U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

NHTSA
www.nhtsa.gov

DOT HS 812 014 **August 2014**

Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application

DISCLAIMER

This publication is distributed by the U.S. Department of Transportation, National Highway Traffic Safety Administration, in the interest of information exchange. The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the Department of Transportation or the National Highway Traffic Safety Administration. The United States Government assumes no liability for its contents or use thereof. If trade or manufacturers' names or products are mentioned, it is because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Suggested APA Format Citation:

Harding, J., Powell, G., R., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., & Wang, J. (2014, August). *Vehicle-to-vehicle communications: Readiness of V2V technology for application.* (Report No. DOT HS 812 014). Washington, DC: National Highway Traffic Safety Administration.

Technical Report Documentation Page

1. Report No. DOT HS 812 014	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application		5. Report Date August 2014 6. Performing Organization Code
7. Authors John Harding, Gregory Powell, Rebecca Yoon, Joshua Fikentscher, Charlene Doyle, Dana Sade, Mike Lukuc, Jim Simons and Jing Wang		8. Performing Organization Report No.
9. Performing Organization Name and Address National Highway Traffic Safety Administration 1200 New Jersey Avenue SE. Washington, DC 20590		10. Work Unit No. (TRAIS) 11. Contract or Grant No.
12. Sponsoring Agency Name and Address		13. Type of Report and Period Covered Research 14. Sponsoring Agency Code
15. Supplementary Notes		

16. Abstract

The purpose of this research report is to assess the readiness for application of vehicle-to-vehicle (V2V) communications, a system designed to transmit basic safety information between vehicles to facilitate warnings to drivers concerning impending crashes. The United States Department of Transportation and NHTSA have been conducting research on this technology for more than a decade. This report explores technical, legal, and policy issues relevant to V2V, analyzing the research conducted thus far, the technological solutions available for addressing the safety problems identified by the agency, the policy implications of those technological solutions, legal authority and legal issues such as liability and privacy. Using this report and other available information, decision-makers will determine how to proceed with additional activities involving vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P) technologies.

17. Key Words vehicle-to-vehicle communications, crash avoidance, connected vehicle, safety applications, model deployment, safety pilot, vehicle awareness device, integrated device, aftermarket safety device, communication security, security credential management system, V2V technology		18. Distribution Statement Document is available to the public from the National Technical Information Service www.ntis.gov	
19 Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21 No. of Pages 327	22. Price

Table of Contents

Acronyms

AAMVA	American Association of Motor Vehicle Administrators
ABS	antilock braking system
ACM	a la carte message set
ACN	automatic crash notification
AERIS	Applications for the Environment: Real-Time Information Synthesis
AHS	Automated Highway System Program
ANPRM	Advanced Notice of Proposed Rulemaking
ARIB	Association of Radio Industries and Businesses
ARINC	Aeronautical Radio Incorporated
ASD	aftermarket safety device
ASTM	American Society for Testing and Materials
ATM	automatic teller machine
ATMIA	ATM Industry Association
BAH	Booz Allen Hamilton
BSM	basic safety message
BSW	blind spot warning
CA	certificate authority
CAMP	Crash Avoidance Metrics Partnership
CAN	controller area network
CARS	Car Allowance Rebate System - "Cash for Clunkers"
CBP	channel busy percentage
CCH	control channel
CFR	Code of Federal Regulations
CICAS-V	Cooperative Intersection Collision Avoidance System-Violation
CLW	control loss warning
CME	certificate management entity
CP	certificate policy
CRL	certificate revocation list
CSR	common safety request (message set)
CSW	curve speed warning
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DAC	(V2V Light Vehicle) Driver Acceptance Clinics
DCM	device configuration manager
DE	data element
DF	data frame
DG CONNECT	European Commission Directorate General for Communication Networks, Content and Technology
DIACAP	DOD Information Assurance Certification and Accreditation Process
DNPW	do not pass warning

