
The Next Step in Auto Safety: Vehicle-to-Vehicle Communications

Course No: C04-036

Credit: 4 PDH

Mark Rossow, PhD, PE, Retired



Continuing Education and Development, Inc.
22 Stonewall Court
Woodcliff Lake, NJ 07677

P: (877) 322-5800
info@cedengineering.com

Introduction to the Study Guide

The U.S. Department of Transportation's National Highway Traffic Safety Administration has issued a Notice of Proposed Rulemaking (NPRM) that 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. The new standard 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 V2V safety applications that are estimated to prevent hundreds of thousands of crashes and prevent over one thousand fatalities annually.

The Study Guide for the present course consists of Section II, "**Background**," of the NPRM. This section has been excerpted and begins near the bottom of the next page.

The entire NPRM can be downloaded by clicking on this [link](#), but the present course is based solely on the material in Section II.

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.

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 industry⁴ – 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

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.

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_ihs_commitment_on_aeb_03172016 (last accessed Dec 7, 2016).

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.

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 2010-2013¹¹ 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 MAIS¹² 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).

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.

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.

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.

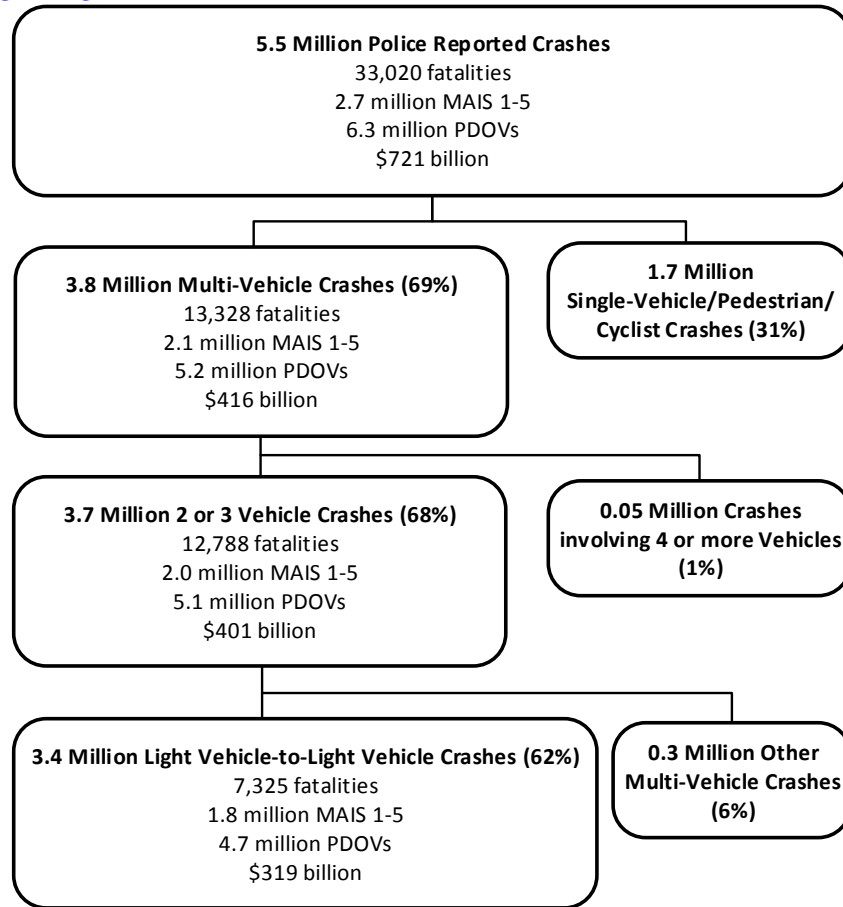


Figure II-1 Crash Population Breakdown for V2V Technology

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)

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.

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).

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.

