained above, further research for establishing practicable and objective test procedures and performance requirements for the applications will likely need to be conducted prior to mandate to avoid potential unintended consequences which could have broader negative effects, such as false warnings causing consumers to dismiss the technology, on the development and deployment of V2V-based applications.

Additional details on the analysis of the "plus applications" alternative can be found in the PRIA accompanying this proposal rule.

We request comment on the alternative cost and benefits analysis including the approach for the alternative? Do commenters agree with the costs assumptions used for developing and implementing safety applications? Why or why not? Please provide supporting data. Do commenters agree with our assessment that mandating applications would result in accruing benefits sooner? Do commenters have estimates for the potential costs that an earlier mandate (like, consumer rejection of tech, opportunity cost, etc.) that are not quantified or are not quantifiable but hold great importance? Do commenters have any information that could assist the agency in learning more about these and any other applications that may be useful in a potential agency decision to mandate V2V-enabled safety applications.

VIII. Proposed implementation timing

This section of the NPRM describes the proposed timing for implementing the requirements for new vehicles and aftermarket devices, and also describes our expectations of the availability of the national SCMS.

A. New Vehicles

The agency proposes the following lead time and phase-in period for all new light vehicles sold in the U.S. to comply with this proposed rule.

1. Lead Time

We are proposing two years of lead time, with the two years starting on Sept. 1 following issuance of a final rule to this proposal. This approach would allow a minimum of two full calendars of lead time. New light vehicles manufactured for sale in the U.S. would not be required to comply until that time. NHTSA believes that a lead time period is necessary to allow for the development and production of automotive-grade V2V communications devices by the automotive supplier industry. While a quantity of DSRC devices were developed for the Safety Pilot Model Deployment in Ann Arbor, MI, these were mostly prototype aftermarket devices that were not designed to directly integrate into the vehicle's controller area network. Furthermore, the expected lifespan of these devices is only 3 to 5 years instead of the lifespan of a typical vehicle. Those devices, or ones based on their design, would therefore not be appropriate for meeting this proposed standard. At the time of issuance of this NPRM, we have limited information regarding the capability of automotive suppliers to produce the quantities of DSRC devices to equip all new light vehicles sold in the U.S. annually (approximately 15 million[376]). However, the agency was able to confirm, confidentially, with at least one supplier while gathering information for this proposal that request for quotations were being issued by original equipment manufacturers for V2V capable devices. In addition, the ITSA market study commissioned by the agency indicated the industry would need approximately 18 months to two years to "ramp-up' V2V devices for mass production, considering the device itself and the perceived integration as original equipment are less complex than other technologies such as ESC or powertrain components.

Depending on when the final rule establishing DSRC FMVSS is issued, the agency concurs with the ITSA market study and its own regulatory experience that automotive suppliers with need some lead time to generate production-level devices in the quantities that would be required annually by automotive OEMs.

Lead time also allows the automotive OEMs time to integrate V2V communications devices into their product lines, as these devices are not currently part of any production vehicles sold in the U.S. This will minimize costs by allowing OEMs to incorporate the new technology into product cycle planning. Many OEMs conduct "refreshes" (i.e. minor cosmetic changes, new features, quality fixes, etc.) on their product lines in a staggered fashion approximately three to four years after a major redesign.

For these reasons, the agency is proposing a two year lead time after issuance of the final rule before manufacturers are required to begin complying with the requirements. Two years was chosen because it is approximately half the amount of time between average vehicle refreshes, allowing OEMs to integrate V2V technology into their existing product cycles. This will minimize the cost burden on the OEMs by not requiring concurrent redesigns of all

[376] See the 2015 EIA Annual Energy Outlook, available at http://www.eia.gov/forecasts/aeo/tables_ref.cfm

production lines at the same time. We seek comment on whether this amount of lead time is necessary and appropriate. If commenters believe that additional lead time is needed, or that less lead time is needed, we ask that they support their comments as best as possible with specific information as to why.

2. Phase-In Period

While the agency understands that design changes may be required in order to integrate V2V communications devices into all light vehicles, since V2V technology is a cooperative system, the potential benefits associated with V2V devices depend on a high penetration rate of equipped vehicles. As such, the agency proposes an aggressive phase-in schedule after the conclusion of the lead time period. In addition to the proposed two years of lead time, NHTSA proposes a three year phase-in period. The three year phase-in schedule, which starts immediately after the conclusion of the lead time, would be as follows:

- End of Year 1 – 50% of all new light vehicles must comply with the rule
- End of Year 2 – 75% of all new light vehicles must comply with the rule
- End of Year 3 – 100% of all new light vehicles must comply with the rule

This proposed schedule allows a total of five years until all new vehicles would be required to comply with the final rule. This is consistent with a DOT-sponsored market study[377] conducted by ITS America, in which interviews were conducted with a wide range of V2V stakeholders including:

- Automotive OEMs
- Tier 1 Suppliers
- Tier 2 Suppliers
- Automotive Insurance Companies
- Component Manufacturers
- System Integrators and Service Providers
- Roadside Infrastructure Operators and Manufacturers

The consensus from that research was that OEMs and suppliers will need approximately three to five years after the final rule in order for all new vehicles to comply with the regulation.[378] Therefore, the agency believes that this comprehensive input from the industry

[377] Impact of Light Vehicle Rule on Consumer/Aftermarket Adoption- Dedicated Short Range Communications Market Study, Intelligent Transportation Society of America, FHWA-JPO-17-487, available at http://ntl.bts.gov/lib/60000/60500/60535/FHWA-JPO-17-487_Final_.pdf (last accessed Dec 12, 2016)
[378] Vehicle to Vehicle Crash Avoidance Safety Technology Public Acceptance Final Report - FHWA-JPO-17-491, See Docket No. NHTSA-2016-0126

provides a sufficient justification for the lead time and phase-in period. See Table VIII-1 for the full schedule.

Finally, depending on the number of product lines and the timing of their redesigns, it may be economically advantageous for some OEMs to comply with the regulation prior to the proposed schedule. These OEMs will be able to capitalize on arriving to market earlier than their competitors, and the customers of these OEMs will realize safety, mobility, and environmental benefits earlier than others. As such, the agency does not envision granting credits for early compliance with this schedule as there are sufficient incentives already in place for OEMs to consider early compliance.

Table VIII-1 Proposed Lead Time and Phase-In Schedule

Time Period	Percentage of Vehicles
1 year after final rule	0%
2 years after final rule	0%
3 years after final rule	50%
4 years after final rule	75%
5 years after final rule	100%

B. Aftermarket

Based on market study research,[379] the agency believes that the aftermarket device industry will move quickly (within one year) after the issuance of the final rule to develop and market V2V communications devices that support safety applications as well as mobility, environmental, and other applications. While these aftermarket devices will support V2V, they will also enable more fee-based services such as mobility applications and data and communications suites to be marketed to device owners. While safety is important to consumers, the other applications offered by these devices may be potentially more attractive to the consumer. The agency believes that there will be a market for these aftermarket devices; however, it will be driven by the totality of features offered by these devices that directly impact the consumers' time spent in their vehicles, as well as by device cost.

The agency believes aftermarket device suppliers would need to react to a newly issued FMVSS to capitalize on the large volume of light vehicles that will not be equipped with V2V communications devices. The prevailing view is the market for such aftermarket devices will exist only during the transition period between the issuance of the final rule and the turnover of the entire fleet. NHTSA typically assumes that the maximum life span of a light vehicle is 39 years. We would anticipate that the vast majority of the light vehicle fleet in the U.S. will be completely replaced in less than 20 years, and they will be capable of V2V communications.

[379] "Impact of Light Vehicle Rule on Consumer/Aftermarket Adoption – Dedicated Short Range Communications Market Study", ITS America Research, 2015, pp21

This gives the aftermarket device industry a relatively small window of time to sell aftermarket devices to light vehicles without V2V communications capabilities installed by the OEMs.

Additionally, based on research from the Safety Pilot Model Deployment and additional market research, we believe the aftermarket industry is capable of producing V2V communications devices that can meet the proposed performance requirements and could be installed by a qualified installer, if needed. These aftermarket devices do not need to be connected to the vehicle controller area network vehicle bus; however, an external GPS and V2V antenna will need to be installed as well as a connection to the in-vehicle power. Therefore, the agency expects that specially-trained installers should be able to install these devices in a similar manner to other devices such OnStar FMV, which is installed at major electronics retailers as well as at car dealerships. Therefore, these devices could deploy faster than OEM integrated as they do not require an OEM to integrate them into their vehicle build and testing processes. For these reasons, the agency believes it is technically possible that these devices could be available on the market within one to two years after this proposed FMVSS is finalized.

Based on this, the agency anticipates that aftermarket devices will be available for purchase and installation during the lead time period and prior to the start of the first year of the phase-in period (i.e. less than two years after the final rule is issued).

The agency seeks comment on these lead time projections for both OEM and aftermarket devices. Specifically, do commenters believe the proposed lead times are reasonable? If so, why? If not, why? What type of adjustments, if any, should agency make? Do commenters agree with the agency's perspective on a "window of opportunity" for aftermarket devices? If so, why? If not, why? Please provide any supporting data for your response.