DOD	U.S. Department of Defense
DOT	U.S. Department of Transportation
DSRC	dedicated short-range communications
DSRCS	Dedicated Short Range Communications Systems
DVI	driver-vehicle interface
ECA	enrollment certificate authority
ECU	electronic control unit
EEBL	emergency electronic brake lights
EIA	Energy Information Administration
ELVS	End of Life Vehicle Consortium
EPA	Environmental Protection Agency
ESC	electronic stability control
ETSI	European Telecommunications Standards Institute
EU	European Union
EUR	European Union Region
FAA	Federal Aviation Administration
FARS	Fatality Analysis Reporting System
FCC	Federal Communication Commission
FCW	forward collision warning
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
FMVSS	Federal Motor Vehicle Safety Standard
FOT	field operational test
FSS	fixed satellite service
FTC	Federal Trade Commission
GDP	gross domestic product
GES	General Estimates System
GHz	gigahertz - frequency measurement
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
HUD	heads-up display
HV	host vehicle
HW	hardware
ICA	intersection collision avoidance
ICANN	Internet Corporation for Assigned Names and Numbers
ID	identification
IEEE	Institute of Electrical and Electronics Engineers
IMA	Intersection Movement Assist
IPG	inter-packet gap
ISACA	Information Systems Audit and Control Association
ISM	Industrial, Scientific and Medical
ISTEA	Intermodal Surface Transportation Efficiency Act
ITIS	Integrated Taxonomic Information System
ITS	Intelligent Transportation System
IVBSS	Integrated Vehicle-Based Safety Systems

IVI	Intelligent Vehicle Initiative
JPO	Joint Program Office
LA	Linkage Authority
LCW	lane change warning
LDW	lane departure warning
LLC	logical link control
LOP	location obscurer proxy
LTA	left turn assist
LTAP/OD	left turn across path/opposite direction
LTV	Light-truck vehicle
LVD	lead vehicle decelerating
LVM	lead vehicle moving
LVS	lead vehicle stopped
MA	misbehavior authority
MAC (Section IV)	Message Authentication Code
MAC (Section VIII)	Medium Access Control
MAIS	Maximum Abbreviated Injury Scale
MLIT	Japanese Ministry of Land, Infrastructure, Transportation and Tourism
MOU	Memorandum of Understanding
MY	model year
NAS	National Academy of Sciences
NCAP	New Car Assessment Program
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NPRM	Notice of Proposed Rulemaking
NTCIP	National Transportation Communications for Intelligent Transportation System Protocol
NTIA	National Telecommunications and Information Administration
NTTAA	National Technology Transfer and Advancement Act
OBE	on-board equipment
OBU	on board units
ODI	Office of Defects Investigations
OE	original equipment
OEM	original equipment manufacturer
OST-R	Department of Transportation Office of the Assistant Secretary for Research and Technology
OTA	Over the air
OVW	Oversize Vehicle Warning
PC	Passenger car
PCA	Pseudonym Certificate Authority
PCI DSS	Payment Card Industry Data Security Standard
PDO	property-damage-only
PER	packet error rate
PII	Personally-identifiable information
PKI	public key infrastructure

POC	proof of concept
PPP	public private partnership
PPS	pulse per second
PPSG	NTIA’s Policy and Plans Steering Group
PRA	Paperwork Reduction Act
PSID	provider service identifier
PTE	position tracking error
RA	registration authority
RCVW	railroad crossing violation warning
RF	radio frequency
RLVW	red light violation warning
RSD	retrofit safety device
RSE	road-side equipment
RSU	road side unit
RSZW	reduced speed zone warning
RTCM	Radio Technical Commission for Maritime Services
RTK	right turn into path
RV	remote vehicle
SAE	Society of Automotive Engineers
SCH	service channel
SCMS	Security Credentials Management System
SCP	straight crossing path
SD	secure digital
SE	system engineering
SHRP2	Strategic Highway Research Program 2
SP	single point
SPaT	signal phase and timing
SSGA	stop sign gap assist
SSP	service specific priority
SSVW	stop sign violation warning
STD	Standard
SW	Software
SWIW	spot weather information warning
TEA-21	Transportation Equity Act for 21st Century
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
UBI	usage based insurance
UDP	user datagram protocol
UMRA	Unfunded Mandates Reform Act
UMTRI	University of Michigan Transportation Institute
U-NII	Unlicensed-National Information Infrastructure
USDOT	U.S. Department of Transportation
UTC	Coordinated Universal Time
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Other [pedestrian, bicycle, etc.]