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

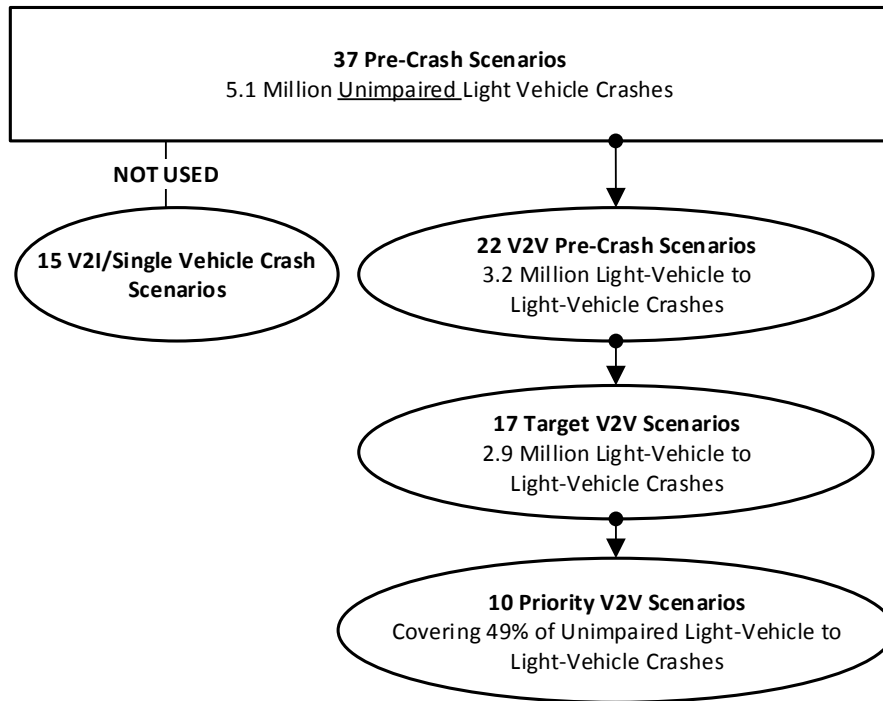


Figure II-2 V2V Pre-Crash Scenario Breakdown¹⁶

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 Warning/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

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.

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).

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.

(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

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.

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 component

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.

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.

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

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.

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”).

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.

possibly introduce security risks, such as cyberattacks or privacy concerns²⁵, 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.

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.

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.

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.

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

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.

cannot (e.g., vehicles approaching each other at intersections).³⁰ Honda Motor Co., 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 un contemplated 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

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.

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).

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.

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;

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.

- 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

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.

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

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.

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.

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.

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

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.

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).

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.

- 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 V2V deployment 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.

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.

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	[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.	DSRC On-Board Unit Performance Measures Booze Allen and Hamilton	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).	BAH Completion date – Requirements October 2015/Test Procedures October 2015
Research Need V-3 DSRC Data Communication System Performance Measures		Crash Avoidance Metrics Partnership - Documentation of On-Board Unit Requirements and Certification Procedures for V2V Systems (System Engineering Project)		CAMP System Engineering Completion date – Requirements Aug 2015/Test Procedures Sept 2015
Research Need V-5 BSM Congestion Sensitivity	[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.	and		CAMP Communications research completion date – August 2016
Research Need V-6 Relative Positioning Performance Test		V2V-Communication Research project	CAMP will develop a single comprehensive document summarizing the minimum level of Connected Vehicle (CV) V2V safety system on-board requirements and	

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.

<p>Research Need V-7 Vehicle and Receiver Positioning Biases</p> <p>Research Need VI-7 Compliance Specifications and Requirements</p>	<p>[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.</p> <p>[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.</p> <p>[V-7] Research to understand potential erroneous position reporting due to positional biases across multiple GPS receiver combinations.</p> <p>[VI-7] Development of performance requirements, test procedures, and test scenarios</p>		<p>certification procedures.</p> <p>CAMP V2V Communications Research Project will identify requirement in relation to BSM message congestion mitigation and misbehavior detection</p>	
---	--	--	---	--

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.

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

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.

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

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.

				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	[VIII-1] Assess the availability of information and technologies that facilitate linking data in the BSM to determine a motor vehicle's path	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
Research Need VIII-2 V2V Identification Capabilities				
Research Need VIII-3 V2V Inventory of Privacy Controls	[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)			
Research Need VIII-4 V2V Privacy Risk Assessment				
Research Need IX-2				

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.

<p>Cryptographic flexibility</p> <p>Research Need IX-3 Independent Security Design Assessment</p>	<p>[VIII-3] Inventory and assess the privacy controls applicable to the SCMS in connection with our comprehensive privacy assessment</p> <p>[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.</p> <p>[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.</p> <p>[IX-3] Independent evaluation</p>			
---	---	--	--	--

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.

	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.

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.

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
<p>Research Need V-4 Development of Safety Application Test Metrics and Procedures</p> <p>Research Need VI-2 Safety Application Performance Measure Rationale</p> <p>Research Need VI-3 Practicability of Non-Ideal Driving Condition Testing</p> <p>Research Need VI-4 Fused and Non-Fused V2V Safety Application Test Procedures</p> <p>Research Need VI-5 Performance and Test Metric Validation</p>	<p>[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.</p> <p>[VI-1] Assess the capability and capacity of possible refinements to reduce frequency of false positive warning while maintaining crash avoidance effectiveness.</p> <p>[VI-2] Develop a rationale to support each performance and test metric recommended for incorporation into an FMVSS.</p> <p>[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.</p>	<p>Volpe False Alert Scenarios and Objective Test Procedures for Crash Avoidance Applications project and</p> <p>Vehicle Research and Test Center project</p>	<p>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.</p> <p>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.</p>	<p>Volpe Completion Date – December 2018</p> <p>VRTC Completion Date – April 2019</p>

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.

	<p>[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).</p> <p>[VI-5] Conduct test validation to ensure that the performance and test metrics are objective, repeatable, and practicable.</p>			
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: November 2016

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.

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.

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.

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

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.

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)

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.

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

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.

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)

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.

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.

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.

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.*

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.

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.

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.

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 good⁷⁶ 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.

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.

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, DENSO⁸⁸ 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.

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.

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., Qualcomm¹⁰⁰) and other associations (e.g., the Wi-Fi Alliance¹⁰¹) 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.

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.

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 Institute¹⁰⁹ 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.

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.

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).

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.

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