IX. Public Participation

A. How do I prepare and submit comments?

Your comments must be written and in English. To ensure that your comments are correctly filed in the Docket, please include the Docket Number NHTSA–2016–0126 in your comments. Your comments must not be more than 15 pages long.[380] NHTSA established this limit to encourage you to write your primary comments in a concise fashion. However, you may attach necessary additional documents to your comments, and there is no limit on the length of the attachments. If you are submitting comments electronically as a PDF (Adobe) file, we ask that you scan the documents submitted using the Optical Character Recognition (OCR) process,[381] thus allowing the agency to search and copy certain portions of your submissions in

[380] See 49 CFR 553.21.
[381] Optical character recognition (OCR) is the process of converting an image of text, such as a scanned paper document or electronic fax file, into computer-editable text.

order to better evaluate them. Please note that pursuant to the Data Quality Act, in order for the substantive data to be relied upon and used by the agency, it must meet the information quality standards set forth in the OMB and Department of Transportation (DOT) Information Dissemination Quality guidelines. Accordingly, we encourage you to consult the guidelines in preparing your comments. OMB's guidelines may be accessed at https://www.whitehouse.gov/omb/fedreg_reproducible (last accessed Dec. 7, 2016). DOT's guidelines may be accessed at http://www.dot.gov/regulations/dot-information-dissemination-quality-guidelines (last accessed Dec. 7, 2016).

B. Tips for preparing your comments

When submitting comments, please remember to:

- Identify the rulemaking by docket number and other identifying information (subject heading, Federal Register date and page number).
- Explain why you agree or disagree, suggest alternatives, and substitute language for your requested changes.
- Describe any assumptions and provide any technical information and/or data that you used.
- If you estimate potential costs or burdens, explain how you arrived at your estimate in sufficient detail to allow for it to be reproduced.
- Provide specific examples to illustrate your concerns, and suggest alternatives.
- Explain your views as clearly as possible, avoiding the use of profanity or personal threats.
- Make sure to submit your comments by the comment period deadline identified in the DATES section above.

C. How can I be sure that my comments were received?

If you submit your comments by mail and wish Docket Management to notify you upon its receipt of your comments, enclose a self-addressed, stamped postcard in the envelope containing your comments. Upon receiving your comments, Docket Management will return the postcard by mail.

If you submit your comments through www.regulations.gov, you can find very useful information about how to confirm that your comments were successfully received and uploaded under the "Help" link on the top right of the home page, under "FAQs."

D. How do I submit confidential business information?

If you wish to submit any information under a claim of confidentiality, you should submit three copies of your complete submission, including the information you claim to be confidential business information, to the Chief Counsel, NHTSA, at the address given above under **FOR**

NOTE: This document has been signed and we are submitting it for publication in the Federal Register. While we have taken steps to ensure the accuracy of this Internet version of the document, it is not the official version. Please refer to the official version in a forthcoming Federal Register publication or on GPO's Web Site. You can access the Federal Register at: www.federalregister.gov.

FURTHER INFORMATION CONTACT. When you send a comment containing confidential business information, you should include a cover letter setting forth the information specified in our confidential business information regulation.[382]

In addition, you should submit a copy from which you have deleted the claimed confidential business information to the Docket by one of the methods set forth above.

E. Will NHTSA consider late comments?

NHTSA will consider all comments received before midnight E.S.T. on the comment closing date indicated above under **DATES**. To the extent practicable, we will also consider comments received after that date. Additionally, if interested persons believe that any information that NHTSA may place in the docket after the issuance of the NPRM affects their comments, they may submit comments after the closing date concerning how NHTSA should consider that information for the final rule. If a comment is received too late for us to practicably consider in developing a final rule, we will consider that comment as an informal suggestion for future rulemaking action.

F. How can I read the comments submitted by other people?

You may read the materials placed in the docket for this document (*e.g.*, the comments submitted in response to this document by other interested persons) at any time by going to http://www.regulations.gov. Follow the online instructions for accessing the docket.

You may also read the materials at the DOT Docket Management Facility by going to the street address given above under **ADDRESSES**.

X. Regulatory Notices and Analyses

A. Executive Order 12866, Executive Order 13563, and DOT Regulatory Policies and Procedures

Executive Order 12866, "Regulatory Planning and Review" (58 FR 51735, Oct. 4, 1993), as amended by Executive Order 13563, "Improving Regulation and Regulatory Review" (76 FR 3821, Jan. 21, 2011), provides for making determinations whether a regulatory action is "significant" and therefore subject to OMB review and to the requirements of the Executive Order. The Order defines a "significant regulatory action" as one that is likely to result in a rule that may:

- Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity,

[382] See 49 CFR part 512.

competition, jobs, the environment, public health or safety, or State, local, or Tribal governments or communities;

- Create a serious inconsistency or otherwise interfere with an action taken or planned by another agency;
- Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof; or
- Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in the Executive Order.

The rulemaking proposed in this NPRM will be economically significant if adopted. Accordingly, OMB reviewed it under Executive Order 12866. The rule, if adopted, would also be significant within the meaning of the Department of Transportation's Regulatory Policies and Procedures.[383]

The benefits and costs of this proposal are described above in Section VII of this preamble. Because the proposed rule would, if adopted, be economically significant under both the Department of Transportation's procedures and OMB guidelines, the agency has prepared a Preliminary Regulatory Impact Analysis (PRIA) and placed it in the docket and on the agency's website. Further, pursuant to Circular A–4, we have prepared a formal probabilistic uncertainty analysis for this proposal.[384] The circular requires such an analysis for complex rules where there are large, multiple uncertainties whose analysis raises technical challenges or where effects cascade and where the impacts of the rule exceed $1 billion. This proposal meets these criteria on all counts.

B. Regulatory Flexibility Act

Pursuant to the Regulatory Flexibility Act (5 U.S.C. 601 et seq.), as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996, whenever an agency is required to publish a notice of rulemaking for any proposed or final rule, it must prepare and make available for public comment a regulatory flexibility analysis that describes the effect of the rule on small entities (i.e., small businesses, small organizations, and small governmental jurisdictions). The Small Business Administration's regulations at 13 CFR Part 121 define a small business, in part, as a business entity "which operates primarily within the United States." (13 CFR 121.105(a)). No regulatory flexibility analysis is required if the head of an agency certifies the rule will not have a significant economic impact on a substantial number of small entities. SBREFA amended the Regulatory Flexibility Act to require Federal agencies to provide a statement of the factual basis for certifying that a rule will not have a significant economic impact on a substantial number of small entities.

---

[383] DOT Order 2100.5, "Regulatory Policies and Procedures," *available at* http://www.dot.gov/regulations/rulemaking-requirements (last accessed Mar. 16, 2015).
[384] See Chapter 12 of the PRIA accompanying this NPRM.

NHTSA has considered the effects of this proposed rule under the Regulatory Flexibility Act. I certify that this proposed rule will not have a significant economic impact on a substantial number of small entities. The following is NHTSA's statement providing the factual basis for the certification (5 U.S.C. 605(b)).[385]

If adopted, the proposal would directly affect twenty large single stage motor vehicle manufacturers.[386] None of these would qualify as a small business, however. Based on our preliminary assessment, the proposal would also affect 3 entities that fit the Small Business Administration's criteria for a small business (Panoz, Saleen, and Shelby). According to the Small Business Administration's small business size standards (see 13 CFR 121.201), a single stage automobile or light truck manufacturer (NAICS code 336111, Automobile Manufacturing; 336112, Light Truck and Utility Vehicle Manufacturing) must have 1,000 or fewer employees to qualify as a small business. We believe that the rulemaking would not have a significant economic impact on these small vehicle manufacturers because we believe that the market for the products of these several small manufacturers is highly inelastic, and purchasers of these products are enticed by the desire to have an unusual vehicle. Additionally, all vehicle models would incur a similar cost to meet the proposed standard, so raising the price to include the value of V2V technology should not have much, if any, effect on sales of these vehicles, and costs should be able to be passed on to consumers. Based on this analysis, we do not believe that the proposed rule would have a significant economic impact on these three small domestic vehicle manufacturers. Therefore, a regulatory flexibility analysis was not prepared, but we welcome comments on this issue for the final rule.

C. Executive Order 13132 (Federalism)

NHTSA has examined today's proposal pursuant to Executive Order 13132 (64 FR 43255, August 10, 1999) and concluded that no additional consultation with States, local governments or their representatives is mandated beyond the rulemaking process. The agency has concluded that the rulemaking will not have sufficient federalism implications to warrant consultation with State and local officials or the preparation of a federalism summary impact statement. The proposal will not have "substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government."

NHTSA rules can preempt in two ways. First, the National Traffic and Motor Vehicle Safety Act contains an express preemption provision: When a motor vehicle safety standard is in effect under this chapter, a State or a political subdivision of a State may prescribe or continue in

---

[385] See also Chapter 13 of the PRIA accompanying this NPRM.

[386] BMW, Daimler (Mercedes), Fiat/Chrysler (which also includes Ferrari and Maserati), Ford, Geely (Volvo), General Motors, Honda (which includes Acura), Hyundai, Kia, Lotus, Mazda, Mitsubishi, Nissan (which includes Infiniti), Porsche, Subaru, Suzuki, Tata (Jaguar Land Rover), Toyota, and Volkswagen/Audi.

effect a standard applicable to the same aspect of performance of a motor vehicle or motor vehicle equipment only if the standard is identical to the standard prescribed under this chapter. 49 U.S.C. § 30103(b)(1). It is this statutory command by Congress that preempts any non-identical State legislative and administrative law addressing the same aspect of performance.