VAD	vehicle awareness device
VII	vehicle infrastructure integration
VIIC	Vehicle-Infrastructure Integration – Consortium
VIN	Vehicle Identification Number
VMT	vehicle miles traveled
VSC	vehicle safety communications
VSL	value of statistical life
VTTI	Virginia Tech Transportation Institute
WAAS	Wide Area Augmentation System
WAVE	Wireless Access for Vehicular Environments
WLAN	wireless local area network
WRV	warning range variance
WSM	wave short message
XML	Extensible Markup Language

I. Executive Summary

The National Highway Traffic Safety Administration helps to reduce deaths, injuries, and economic losses resulting from motor vehicle crashes by setting and enforcing safety performance standards for motor vehicles and motor vehicle equipment. Vehicle manufacturers respond to NHTSA's standards by building safer vehicles. Combined with State and local government efforts, market effects, and driver behavior improvements, NHTSA's standards have contributed to a significant reduction in annual highway fatalities and injuries, from 52,627 fatalities in 1970,[1] to 32,479 fatalities in 2011.[2]

The purpose of this research report is to assess the readiness for application of vehicle-to-vehicle (V2V) communications, a system designed to transmit basic safety information between vehicles to facilitate warnings to drivers concerning impending crashes. The United States Department of Transportation and NHTSA have been conducting research on this technology for more than a decade.

Safety technology has developed rapidly since NHTSA began regulating the auto industry – vehicles protect occupants much better in the event of a crash due to advanced structural techniques propagated by more stringent crashworthiness standards, and some crash avoidance technologies are now standard equipment. Between existing crashworthiness and required standard crash avoidance technologies, motor vehicles are safer now than they have ever been.

However, a significant number of annual crashes remains that could potentially be addressed through expanded use of more advanced crash avoidance technologies. The agency estimates there are approximately five million annual vehicle crashes, with attendant property damage, injuries, and fatalities. While it may seem obvious, if technology can help drivers avoid crashes, the damage due to crashes simply never occurs.

The agency's push thus far for adoption of crash avoidance technologies, like electronic stability control, has helped *vehicles* react to crash-imminent situations, but has not yet been able to help the *driver* react ahead of time. To fill that gap, some of the most advanced crash

[1] National Center for Health Statistics, HEW and State Accident Summaries (Adjusted to 30-Day Traffic Deaths by NHTSA).
[2] National Highway Traffic Safety Administration, Fatality Analysis Report System (FARS) final 2011 data. For more information, see*:* www.nhtsa.gov/FARS (last accessed Feb. 12, 2014).

avoidance technologies present on vehicles today include a host of on-board sensors, cameras, and radar applications. These technologies may warn drivers of impending danger so that the driver can take corrective action, or may even be able to intervene on the driver's behalf.

While these "vehicle-resident" crash avoidance technologies can be highly beneficial, V2V communications represent an additional step in helping to warn drivers about impending danger. V2V communications use on-board dedicated short-range radio communication devices to transmit messages about a vehicle's speed, heading, brake status, and other information to other vehicles and receive the same information from the messages, with range and "line-of-sight" capabilities that exceed current and near-term "vehicle-resident" systems -- in some cases, nearly twice the range. This longer detection distance and ability to "see" around corners or "through" other vehicles helps V2V-equipped vehicles perceive some threats sooner than sensors, cameras, or radar can, and warn their drivers accordingly. V2V technology can also be fused with those vehicle-resident technologies to provide even greater benefits than either approach alone. V2V can augment vehicle-resident systems by acting as a complete system, extending the ability of the overall safety system to address other crash scenarios not covered by V2V communications, such as lane and road departure. A fused system could also augment system accuracy, potentially leading to improved warning timing and reducing the number of false warnings. For a discussion of NHTSA's views as to how the various levels of vehicle automation will play an important role in reducing crashes and how on-board systems may someday work cooperatively with V2V technology, see NHTSA's Preliminary Statement of Policy on Vehicle Automation (May 2013).[3]

For several years, NHTSA has been working under a self-imposed goal of making an agency decision regarding light-duty V2V communication systems in 2013. NHTSA substantially completed the work necessary to reaching that decision by the end of 2013, and announced that decision in early 2014. "Agency decision," in this case, means the agency's choice of the best course of action with regard to exercise of its regulatory and research authority in the V2V context. Among the factors considered in making that decision were NHTSA's preliminary estimates of V2V technology's ability to reduce fatalities and injuries from motor vehicle crashes; the practicality of the technology from the perspectives of maturity, cost, reliability, and performance; and the existence of ways to test and measure V2V technology performance objectively.