The express preemption provision described above is subject to a savings clause under which "[c]ompliance with a motor vehicle safety standard prescribed under this chapter does not exempt a person from liability at common law." 49 U.S.C. § 30103(e). Pursuant to this provision, State common law tort causes of action against motor vehicle manufacturers that might otherwise be preempted by the express preemption provision are generally preserved. However, the Supreme Court has recognized the possibility, in some instances, of implied preemption of such State common law tort causes of action by virtue of NHTSA's rules, even if not expressly preempted. This second way that NHTSA rules can preempt is dependent upon there being an actual conflict between an FMVSS and the higher standard that would effectively be imposed on motor vehicle manufacturers if someone obtained a State common law tort judgment against the manufacturer, notwithstanding the manufacturer's compliance with the NHTSA standard. Because most NHTSA standards established by an FMVSS are minimum standards, a State common law tort cause of action that seeks to impose a higher standard on motor vehicle manufacturers will generally not be preempted. However, if and when such a conflict does exist - for example, when the standard at issue is both a minimum and a maximum standard - the State common law tort cause of action is impliedly preempted. See Geier v. American Honda Motor Co., 529 U.S. 861 (2000).

Pursuant to Executive Order 13132 and 12988, NHTSA has considered whether this proposal could or should preempt State common law causes of action. The agency's ability to announce its conclusion regarding the preemptive effect of one of its rules reduces the likelihood that preemption will be an issue in any subsequent tort litigation.

To this end, the agency has examined the nature (e.g., the language and structure of the regulatory text) and objectives of today's proposal and finds that this proposal, like many NHTSA rules, would prescribe only a minimum safety standard. As such, NHTSA does not intend that this proposal preempt state tort law that would effectively impose a higher standard on motor vehicle manufacturers than that to be established by today's proposal. Establishment of a higher standard by means of State tort law would not conflict with the minimum standard announced here. Without any conflict, there could not be any implied preemption of a State common law tort cause of action.

D. Executive Order 12988 (Civil Justice Reform)

With respect to the review of the promulgation of a new regulation, section 3(b) of Executive Order 12988, "Civil Justice Reform" (61 FR 4729; Feb. 7, 1996), requires that Executive agencies make every reasonable effort to ensure that the regulation: (1) clearly specifies the preemptive effect; (2) clearly specifies the effect on existing Federal law or regulation; (3) provides a clear legal standard for affected conduct, while promoting simplification and burden reduction; (4) clearly specifies the retroactive effect, if any; (5)

specifies whether administrative proceedings are to be required before parties file suit in court; (6) adequately defines key terms; and (7) addresses other important issues affecting clarity and general draftsmanship under any guidelines issued by the Attorney General. This document is consistent with that requirement.

Pursuant to this Order, NHTSA notes as follows. The issue of preemption is discussed above. NHTSA notes further that there is no requirement that individuals submit a petition for reconsideration or pursue other administrative proceedings before they may file suit in court.

E. Protection of Children from Environmental Health and Safety Risks

Executive Order 13045, "Protection of Children from Environmental Health and Safety Risks" (62 FR 19855, April 23, 1997), applies to any rule that: (1) is determined to be "economically significant" as defined under Executive Order 12866, and (2) concerns an environmental, health, or safety risk that the agency has reason to believe may have a disproportionate effect on children. If the regulatory action meets both criteria, the agency must evaluate the environmental health or safety effects of the planned rule on children, and explain why the planned regulation is preferable to other potentially effective and reasonably feasible alternatives considered by the agency.

This notice is part of a rulemaking that is not expected to have a disproportionate health or safety impact on children. Consequently, no further analysis is required under Executive Order 13045.

F. Paperwork Reduction Act

Under the Paperwork Reduction Act of 1995 (PRA), a person is not required to respond to a collection of information by a Federal agency unless the collection displays a valid OMB control number. There is no information collection requirement associated with this proposal. The proposal would require new vehicles to be capable of V2V communications, which would require a new aspect of performance where the vehicle broadcasts Basic Safety Messages (BSMs) during operation, which other vehicles could then receive and interpret as appropriate. BSMs include information about a vehicle's current location, heading, and speed, among other things – information that safety applications on other vehicles could interpret to determine whether a warning to the driver is needed for the driver to avoid a potential crash. The agency does not foresee any reporting requirements or PRA related impacts directly attributable to the proposed performance requirements in this proposal.

G. National Technology Transfer and Advancement Act

Section 12(d) of the National Technology Transfer and Advancement Act (NTTAA) requires NHTSA to evaluate and use existing voluntary consensus standards in its regulatory activities unless doing so would be inconsistent with applicable law (e.g., the statutory provisions

regarding NHTSA's vehicle safety authority) or otherwise impractical. Voluntary consensus standards are technical standards developed or adopted by voluntary consensus standards bodies. Technical standards are defined by the NTTAA as "performance-based or design-specific technical specification and related management systems practices." They pertain to "products and processes, such as size, strength, or technical performance of a product, process or material."

Examples of organizations generally regarded as voluntary consensus standards bodies include ASTM International, SAE International (SAE), and the American National Standards Institute (ANSI). If NHTSA does not use available and potentially applicable voluntary consensus standards, we are required by the Act to provide Congress, through OMB, an explanation of the reasons for not using such standards.

This proposal would require new light vehicles to be capable of V2V communications. Section III.D.10 above discusses how voluntary consensus standards by SAE, IEEE, and ISO interact with the agency's proposed requirements for V2V communication. In summary, the voluntary consensus standards provide information that support both performance requirements and design specifications, and are the bridge for connecting the requirements to the specifications. In relation to this proposal, NHTSA's job is to identify and define performance requirements and verification tests that will indicate that V2V devices have been designed and implemented such that they will operate to provide V2V communications and security that will support crash avoidance applications. The voluntary consensus standards are building blocks for those requirements, but as they are not at the vehicle-level, they cannot be incorporated wholesale into the FMVSS. We seek comment on NHTSA's approach to inclusion of relevant voluntary consensus standards in the development of our proposed requirements.

H. Unfunded Mandates Reform Act

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) requires federal agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of more than $100 million annually (adjusted for inflation with base year of 1995). Before promulgating a rule for which a written statement is needed, section 205 of the UMRA generally requires the agency to identify and consider a reasonable number of regulatory alternatives and adopt the least costly, most cost-effective, or least burdensome alternative that achieves the objectives of the rule. The provisions of section 205 do not apply when they are inconsistent with applicable law. Moreover, section 205 allows the agency to adopt an alternative other than the least costly, most cost-effective, or least burdensome alternative if the agency publishes with the final rule an explanation of why that alternative was not adopted.

As noted above, NHTSA has prepared a detailed economic assessment of this proposal in the PRIA. In that assessment, the agency analyzes the benefits and costs of requiring new light vehicles to be capable of V2V communications. NHTSA's preliminary analysis indicates that this proposal could result in private expenditures of between $2 and $5 billion annually.

The PRIA also analyzes the benefits and costs of a range of regulatory alternatives. While the "No Action" alternative would result in no costs, it would also result in no benefits. For the alternative that would include mandates for safety applications, NHTSA's preliminary analysis indicates that the costs would not be significantly different from the proposal, but that benefits would accrue faster, such that the alternative would be cost-effective and achieve positive net benefits two model years before the proposal would. The agency is proposing *not* to require applications at this time, however, due to the need for significant additional research to establish performance requirements and test procedures for them, and without which unintended consequences such as high false positive rates could occur.

Since the agency has estimated that this proposal could result in expenditures of over $1 billion annually, NHTSA has performed a probabilistic uncertainty analysis to examine the degree of uncertainty in its cost and benefit estimates and included that analysis in Chapter 12 of the PRIA.

I. National Environmental Policy Act

NHTSA has analyzed this rulemaking action for the purposes of the National Environmental Policy Act. The agency has determined that implementation of this proposed action will not have any significant impact on the quality of the human environment.

J. Plain Language

Executive Order 12866 requires each agency to write all rules in plain language. Application of the principles of plain language includes consideration of the following questions:

- Have we organized the material to suit the public's needs?
- Are the requirements in the rule clearly stated?
- Does the rule contain technical language or jargon that isn't clear?
- Would a different format (grouping and order of sections, use of headings, paragraphing) make the rule easier to understand?
- Would more (but shorter) sections be better?
- Could we improve clarity by adding tables, lists, or diagrams?
- What else could we do to make the rule easier to understand?

If you have any responses to these questions, please include them in your comments on this proposal.

K. Regulatory Identifier Number (RIN)

The Department of Transportation assigns a regulation identifier number (RIN) to each regulatory action listed in the Unified Agenda of Federal Regulations. The Regulatory Information Service Center publishes the Unified Agenda in April and October of each year.

NOTE: This document has been signed and we are submitting it for publication in the Federal Register. While we have taken steps to ensure the accuracy of this Internet version of the document, it is not the official version. Please refer to the official version in a forthcoming Federal Register publication or on GPO's Web Site. You can access the Federal Register at: www.federalregister.gov.
You may use the RIN contained in the heading at the beginning of this document to find this action in the Unified Agenda.

L. Privacy Act

Anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (65 FR 19477-78).

XI. Proposed Regulatory Text

List of Subjects in 49 CFR Part 571

Motor vehicles, Motor vehicle safety

In consideration of the foregoing, NHTSA proposes to amend 49 CFR part 571 as follows:

PART 571 – FEDERAL MOTOR VEHICLE SAFETY STANDARDS

1. The authority citation for part 571 of title 49 continues to read as follows:

Authority: 49 U.S.C. 322, 30111, 30115, 30117, and 30166; delegation of authority at 49 CFR 1.95.

2. Add Section 571.150 to subpart B to read as follows:

Sec. 571.150 Standard No. 150; V2V Communications.

S1 Scope. This standard specifies performance requirements for vehicle-to-vehicle communications capability.

S2 Purpose. The purpose of this standard is to ensure that new motor vehicles are able to transmit and receive standardized, authenticated Basic Safety Messages (BSMs), in order to create an information environment upon which a variety of safety applications can rely, which in turn can reduce deaths and injuries on the roads.

S3 Application. This standard applies to new passenger cars, multipurpose passenger vehicles, trucks, and buses with a gross vehicle weight rating of 10,000 pounds (4,536 kilograms) or less.

S4 Definitions.

Basic Safety Message (BSM) contains safety data according to specific requirements and is used in a variety of applications to exchange safety data regarding vehicle status. BSM transmission of 10 times per second is typical when congestion control is not active. BSM content, initialization time, transmission requirements, and other characteristics must comply with the requirements of S5, below.

Channel busy ratio is a measure of the amount of time a channel is designated as busy over the total observed time channel is available.

Coordinated Universal Time (UTC) is the international standard of time that is kept by atomic clocks around the world

Denial of Service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend such as disrupting DSRC communications

DSRC device means a device uses Dedicated Short Range Communications to transmit and receive a variety of message traffic to and from other DSRC devices that include On-Board Units (integrated into a vehicle), Aftermarket Safety Devices, and Road-Side Units.

Event Flag is part of the Basic Safety Message. An Event Flag conveys the sender's status with respect to safety-related events such as Antilock Brake System activation, Stability Control Activation, hard braking, and airbag deployment.

GNSS (Global Navigation Satellite System) means a satellite system that is used to pinpoint the geographic location of a user's receiver anywhere in the world.

Packet Error Rate refers to the unit of data for radio transmission subject to Forward Error Correction (FEC). The number of error packets after FEC divided by the total number of received packets is the Packet Error Rate.

Reasonably Linkable refers to data elements in the BSM or other aspects of V2V transmissions capable of being used to identify a specific individual on a persistent basis without unreasonable cost or effort, in real time or retrospectively, given available data sources. This is intended to have the same meaning as "linkable as a practical matter" as used in this standard.

Roadside Equipment (RSE) means any roadside equipment that prepares and transmits messages to V2V devices and receives messages from V2V devices for the purpose of supporting V2I applications or, potentially, security. This is intended to include the DSRC radio, traffic signal controller where appropriate, interface to the backhaul communications network necessary to support the applications, and support such functions as data security, encryption, buffering, and message processing.

Timestamp means the current time of an event that is recorded by a computer.

Vehicle reference point means the theoretical point projected on the surface of the roadway that is in the center of a rectangle oriented about the vehicle's axis of symmetry front-to-back, encompassing the farthest forward and rearward points and side-to-side points on the vehicle, including original equipment such as outside side view mirrors.

S5 Requirements. Each vehicle to which this standard applies must transmit and receive messages consistent with the requirements below. To obtain interoperable V2V communications for crash avoidance safety, DSRC devices must be capable of: First, transmitting and receiving an established message (i.e. the BSM that has specified content of information, but also the measuring unit for each information element and the level of precision needed); Second, conforming to DSRC transmission protocols that will support crash avoidance safety (i.e., how far, how often, on what frequency, etc.); Third, implementing a method for a device to add validation context to message transmissions such that a receiver of that message can authenticate certain information about the sender of the message; Fourth, incorporating a uniform method for dealing with possible occurrences of high volumes of DRSC messages (i.e., potentially reducing the frequency or range of messages in high congestion situations) and; Fifth, robustness to incorrect or malicious incoming messages.

S5.1 Content. Each BSM must contain the following elements, except as provided in S5.1.7.:

S5.1.1 Message packaging. As part of each BSM, a DSRC device must transmit a Message ID, a Message Count, and a Temporary ID, as follows:

S5.1.1.1 The Message ID must be the digit "2."

S5.1.1.2 The Message Count must contain an integer between 0 and 127 that is 1 integer greater than the integer used in the last BSM transmitted by the same DSRC device. If the last BSM Message Count was 127, then the Message Count for the following BSM is 0.

S5.1.1.3 The Temporary ID must be a randomly generated 4-digit number. The DSRC device must randomly generate a new 4-digit number every five minutes. However, if other temporary identifiers, such as pseudonym certificates, are used, the Temporary ID should be changed every time another identifier (such as a pseudonym certificate) is changed.

S5.1.2 Time. As part of each BSM, a DSRC device must transmit a data element indicating the time, expressed in UTC, and within +/- 1 milliseconds of the actual UTC time.

S5.1.3 Location. As part of each BSM, a DSRC device must transmit:

S5.1.3.1 Longitudinal and lateral location within 1.5 meters of the actual position at a Horizontal Dilution of Precision (HDOP) smaller than 5 within the 1 sigma absolute error; and

S5.1.3.2 Elevation location within 3 meters of the actual position at a Horizontal Dilution of Precision (HDOP) smaller than 5 within the 1 sigma absolute error.

S5.1.4 Movement. As part of each BSM, a DSRC device must transmit speed, heading, acceleration, and yaw rate, as follows:

S5.1.4.1 Speed must be reported in increments of 0.02 m/s, within 1 km/h (0.28 m/s) of the vehicle's actual speed.

S5.1.4.2 Heading must be reported accurately to within 2 degrees when the vehicle speed is greater than 12.5 m/s (~28 mph); and to within 3 degrees when the vehicle speed is less than or equal to 12.5 m/s. Additionally, when the vehicle speed is below 1.11 m/s (~2.5 mph), the DSRC device must latch the current heading and transmit the last heading information prior to the speed dropping below 1.11 m/s. The device is to unlatch the latched heading when the vehicle speed exceeds 1.39 m/s (~3.1 mph) and transmit a heading within 3 degrees of its actual heading until the vehicle reaches a speed of 12.5 m/s where the heading must be transmitted at 2 degrees accuracy of its actual heading.

S5.1.4.3 Acceleration. Horizontal (longitudinal and lateral) acceleration must be reported accurately to 0.3 m/s^2, and vertical acceleration must be reported accurately to 1 m/s^2.

S5.1.4.4 Yaw rate. Yaw rate must be reported accurately to 0.5 degrees/second.

S5.1.5 Other event based information.

S5.1.5.1 Path History. The Path History data frame will be transmitted as a required BSM element at the operational frequency of the BSM transmission

S5.1.5.1.1 Path History data frame requires a history of a vehicles past GNSS locations as dictated by GNSS data elements including UTC time, latitude, longitude, heading, elevation sampled at a periodic time interval of 100 ms and interpolated in-between by circular arcs, to represent the vehicle's recent movement over a limited period of time or distance.

S5.1.5.1.2 Path History points should be incorporated into the Path History data frame such that the perpendicular distance between any point on the vehicle path and the line connecting two consecutive PH points shall be less than 1 m

S5.1.5.1.3 Minimum number of Path History points vehicles should report the minimum number of points so that the represented Path History distance (i.e., the distance between the first and last Path History point) is at least 300 m and no more than 310 m, unless initially there is less than 300 m of Path History. If the number of Path History points needed to meet both the error and distance requirements stated above exceeds the maximum allowable number of points (23), the Path History data frame shall be populated with only the 23 most recent points from the computed set of points.

S5.1.5.1.3 Path History data frame shall be populated with time-ordered Path History points, with the first Path History point being the closest in time to the current UTC time, and older points following in the order in which they were determined.

S5.1.5.2 Path Prediction. Trajectories in the Path Prediction data frame are represented, at a first order of curvature approximation, as a circle with a radius, R, and an origin located at (0,R), where the x-axis is aligned with the transmitting vehicle's perspective and normal to the vehicle's vertical axis. The radius, R, will be positive for curvatures to the right when observed from the transmitting vehicle's perspective, and radii exceeding a maximum value of 32,767 are to be interpreted as a "straight path" prediction by receiving vehicles.

S5.1.5.2.1 When a device is in steady state conditions over a range from 100 m to 2,500 m in magnitude, the subsystem will populate the Path Prediction data frame with a calculated radius that has less than 2% error from the actual radius. For the purposes of this performance requirement, steady state conditions are defined as those which occur when the vehicle is driving on a curve with a constant radius and where the average of the absolute value of the change of yaw rate over time is smaller than 0.5 deg/s^2.

S5.1.5.2.2 After a transition from the original constant radius (R1) to the target constant radius (R2), the subsystem shall repopulate the Path Prediction data frame within four seconds under the maximum allowable error bound defined above.

S5.1.5.2.3 Path Prediction trajectories will be transmitted as a required BSM element at the operational frequency of the BSM transmission.