The objective of this report is to analyze the research conducted thus far, the technological solutions available for addressing the safety problems identified by the agency, the policy implications of choosing those technological solutions, legal authority and legal issues

[3] NHTSA's Preliminary Statement of Policy on Vehicle Automation (May 2013). See www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf (last accessed Jan. 22, 2014).

such as liability and privacy. Using this report and other available information, decision-makers will determine how to proceed with additional activities involving V2V, V2I, and V2P technologies.

In summary, based on the research and analysis conducted by NHTSA and its partners so far, it appears that:

- V2V devices installed in light vehicles as part of the Connected Vehicle Safety Pilot Model Deployment were able to transmit and receive messages from one another, with a security management system providing trusted and 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 others participating in the Model Deployment (e.g., its research partners and devices suppliers) found that the standards did not contain enough detail and left too much room for interpretation. 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 recognizes 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. Based on the agency's understanding of how these prototype safety applications operate, preliminary effectiveness estimates indicate substantial ability to mitigate crashes, injuries or fatalities in these crash scenarios. Also, 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). Finally, more research would help the agency develop objective performance tests that would ensure consistent operation that is helpful to drivers.

- The agency has the legal authority to mandate V2V (DSRC) devices in new light vehicles, and could also require them to be installed in commercial vehicles already in use on the road. 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 required to support deployment of V2V technologies in motor vehicles.

- Based on preliminary information, NHTSA currently estimates that the V2V equipment and supporting communications functions (including a security management system) would cost approximately $341 to $350 per vehicle in 2020. 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). 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 range from $1 to $6 per vehicle, and they will increase over time due to the need to support an increasing number of vehicles with the V2V technologies. The communications costs range from $3 to $13 per vehicle. Cost estimates are 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, the total projected preliminary annual costs of the V2V system fluctuate year after year but generally show a declining trend. The estimated total annual costs range from $0.3 to $2.1 billion in 2020 with the specific costs being dependent upon the technology implementation scenarios and discount rates. The costs peak to $1.1 to $6.4 billion between 2022 and 2024, and then they gradually decrease to $1.1 to $4.6 billion.

- In terms of safety impacts, the agency estimates annually 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. We chose those two applications for analysis at this stage because they are good illustrations of benefits that V2V can provide above and beyond the safety benefits of vehicle-resident cameras and sensors. Of course, the number of lives potentially saved would likely increase significantly with the implementation of additional V2V and V2I safety applications that would be enabled if vehicles were equipped with DSRC capability.

Even with the success of the Safety Pilot Model Deployment in proving that V2V technology can work in a real-world environment on actual roads with regular drivers, additional items need to be in place beyond having the authority to implement a V2V system, in order for a potential V2V system to be successful. These items include:

- Wireless spectrum: V2V communications transmit and receive messages at the 5.8-5.9 GHz frequency. The FCC is currently 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. Given that Wi-Fi use is growing exponentially, "opening" the 5.8-5.9 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 needs to be done on whether these Wi-Fi enabled devices can share the spectrum successfully with V2V, and if so, how.

- 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 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. It is 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 current security design, it also is likely that the 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.

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

  NHTSA is currently engaged in research to examine the minimum performance measures for DSRC communication and system security. This research will include functional and performance requirements for the DSRC device and is intended to include how to address end-of-life issues on the DSRC components and security system.

  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 has yet to determine 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. In order to create the required environment of trust, a V2V system must include security infrastructure to credential each 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). NHTSA currently anticipates that private entities will create, fund, and manage the security and communications components of a V2V system. While NHTSA has identified several potential types of entities, including some specific entities, which might be interested in participating in a V2V security system, private entities have not committed to doing so to date.

- Liability concerns from industry: Auto manufacturers repeatedly have expressed to the agency their concern 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 currently under consideration by NHTSA involve safety warning technologies -- not control technologies. NHTSA’s legal analysis indicates 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 does not view V2V warning technologies as creating new or unbounded liability exposure for the industry.