S5.1.5.3 Exterior lights. The subsystem shall set the individual light indications in the data element to be consistent with the vehicle status data that is available. If meaningful values are unavailable, or no light indications will be set to indicate the light is on, the data element should not be transmitted.

S5.1.5.3.1 The Exterior Lights data element, if available, provides the status of all exterior lights on the vehicle, including parking lights, headlights (including low and high beam, and automatic light control), fog lights, daytime running lights, turn signal (right and left), and hazard signals.

S5.1.5.4 Event flags. If a stated criterion is met as indicated for each Event Flag listed, the sender shall set the Event Flag to 1. If, and only if, one or more of the defined Event Flags are set to 1, the subsystem shall transmit a BSM with the corresponding Event Flags within 250 ms of the initial detection of the event at the sender. The Event Flags data element shall be included in the BSM for as long as an event is active.

- ABS Activation: The system is activated for a period of time exceeding 100 ms in length and is currently active.
- Stability Control Activation: The system is activated for a period of time exceeding 100 ms in length and is currently active.
- Hard Braking: The vehicle has decelerated or is decelerating at a rate of greater than 0.4 g.
- Air Bag Deployment: At least one air bag has been deployed.
- Hazard Lights: The hazard lights are currently active.

- Stop Line Violation: The vehicle anticipates that it will pass the line without coming to a full stop before reaching it.
- Traction Control System Activation: The system is activated for a period of time exceeding 100 ms in length and is currently active.
- Flat Tire: The vehicle has determined that at least one tire has run flat.
- Disabled Vehicle: The vehicle considers itself to be disabled.
- Lights Changed: The status of the external lights on the vehicle has changed recently.
- Wipers Changed: The status of the front or rear wipers on the vehicle has changed recently.
- Emergency Response: The vehicle is a properly authorized public safety vehicle, is engaged in a service call, and is currently moving. Lights and/or sirens may not be evident.
- Hazardous Materials: The vehicle is known to be carrying hazardous materials and is labeled as such.

S5.1.6 Vehicle-based motion indicators. As part of each BSM, a DSRC device must transmit transmission state and steering wheel angle.

S5.1.6.1 Transmission state must be reported as either "neutral," "reverse," or "forward" for any forward gear.

S5.1.6.2 Steering wheel angle must be reported accurately to 5 degrees.

S5.1.7 Vehicle size. Vehicle size must be reported accurately to 0.2 meters of the vehicle's length and width.

S5.1.9 Prohibited elements of the BSM. No BSM may contain data linked or reasonably linkable to a specific private vehicle or its driver or owner, including but not limited to VIN, VIN string, vehicle license plate, vehicle registration information, or owner code.

S5.2 Initialization time. A DSRC device must begin transmitting the BSM within 2 seconds after the V2V device power is initiated.

S5.3 Transmitting the BSM. A DSRC device must transmit the BSM with the following power/range, on the following channel, and at the following data rate(s) and times:

S5.3.1 Transmission range. A DSRC device must transmit the BSM in all directions on the same plane as the device (i.e., 360 degrees) and at least 10 degrees above the vehicle and 6 degrees below the vehicle (i.e., along the vertical axis) such that it can be received at any point within at least 300 meters from the transmission antenna, with a Packet Error Rate (PER) of less than 10 percent.

S5.3.2 Transmission channel. A DSRC device must transmit the BSM on Channel 172, as allocated for "public safety applications involving safety of life and property" in 47 C.F.R part

90, subpart M. All non safety-critical communications will occur on the remaining channels allocated for DSRC in subpart M.

S5.3.3 Transmission data rate. A DSRC device must transmit the BSM at a bit rate of 6 Mbps.

S5.3.4 Transmission staggering timing. A DSRC device must transmit the BSM every 100 ms +/1 a random value between 0 and 5 ms.

S5.4 Signing the BSM. [Reserved for message signature requirement if needed; please refer to the preamble]

S5.4.1 Rotating certificates. [Reserved for rotating certificate requirement if needed; please refer to the preamble]

S5.5 Congestion Mitigation

A DSRC device must transmit the BSM as follows under the following circumstances:

S5.5.1 Calculate Tracking Error

This section specifies the set of steps that calculate the tracking error in the congestion control algorithm for the system. Note that the tracking error is communications-induced and independent of the positioning system tracking error. The system performs the following operations every 100 ms.

- The system estimates the position of the HV at the current time, defined as HV local estimator, per defined below

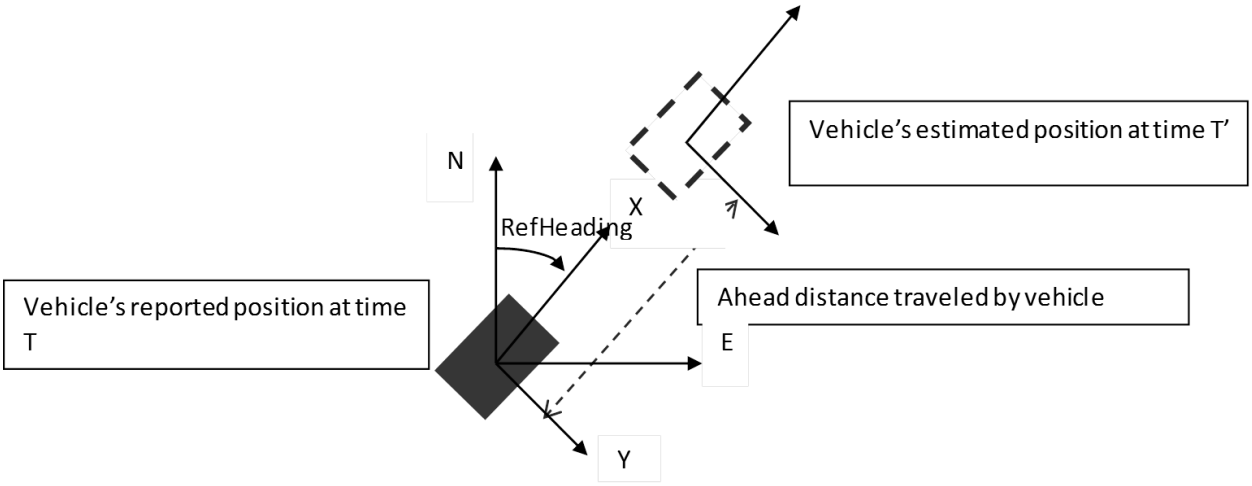

Figure XI-1 GNSS Position Extrapolation

1. First find Delta_time, the time since vehicle's last known position.

(1) Delta_time_ms = T' – T

2. Do not perform position extrapolation in the following cases:

   - If Delta_time_ms < 0, then there is a time-related error.
   - If Delta_time_ms > 150 ms, then the vehicle has not received a position update for a very long time and its position is outdated.

3. If 50 ms <= Delta_time_ms <= 150 ms, then perform position extrapolation:

   - Calculate the estimated distance traveled by the vehicle in Delta_time_ms.
     - Ahead_distance_m = Speed_mps * Delta_time_ms / 1000
     - Across_distance_m = 0

4. Use ConvertXYtoLatLon function to find the vehicle's new position at time T'.

   ConvertXYtoLatLon(…)

   INPUT

   RefLat = e.g., REF_LATITUDE (rad)

   RefLon = e.g., REF_LONGITUDE (rad)

   RefHeading = e.g., REF_HEADING (rad)

   Y = ACROSS_DISTANCE (m w.r.t. REF LATLON)

   X = AHEAD_DISTANCE (m w.r.t. REF LATLON)

   a = 6378137; # semi-major axis of earth

   f = 0.003353; # flattening

   f1 = (f*(2-f))^0.5; # eccentricity

   f2 = a*(1-f1^2)/(1-f1^2*(sin(RefLat))^2)^(3/2); # radius of earth in meridian

   f3 = a/(1-f1^2*(sin(RefLat))^2)^(1/2); # radius of earth in prime vertical

   E = (cos(RefHeading)*Y + sin(RefHeading)*X;

   N = (cos(RefHeading)*X - sin(RefHeading)*Y;

OUTPUT

NEW_LATITUDE (rad) = (1/f2)*N + RefLat;

NEW_LONGITUDE (rad) = (1/(f3*cos(RefLat)))*E + RefLon;

5. For all future calculations, use the calculated New_Latitude and New_Longitude as vehicle's position, and current time.

- The system makes an assumption of the latest HV state information received by the RVs based on a Bernoulli trial corresponding to the quality of channel indicator as defined below:

Assumption of latest HV State Information at RVs

After each transmission, use a Bernoulli trial with the channel quality indicator $\Pi(k)$ to infer whether this previous transmission is successfully received by RVs.

- Channel Quality Indicator (Π): The system calculates Π as an average of the PERs observed by the HV from all of the RVs within 100 m of the HV over an interval 5000 ms, and updated at the end of each 1000 ms sub-interval.

Let AVGPER be calculated as:

$$AVGPER(k) = \frac{1}{N(k)} \sum_{i=1}^{N(k)} PER_i(k) \qquad (4)$$

where PER_i is for RV 'i' and N(k) is the Vehicle Density within 100 m.

Next, Π is calculated by smoothening AVGPER to filter out temporal noise or disturbance in the measurement as follows:

$$\Pi(k) = \lambda_1 \times AVGPER(k) + (1 - \lambda_1) \times \Pi(k-1)$$
$$\text{If } (\Pi(k) > vPERMax)$$
$$\Pi(k) = vPERMax \qquad (5)$$

where λ_1 is the weight factor 0.9, $\Pi(k)$ is the channel quality indicator for the current interval window. Note that, if $\Pi(k)$ exceeds 0.3, then it is set to 0.3.

1. If the outcome of this Bernoulli trial is positive, assume that the previous transmission by HV is successfully received by RVs. Update the latest information the RVs have about the HV as the state information contained in previous transmission.

2. If, however, the outcome of this Bernoulli trial is negative, treat the previous transmission by HV as a failure and do not update the latest HV state information as that received by RVs.

3. Count the number of Bernoulli trials with successive negative outcomes. If this count is greater than 3, set the previous transmission as successful and update the latest information the RVs have about the HV as the state information contained in the previous transmission.

The state information is defined:

Let $\begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Latest}}$ be the HV's assumed latest state information received by RVs and $\begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Pre-Tx}}$ be the HV's state information contained in the message of its previous transmission (where t is the time in msec when the longitudinal position x (in degrees), lateral position y (in degrees), speed v (in m/s), and heading $\theta(t)$ (in degrees) are measured. The HV's assumed latest state information received by RVs is updated after each transmission as follows:

$$\begin{aligned} &\text{If } rand() < \Pi(k) \\ &TxFailed = TxFailed + 1 \\ &Else \\ &TxFailed = 0 \end{aligned}$$

$$\begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Latest}} = \begin{cases} \begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Pre-Tx}} & \text{TxFailed} > 0 \text{ and TxFailed} <= \text{vMaxSuccessiveFail} \\ \begin{bmatrix} t \\ x \\ y \\ v \\ \theta \end{bmatrix}_{\text{Latest}} & \text{otherwise set TxFailed} = 0 \end{cases}$$

where $rand()$ is a uniform random number generator and $\Pi(k)$ is the estimated channel quality indicator.

- Using the latest HV state information assumption at RVs, the system estimates the position of the HV at the current time, defined as HV remote estimator, using the estimator described above. This indicates where the HV believes the RVs "thinks" that the HV is located at the current time.

- The system then calculates the tracking error e(k), between where the HV believes its current position is and where the HV believes RVs think the HV is located at the current time. It is also known as the suspected, expected or estimated tracking error between the HV local estimator and the HV remote estimator.

  Where:

the tracking error is defined as the distance between HV local estimator position $(\hat{x}(k)$, $(\hat{y}(k)$) and output of the HV remote estimator position, ($\tilde{x}(k)$, $\tilde{y}(k)$) using the great circle formula, i.e.

$$e(k) = R(\hat{x}(k)) \times (\cos^{-1}(\sin(\hat{x}(k)) \times \sin(\tilde{x}(k)) + \cos(\hat{x}(k)) \times \cos(\tilde{x}(k)) \times \cos(\hat{y}(k) - \tilde{y}(k))))$$

where

$$R(\hat{x}(k)) = a \times (1 - f_1^2) / (1 - f_1^2 \times \sin^2(\hat{x}(k)))^{1.5}$$

is the Meridian Radius of the Earth in meters $\hat{x}(k)$, at latitude, a = 6378137 is the mean radius of earth in meters, $f_1 = (f \times (2 - f))^{0.5}$ is the Eccentricity, and f = 0.003353 is earth's flattening.

Here $(\hat{x}(k), \hat{y}(k))$ are the latitude and longitude from the HV Local Estimator, converted to radians, and $(\tilde{x}(k), \tilde{y}(k))$ are the latitude and longitude from the HV Remote Estimator, converted to radians.

S5.5.2 Transmission power must vary depending on the following:

S5.5.2.1 If there is an Event Flag or a transmission decision is based on p(k), the BSM must be transmitted at maximum power despite the presence of any other conditions;

S5.5.2.2 If the channel busy ratio is below 50% (Umin)and the transmission is based on Max_Trans_Time, then the BSM must be transmitted at maximum power (20 dBm, Pmax);

S5.5.2.3 If the channel busy ratio is above 80% (Umax) and the transmission is based on Max_Trans_Time, then the BSM must be transmitted at minimum power (10 dBm, Pmin);

S5.5.2.4 If the channel busy ratio is between (c) and (b), then the BSM must be transmitted at a power based on a linear function that proportionally reduces the transmission power based on the channel busy ratio value during the previous transmission (U(k-1)) and the previous transmission power (P(k-1). Where the transmitted power (P(k)) is defined by:

$$P_K = P_{k-1} + 0.5\left(\left[P_{\max} - \left(\frac{P_{max} - P_{\min}}{U_{max} - U_{min}}\right) \times (U_{k-1} - U_{min}) \right] - P_{k-1} \right)$$

S5.6 Detecting misbehavior. A DSRC device must detect misbehavior in the following ways:

S5.6.1 Internal self-diagnostics. A DSRC device must be able to perform the following self-diagnostic checks:

S5.6.1.1 If a DSRC device detects a malfunctioning sensor which may cause misbehavior, the device must:

(a) Either transmit the BSM with the affected elements set to "Unavailable" if relevant standards allow the element to be set to "Unavailable"; or

(b) Cease BSM transmission if relevant standards do not allow the element to be set to "Unavailable."

If either (a) or (b) is detected, [Reserved for requirement to report malfunctions if needed; please refer to the preamble]

S5.6.1.2 [Reserved for requirement to report physical tampering; please refer to the preamble]

S5.6.2 Checking and reporting on the plausibility of incoming BSMs. A DSRC device must perform a preliminary plausibility check on all incoming BSMs and respond accordingly, as follows:

S5.6.2.1 The preliminary plausibility check must identify as an implausible message any BSM for which the components of the vehicle dynamic state (position, speed, acceleration, and yaw rate) are outside the following values:

(a) Speed greater than 70 m/s (252 km/h or 156 mph);
(b) Longitudinal acceleration of 0-100 km/h in fewer than 2.3 seconds (greater than 12 m/s^2);
(c) Longitudinal deceleration of 100-0 km/h in fewer than 95 feet (greater than 12 m/s^2);
(d) Lateral acceleration of greater than 11 m/s^2 (1.12 G);
(e) Yaw rate of greater than 1.5 radian/s

Additionally, a BSM must be identified as implausible if values within the BSM are not internally consistent given the formula $V^2 = a_c / (Y')^2$.

S5.6.2.2 A DSRC device must be able to perform the plausibility checks described in S5.6.2.1 on at least 5,500 BSMs per second.

S5.6.2.3 [Reserved for requirement to report any failed plausibility check; please refer to the preamble]

S5.6.2.4 A DSRC device must support the detection of other devices which are suspected of misbehaving, and at a minimum detect the following types of misbehavior:

(a) Proximity Plausibility: Instances are detected of two or more vehicles, either partially or wholly, occupying the same physical space based on the reported GPS positions.
(b) Motion Validation: Attempts to validate the reported position of a transmitting vehicle based on the previously-reported velocity and heading values of the vehicle.
(c) Content and Message Verification: Attempts to categorize BSMs as suspicious by checking the data validity of the BSM.
(d) Denial of Service Detection: Attempts to disrupt, limit, or alter the functionality of V2V device to meet the requirements through exhaustions of storage, computation, or other limited resources of the V2V device.

S5.6.3 [Reserved for requirements for sending misbehavior reports; please refer to the preamble]

S5.7 Indicating a malfunction. The DSRC device must be able to indicate to its user the occurrence of one or more malfunctions that affect the performance of the device, its supporting equipment, or the inputs used to form, transmit, or receive a BSM, as follows:

S5.7.1 Malfunctions could include, but are not limited to, the following:

(a) device components not operating properly;
(b) input sensor data falling outside tolerance levels;
(c) on-board memory failures;
(d) GPS receiver failures;
(e) an inability to transmit or receive BSMs; or
(f) any other failure that could prevent normal operation.

S5.7.2 The malfunction indication must be clearly presented to device users in the form of a telltale lamp or message.

S5.7.3 Owners' information for the device (or vehicle, if the DSRC device is installed as original equipment) must clearly describe the malfunction indication, potential causes, and when the device must be taken in for service (as needed).

S5.7.4 The malfunction indication must remain present and/or illuminated until the malfunction no longer exists and the DSRC device is returned to proper operation.

S5.8 [Reserved for requirement to communicate with the SCMS if needed, please refer to the preamble]

S5.9 Communicating about and obtaining software and security updates. A DSRC device must be able to indicate clearly to users that either device software or security updates are available and that the user must consent to the update before it can occur. If the DSRC device is included in a vehicle as original equipment, the indicator must be present in the vehicle. If the DSRC device is not included in the vehicle as original equipment, the indicator must be present in the device itself.

S5.10 [Reserved for hardware protection requirement; please refer to the preamble]

S5.11 Consumer Privacy Statement

S5.11.1 Owners information for the device must include the statement set forth in Appendix A below.

S5.11.2 Manufacturers also must make the statement set forth in Appendix A easily accessible to the public, as by publishing it on an easily located web site indexed by make, model, and year.

S6 Test Conditions.

S6.1 Ambient conditions.

S6.1.1 The ambient temperature is between 0°C (32°F) and 40°C (104°F).

S6.1.2 The maximum wind speed is no greater than 10 m/s (22 mph) for passenger cars and 5 m/s (11 mph) for multipurpose passenger vehicles, trucks, and buses.