- Privacy: At the outset, readers should understand some very important points about the V2V system as currently contemplated by NHTSA. The system will not collect or store any data identifying individuals or individual vehicles, nor will it enable the government to do so. There is no data in the safety messages exchanged by vehicles or collected by the V2V system that could be used by law enforcement or private entities to personally identify a speeding or erratic driver. The system—operated by private entities—will not enable tracking through space and time of vehicles linked to specific owners or drivers. Third parties attempting to use the system to track a vehicle would find it extremely difficult to do so, particularly in light of far simpler and cheaper means available for that purpose. The system will not collect financial information, personal communications, or other information 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 will 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, as designed, NHTSA is confident that the V2V system both achieves the agency's safety goals and protects consumer privacy appropriately.[4]

- Consumer acceptance: If consumers do not accept a required safety technology, the technology will not create the safety benefits that the agency expects. One potential issue with consumer acceptance is maintenance. 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 return to a dealership periodically for a download of new certificates, consumers may choose instead to live with non-functioning V2V capabilities. The agency is exploring ways to make such downloads automatic, but more research is needed to understand this issue fully.

The above issues indicate that through the research conducted to date, the agency has a better understanding of the potential of V2V technology, but various aspects of the technology still need further investigation to support transition from a prototype-level to a deployment-level system. Further research to move toward deployment has been identified (and detailed in this report) and will be conducted to address the following:

- The impact of spectrum sharing with U-NII devices;
- Development of performance requirements for DSRC devices;
- Development of performance requirements for safety applications;
- The potential establishment of device certification and compliance procedures;
- The ability to mitigate V2V communication congestion:
- Incorporation of GPS positioning advancements to improve V2V relative positioning;
- Remedies to address false positive warnings from V2V safety applications;
- Driver-vehicle interface performance to enhance crash avoidance warning effectiveness;
- An appraisal of consumer acceptance of the technology;

[4] NHTSA acknowledges that privacy and system security are current and relevant areas of discussion and that some may have concerns about the vulnerability of this system to malicious attack. We understand those concerns and intend to explore the risks and safeguards fully in our in-depth analysis of system security. Recently, for example, we have been in contact with DARPA about possible protections against software vulnerabilities.

- Evaluation of V2V system privacy risks; and
- An assessment of the security system to ensure a trusted and a safe V2V system.

The GAO report "Intelligent Transportation Systems, Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist"[5] confirms the appropriateness of the research identified. This research will facilitate a comprehensive representation of a deployment-ready V2V system. NHTSA, with the Intelligent Transportation System Joint Program Office, has positioned the resources needed to accomplish this research to support the possible deployment of V2V given any agency action.

[5] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

II. Introduction

A. Purpose of this report

For several years, NHTSA has indicated its intention to make an agency decision regarding light-duty V2V communication systems in 2013.[6] NHTSA substantially completed the work necessary to reaching that decision by the end of 2013, and announced that decision in early 2014. "Agency decision," in this case, referred to the agency's choice of the best course of action with regard to exercise of its regulatory and research authority in the V2V context. Among the factors considered in making that decision were V2V technology's ability to reduce fatalities and injuries from motor vehicle crashes; the practicality of the technology from the perspectives of maturity, cost, reliability, and performance; and the existence of ways to test and measure V2V technology performance objectively.

The objective of this report is to assess the readiness for application of V2V communications technology, by discussing the research conducted thus far, of the technological solutions available for addressing the safety problems identified by the agency, the policy implications of choosing those technological solutions, the agency's legal authority and related legal issues such as liability and privacy, and potential implementation options available to the agency for creating a national V2V system. Using this report and other available research, agency decision-makers determined how to proceed with additional activities involving vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-pedestrian technologies.

In September 2012, NHTSA's Senior Associate Administrator for Vehicle Safety formed the V2V Decision Team to examine these and other related issues and summarize the current state of knowledge on V2V. The team consisted of members from the NHTSA's offices of Vehicle Safety Research, Rulemaking, Enforcement, the NHTSA National Center for Statistical Analysis, and Chief Counsel and from the Federal Highway Administration, the Department of Transportation's Office of the Assistant Secretary for Research and Technology (OST-R), the DOT's John A. Volpe National Transportation Systems Center and the Intelligent Transportation System Joint Program Office (ITS-JPO).[7]

In particular, ITS-JPO, OST-R, and FHWA played a vital supporting role in the analysis by representing the broader interests of DOT's Intelligent Transportation Systems wide-ranging programs and assessing the potential impacts that an agency decision on V2V technology could

[6] *E.g.*, NHTSA Vehicle Safety Rulemaking and Research Priority Plan 2009-2011 (July 2009, Docket No. NHTSA-2009-0108-0001) and NHTSA Vehicle Safety and Fuel Economy Rulemaking and Research Priority Plan 2011-2013 (March 2011, Docket No. NHTSA-2009-0108-0032). See www.nhtsa.gov/Laws-Regs (last accessed Jan. 23, 2014).