S6.2 Road test surface.

S6.2.1 The tests are conducted on a dry, uniform, solid-paved surface. Surfaces with irregularities and undulations, such as dips and large cracks, are unsuitable.

S6.2.3 The test surface has a consistent slope between level and 1 percent.

S6.3 Vehicle conditions.

S6.3.2 Test weight. The vehicle may be tested at any weight consisting of the test driver and instrumentation only that fall between its lightly loaded vehicle weight (LLVW) and its gross vehicle weight rating (GVWR) without exceeding any of its gross axle weight ratings.

S6.3.3 Tires. The vehicle is tested with the tires installed on the vehicle at the time of initial vehicle sale. The tires are inflated to the vehicle manufacturer's recommended cold tire inflation pressure(s) specified on the vehicle's placard or the tire inflation pressure label.

S7. Test Procedures.

S7.1 Pre-test / Inspection.

S7.1.1 Inflate the vehicles' tires to the cold tire inflation pressure(s) provided on the vehicle's placard or the tire inflation pressure label

S7.1.2 Vehicle dimensions.

S7.1.2.1 Measure vehicle length including any equipment installed on the vehicle when first sold

S7.1.2.2 Measure vehicle width including any equipment installed on the vehicle when first sold

S7.1.2.3 Measure vehicle height including any equipment installed on vehicle when first sold

S7.1.2.4 Measure the V2V System GNSS Receiver Antenna

S7.1.2.5 Measure the independent instrumented vehicle sensor coordinates

S7.2 Static Performance Test Procedure:

S7.2.1 Place the test vehicle on car wheel rollers and position the vehicle on the test track

S7.2.2 Two dimensional Range: Position a DSRC packet capture device directly in front of the test vehicle with the following characteristics:

S7.2.2.1 The device is 1.5 m above the test surface;

S7.2.2.2 The device is at a nominal distance of 300 m in front of the test vehicle

S7.2.3 Upward elevation range: Position a DSRC packet capture device at any point along the following line.

S7.2.3.1 The line originates at a point that is directly 1.5 m above the vehicle reference point

S7.2.3.2 The line rises at a +10 degree angle from the test surface proceeding in the direction directly in front of the test vehicle

S7.2.3.3 The line terminates at a point that is directly above the point used in S7.2.2

S7.2.4 Downward elevation range: Position a DSRC packet capture device at any point along the following line

S7.2.4.1 The line originates at a point that is directly 1.5 m above the vehicle reference point

S7.2.4.2 The line falls at a -6 degree angle from the test surface proceeding in the direction directly in front of the test vehicle

S7.2.4.3 The line terminates at any point where it intersects the test surface

S7.2.5 Configure the DSRC packet capture devices to log BSMs over-the-air (OTA); devices must have a receive sensitivity of -92 dBm

S7.2.6 Activate the DSRC packet capture devices to log BSMs OTA

S7.2.7 Activate the test vehicle starting system to initiate BSM transmission

S7.2.7.1 Run the vehicle for 110 mins

S7.2.7.2 Rotate the vehicle 90 degrees in the clockwise direction every 15 minutes until the time in S7.2.7.1 expires

S7.2.8 Deactivate the test vehicle and DSRC packet capture devices

S7.2.9 Retrieve and process the log files to determine compliance with S.5

S7.2.10 Positional Accuracy Test

S7.2.10.1 Using the transmission blocking water filled plastic blanket that will hold one gallon of water with a water width of 1 inch, cover the test vehicle GPS antenna to prevent it from receiving a valid GNSS signal

S7.2.10.2 Connect GPS signal generator to the test vehicle OBE

S7.2.10.3 Activate the test vehicle starting system to initiate BSM transmission

S7.2.10.4 Activate the DSRC packet capture devices to log BSMs OTA

S7.2.10.5 Using the GPS signal generator, inject a known fake GPS signal into the OBE

S7.2.10.6 After 5 minutes, deactivate the test vehicle starting system and DSRC capture packet device

S7.2.10.7 Retrieve and process the log files to determine compliance with the positional accuracy requirements

S7.3 Simulated Performance Tests

S7.3.1 Place the test vehicle on the test track

S7.3.2 Position a DSRC packet capture device directly in front of the test vehicle with the following characteristics:

S7.3.2.1 The device is 1.5 m above the test surface;

S7.3.2.2 The device is at a nominal distance of 300 m in front of the test vehicle

S7.3.3 Configure the DSRC packet capture device to log BSMs over-the-air (OTA); devices must have a receive sensitivity of -92 dBm

S7.3.4 Congestion Mitigation

S7.3.4.1 Position a reference OBE device (i.e. rack of OBE modules) on the test track within a 300 m range of the test vehicle

S7.3.4.2 Activate the DSRC packet capture device to log BSMs OTA

S7.3.4.3 Activate the test vehicle starting system to initiate BSM transmission

S7.3.4.3.1 Run the vehicle for 15 minutes

S7.3.4.3.2 After 5 minutes, activate the reference OBE device in S7.3.4.1 to simulate a congested DSRC environment

S7.3.4.3.3 After another 5 minute period, deactivate the reference OBE device in S7.3.4.1

S7.3.4.3.4 After another 5 minute period, deactivate the test vehicle starting system

S7.3.4.4 Retrieve and process the log files to determine compliance with the correct congestion mitigation strategy in S5.5

S7.3.5 Misbehavior Detection

S7.3.5.1 Position a reference OBE device on the test track within a 300 m range of the test vehicle

S7.3.5.2 Activate the DSRC packet capture device to log BSMs OTA

S7.3.5.3 Activate the test vehicle starting system to initiate BSM transmission

S7.3.5.4 Using the reference OBE device, transmit simulated misbehaving BSMs

S7.3.5.4.1 After 10 mins, deactivate the reference OBE device

S7.3.5.7 Retrieve and process the log files to determine compliance with the misbehavior detection requirement in S5.6

S7.4 Dynamic Performance Test Procedure

S7.4.1 Configure the test vehicle to send BSMs representing the best estimate of the BSM data parameters

S7.4.2 Configure the test vehicle to send ground truth data (position, speed, heading, acceleration, yaw rate, and time) from independent sensors mounted on the test vehicle via non-DSRC wireless link

S7.4.3 Configure the DSRC packet capture device to log BSMs over-the-air (OTA); devices must have a receive sensitivity of -92 dBm

S7.4.4 Configure an RSE on the test track to receive the test vehicles' ground truth data

S7.4.5 Dynamic test maneuver

S7.4.5.1 Activate the test vehicle starting system to initiate BSM transmission

S7.4.5.2 Activate the DSRC packet capture device to log BSMs OTA

S7.4.5.3 Put the test vehicle transmission in "Drive" and accelerate the vehicle to 30 mph +/- 1 mph

S7.4.5.4 Apply the service brake to decelerate the vehicle 0.3 g, bring the vehicle to a stop

S7.4.5.6 Shift the transmission to "Park" and cycle the ignition

S7.4.5.7 Shift the transmission to "Drive" and accelerate the vehicle to 15 mph +/- mph

S7.4.5.8 Proceed up an incline with a minimum rise of ? ft.

S7.4.5.9 Drive the test vehicle in a figure eight at 18 mph

S7.4.5.10 Bring the test vehicle to a stop and shift the transmission to "Reverse"

S7.4.5.11 Accelerate the test vehicle in the reverse direction

S7.4.5.12 Decelerate the vehicle to a stop and shift the transmission to "Park"

S7.4.5.13 Cycle the ignition

S7.4.5.14 Deactivate the test vehicle starting system

S7.4.5.15 Retrieve and process the log files to determine compliance with S5

S7.4.6 Misbehavior Detection: Plausibility

S7.4.6.1 Configure a remote test vehicle (RV1) to offset its positional BSM data laterally into the left adjacent lane

S7.4.6.2 Place RV1 on a two lane test track and position it in the right most lane

S7.4.6.3 Activate the test vehicle starting system to initiate BSM transmission

S7.4.6.4 Activate the DSRC packet capture device to log BSMs OTA

S7.4.6.5 Drive the test vehicle [30 mph +/- 1 mph] along the test track in the left lane and proceed past RV1

S7.4.6.6 Repeat S7.4.6.5 three (3)times

S7.4.6.7 Retrieve and process the log files to determine compliance with S5.6

S7.4.6.8 Drive the test vehicle past the RSE at a constant [30 mph +/- 1 mph]

S7.4.6.9 Bring the test vehicle to a stop

S7.4.6.10 [Reserved for requirement to retrieve and process the log files to determine if a Misbehavior Report was sent to the SCMS; please refer to preamble]

S7.4.7 [Reserved for Misbehavior Detection Signature Failure testing requirement; please refer to the preamble.]

S7.5 V2V Malfunction Detection

S7.5.1 Start-up Self test:

S7.5.2 Position the test vehicle on the test platform

S7.5.3 Position a DSRC packet capture device at a nominal distance of 300 m from the test device

S7.5.4 Create a malfunction on the test vehicle

S7.5.5 Activate the DSRC packet capture device to log BSMs over-the-air (OTA)

S7.5.6 Activate the test vehicle starting system to initiate BSM transmission

S7.5.7 Retrieve and process the log files to determine compliance with S5

S7.5.8 Cycle the test vehicle starting system

S7.5.9 Deactivate the vehicle starting system

S7.5.10 Correct the system malfunction

S7.5.11 Reactivate the test vehicle starting system

S7.5.12 Deactivate the test vehicle starting system

S8 Phase-in schedule.