[7] For more information on ITS-JPO, *see* www.its.dot.gov.

have. Additionally, ITS-JPO has been a supporting partner throughout the Connected Vehicle[8] Safety Pilot program,[9] working collaboratively with NHTSA's Vehicle Safety Research office to develop and execute the valuable information obtained by the program and used, in part, to inform the agency decision on V2V technology.

The Volpe Center played a vital role, as it does with many DOT programs, by providing critical expertise in the many specialized areas of both ITS and V2V. For example, Volpe Center experts developed and validated the Simulation Tool used for determining the preliminary V2V system benefits for this analysis. Additionally, the Volpe Center is contracted to operate as the Independent Evaluator of the data collected during the Safety Pilot Model Deployment.

This report was presented by the team to the SAA and constitutes analysis of the relevant issues and suggestions on various options before the agency. After full discussion of the report and the issues with the political leadership in NHTSA and DOT, the agency reached its decision on the future course of agency action.

The report breaks down the decision by describing and examining elements of the technology and the deployment of the technology using the results of available research. The sections of this report cover:

- how the technology addresses the safety need;
- an investigation of the legal and policy issues associated with the secure operation of the technology and the implications of these issues for privacy;
- a description of the technology, the different types of devices, the elements of the devices, and the security needed for trusted communications; and
- how much the technology may be expected to cost, in terms of both consumer and operational costs and potential effectiveness and benefits of the technology (based on preliminary data).

[8] DOT has long used the term "connected vehicle" to refer to the vehicle-to-vehicle communication technology that supports crash avoidance applications. However, more recently the term has also been associated with vehicle telematics that connects vehicles to various information and "infotainment" applications through other forms of communication. There will be references in this report to "connected vehicle" and in the context of this report these references are intended to mean V2X technology.

[9] The Connected Vehicle Safety Pilot Program is 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. For more information, see www.its.dot.gov/safety_pilot/#sthash.LL2V6yT0.dpuf (last accessed Jan.23, 2014).

B. History of V2V communication research program

1. History of ITS

Before Intelligent Transportation Systems (ITS), the United States developed, planned, and built the interstate highway system. The interstate highway system has provided a high level of mobility for citizens as well as the efficient movement of goods. From the 1950s through the 1980s, the vision of highway transportation was focused on building roads. Yet issues began to emerge as the interstate system was being built: about traffic congestion, especially in our urban centers; about highway-related fatalities and injuries due to crashes; and about the impacts on energy consumption and air quality.

As early as 1986, a group of transportation professionals from academia, Federal agencies, State transportation agencies, and the private sector started to discuss the future of transportation in relation to the post-interstate era.[10] New transportation legislation needed to be developed, meaning that a new transportation paradigm needed to be invented that would use the current infrastructure, but also address the issues of safety, congestion, and environment.

The discussions culminated in a workshop held in Dallas, Texas, in 1990. During the workshop, participants invented the Intelligent Vehicle Highway Systems (IVHS) concept, which was later renamed to ITS.[11] The overall precept was that new transportation efficiencies could be found if current infrastructure could be married with advanced technology. New developments in computing, sensors, information systems, and advanced mathematical methods could be used to increase the operational capacity of the system, and achieve better overall transportation network operations.

The ITS concept became an integral part of the 1991 Intermodal Surface Transportation Efficiency Act (ISTEA). The Act allocated $660 million of funds for ITS research, development, and operational tests over six years. In addition, just before the Act was adopted, the Intelligent Vehicle Highway Society of America advisory organization was established; later renamed Intelligent Transportation Society of America. This advisory organization developed the first strategic plan for ITS in 1992. The plan called for the integrated operation of the system using technology to bring together information about modes and current conditions, and discussed how institutions can be organized to operate the total transportation network.[12]

[10] Perspectives on Intelligent Transportation Systems (Sussman, 2005). See Docket No. NHTSA-2014-0022

[11] Sustainable Build Environment, Vol. II, Intelligent Transportation Systems (Williams). See www.eolss.net/Sample-Chapters/C15/E1-32-08-05.pdf (last accessed Jan. 23, 2014).