S8.1 Vehicles manufactured on or after September 1, [2 years after issuance of a final rule], and before September 1, [3 years after issuance of a final rule]. For vehicles manufactured on or after September 1, [2 years after issuance of a final rule], and before September 1, [3 years after issuance of a final rule], the number of vehicles complying with this standard must not be less than 50 percent of the manufacturer's production on or after September 1, [2 years after issuance of a final rule], and before September 1, [3 years after issuance of a final rule].

S8.2 Vehicles manufactured on or after September 1, [3 years after issuance of a final rule], and before September 1, [4 years after issuance of a final rule]. For vehicles manufactured on or after September 1, [3 years after issuance of a final rule], and before September 1, [4 years after issuance of a final rule], the number of vehicles complying with this standard must not be less than 75 percent of the manufacturer's production on or after September 1, [3 years after issuance of a final rule], and before September 1, [4 years after issuance of a final rule].

S8.3 Vehicles manufactured on or after September 1, [4 years after issuance of a final rule]. All vehicles manufactured on or after September 1, [4 years after issuance of a final rule] must comply with this standard.

S8.4 Calculation of number of complying vehicles.

(a) For purposes of complying with S8.1, a manufacturer may count a vehicle if it is certified as complying with this standard and is manufactured on or after June 5, [1 year after issuance of a final rule], but before September 1, [3 years after issuance of a final rule].
(b) For purposes of complying with S8.2, a manufacturer may count a vehicle if it
    (1) Is certified as complying with this standard and is manufactured on or after June 5, [1 year after issuance of a final rule], but before September 1, [4 years after issuance of a final rule], and is not counted toward compliance with S8.1; or
    (2) Is certified as complying with this standard and is manufactured on or after September 1, [3 years after issuance of a final rule], but before September 1, [4 years after issuance of a final rule].

S8.5 Vehicles produced by more than one manufacturer.

S8.5.1 For the purpose of calculating average annual production of vehicles for each manufacturer and the number of vehicles manufactured by each manufacturer under S8.1 through S8.3, a vehicle produced by more than one manufacturer must be attributed to a single manufacturer as follows, subject to S8.5.2:

(a) A vehicle that is imported must be attributed to the importer.
(b) A vehicle manufactured in the United States by more than one manufacturer, one of which also markets the vehicle, must be attributed to the manufacturer that markets the vehicle.

S8.5.2 A vehicle produced by more than one manufacturer must be attributed to any one of the vehicle's manufacturers specified by an express written contract, reported to the National Highway Traffic Safety Administration under 49 CFR part 585, between the manufacturer so specified and the manufacturer to which the vehicle would otherwise be attributed under S8.5.1.

S8.6 Small volume manufacturers. Vehicles manufactured during any of the two years of the September 1, [2 years after issuance of a final rule] through August 31, [4 years after issuance of a final rule] phase-in by a manufacturer that produces fewer than 5,000 vehicles for sale in the United States during that year.

S8.7 Final-stage manufacturers and alterers. Vehicles that are manufactured in two or more stages or that are altered (within the meaning of 49 CFR 567.7) after having previously been certified in accordance with part 567 of this chapter are not subject to the phase-in requirements of S8.1 through S8.4. Instead, all vehicles produced by these manufacturers on or after September 1, [5 years after issuance of a final rule] must comply with this standard.

S9 Interoperable technology.

S9.1 The agency is also recognizing that communications mediums other than DSRC may be capable of providing equal or better performance than DSRC. These alternative

technologies would be permissible if and only if it satisfies all of the criteria set forth in this section:

S9.1.1 Interoperable technology testing requirements:

S9.1.1.1 Transmitting and receiving an established message with all other V2V devices, including DSRC devices, including BSM content data as specified in S5.1.2, S5.1.3, S5.1.4, S5.1.5, S5.1.6, and S5.1.7;

S9.1.1.2 Utilizing transmissions protocols that achieve at least the same level of performance as DSRC including S5.2, S5.3.1, S5.3.4, and S5.3.5; and

S9.1.1.3 Ensuring, at the minimum, the same robustness to incorrect or malicious incoming messages as DSRC as specified in the plausibility checks specified in S5.6.2.

S9.1.2 Interoperable technology performance requirements:

S9.1.2.1 A device that enables V2V communication, but does not use DSRC technology must perform at the same level as the requirements found in S5.2, S5.3, S5.4, S5.7 - S5.10 for DSRC devices, except that it is not required to meet:

S9.1.2.2 Specific references to DSRC, where the technology meets all other requirements;

S9.1.2.3 The message packaging or protocol suite requirements found in S5.1.1.

S9.1.2.4 The required channel or data rate in S5.3.2 and S5.3.3; and

S9.1.2.5 The requirements associated with message congestion mitigation and misbehavior detection found in S5.5 and S5.6 except as specified in S5.6.2;

S9.1.3 Interoperability technology testing procedures:

S9.1.3.1 The test conditions for testing non-DSRC V2V devices shall be the same as those for DSRC devices in S6.

S9.1.3.2 The test procedures for testing non-DSRC V2V devices to determine whether they can send BSMs that are interoperable with DSRC devices shall be the same as those for DSRC devices in S7, minus any specific references to DSRC in the vehicle being tested, including but not limited to S7.3.4, S7.3.5, and S7.4.6.

S9.1.3.3 [Reserved for test procedures on receiving BSMs from a DSRC test device]

S9.1.3.4 [Reserved for test procedures on ensuring interoperability with other approved non-DSRC V2V devices]

Appendix A: V2V Privacy Statement

a) V2V Messages

The National Highway Traffic Safety Administration (NHTSA) requires that your vehicle be equipped with a Vehicle-to-Vehicle (V2V) safety system. The V2V system is designed to give your vehicle a 360 degree awareness of the driving environment and warn you in the event of a pending crash, allowing you to take actions to avoid or mitigate the crash, if the manufacturer of your vehicle has installed V2V safety applications.

Your V2V system periodically broadcasts and receives from all nearby vehicles a V2V message that contains important safety information, including vehicle position, speed, and direction. V2V messages are broadcast ten times per second in only the limited geographical range (approximately 300 meters) necessary to enable V2V safety application to warn drivers of pending crash events.

To help protect driver privacy, V2V messages do not directly identify you or your vehicle (as through vehicle identification number or State motor vehicle registration), or contain data that is reasonably or, as a practical matter, linkable to you. For purposes of this statement, V2V data is "reasonably" or "as a practical matter" linkable to you if it can be used to trace V2V messages back to you personally for more than a temporary period of time (in other words, on a persistent basis) without unreasonable expense or effort, in real time or after the fact, given available data sources. Excluding reasonably linkable data from V2V messages helps protect consumer privacy, while still providing your V2V system with sufficient information to enable crash-avoidance safety applications.

b) Collection, Storage and Use of V2V Information

Your V2V system does not collect or store V2V messages except for a limited time needed to maintain awareness of nearby vehicles for safety purposes or in case of equipment malfunction. In the event of malfunction, the V2V system collects only those messages required, and keeps that information only for long enough to assess a V2V device's misbehavior and, if a product defect seems likely, to provide defect information to your vehicle's manufacturer.

NHTSA does not regulate the collection or use of V2V communications or data beyond the specific use by motor vehicles and motor vehicle equipment for safety-related applications. That means that other individuals and entities may use specialized equipment to collect and aggregate (group together) V2V transmissions and use them for any purpose including applications such as motor vehicle and highway safety, mobility, environmental, governmental and commercial purposes. For example, States and localities may deploy roadside equipment that enables connectivity between your vehicle, roadways and non-vehicle roadway users (such as cyclists or pedestrians). These technologies may provide direct benefits such as use of V2V data to further increase your vehicle's awareness of its surroundings, work zones, first responders, accidents, cyclists and pedestrians. State and local entities (such as traffic

control centers or transportation authorities) may use aggregate V2V safety messages for traffic monitoring, road maintenance, transportation research, transportation planning, truck inspection, emergency and first responder, ride-sharing, and transit maintenance purposes. Commercial entities also may use aggregate V2V messages to provide valuable services to customers, such as traffic flow management and location-based analytics, and for other purposes (some of which might impact consumer privacy in unanticipated ways). NHTSA does not regulate the collection or use of V2V data by commercial entities or other third parties.

While V2V messages do not directly identify vehicles or their drivers, or contain data reasonably linkable to you on a persistent basis, the collection, storage and use of V2V data may have residual privacy impacts on private motor vehicle owners or drivers. Consumers who want additional information about privacy in the V2V system may review NHTSA's V2V Privacy Impact Assessment, published by The U.S. Department of Transportation at http://www.transportation.gov/privacy.

If you have concerns or questions about the privacy practices of vehicle manufacturers or third party service providers or applications, please contact the Federal Trade Commission. https://www.ftc.gov.

Federal Motor Vehicle Safety Standard (FMVSS), No. 150, mandating vehicle-to-vehicle (V2V) communications for new light vehicles and standardized messages and format of V2V transmissions

Dated: _____

_____

Anthony R. Foxx, Secretary, Department of Transportation

Billing Code: 4910-59-P