[12] The 1992 Strategic Plan by IVHS. See http://ntl.bts.gov/lib/jpodocs/repts_pr/1823.pdf (last accessed Jul. 12, 2013).

ITS covers many areas that have been adjusted and renamed over the years, but the basic tenets of safety, mobility, and environment have remained. The components of ITS have been characterized by various management systems (areas). The management systems cover information, traffic (signal systems and tolling), designated Advanced Traffic Management Systems, and Advanced Vehicle Control Systems. Over the years, the integration of transportation and technology has continued. Currently, Congress authorizes approximately $100 million a year for the continued research and development of ITS.[13]

There are a number of ITS program-developed applications deployed throughout the nation. These include both automated toll collection along with advanced traffic signal control systems and centers that monitor a region's transportation network to address network issues in real time.

Many involved with ITS research and development view the development of the capability to provide connectivity to the transportation system as the next frontier, in order to further improve safety, mobility, and the environment. Using DSRC in the mobile environment may support that connectivity for an array of transportation applications.[14]

Envisioning that vehicles communicating with other vehicles around them could identify potential crash situations and alert the drivers so that these situations could be avoided, DOT and the Crash Avoidance Metrics Partnership (CAMP) initiated the first V2V research in December 2006. DSRC, as a Wi-Fi-based technology, provides 360 degrees of coverage, whereas vehicle-based sensors can be more limited in terms of direction and distance at which they are able to detect a potential conflict. V2V systems predominantly apply to crashes with multiple vehicles, and these systems have the potential to address a large number of crashes.

2. History of V2V research program and its role in ITS

V2V communications research initially began under the Vehicle Infrastructure Integration Initiative in 2003, but its origins date back to the Automated Highway System (AHS) research of the 1990s.

The actual initiation of advanced technology research was mandated by the ISTEA.[15] The Act called for the development of an automated intelligent vehicle highway prototype that would use technology to make highway driving efficient, safe, and predictable. The effort was

[13] Moving Ahead for Progress in the 21st Century Act (MAP-21) at sec. 51001(a)(4) (Pub.L.112-141; July 6, 2012). See www.gpo.gov/fdsys/pkg/PLAW-112publ141/pdf/PLAW-112publ141.pdf (last accessed Jan. 23, 2014)

[14] ITS Strategic Research Plan 2010-2014, Progress Update 2012 (FHWA-JPO-12-019). See www.its.dot.gov/strategicplan/pdf/ITS%20Strategic%20Plan%20Update%202012.pdf (last accessed Jan. 24, 2014).

[15] For more information, see the Automated Highway System, Public Roads (Summer 1994, Vol. 58, No. 1, Nita Congress) at www.fhwa.dot.gov/publications/publicroads/94summer/p94su1.cfm (last accessed Jan. 24, 2014).

designated the "Automated Highway System Program." The goal of the effort was to have a fully automated roadway or test track in operation by 1997.

The AHS Program started in 1992 as part of DOT's ITS initiative that fell within the Advanced Vehicle Control Systems Area. Research activities looked into 16 different precursor areas to support the design of a prototype automated highway. The basic concept was that sensors in the roadway would communicate with sensors on the vehicle, to enable "hands-off" and "feet-off" but not "mind-off" driving. For the first time, the roadway and the vehicle would actually be connected.

The AHS concept required dedicated lanes that would contain magnetic nails that the vehicle sensors would recognize and use to guide the vehicle down the intelligent lane. The benefits of AHS would theoretically be derived from decreasing the amount of driver error; increasing the capacity of the highway; facilitating reduced fuel consumption and tailpipe emissions; and providing more efficient commercial and transit operations.

The research culminated in a 1997 demonstration conducted on I-15 in San Diego, California, with more than 20 AHS-equipped vehicles demonstrating hands- and feet-off driving. However, the idea that AHS needed dedicated lanes for the equipped vehicles posed a problem of where to put those lanes and how to finance them. AHS provided a glimpse of one possible future, but priorities changed in 1998 and the emphasis in relation to highway automation was refocused on developing technology that could address near-term safety.[16]

After AHS, DOT introduced the Intelligent Vehicle Initiative (IVI) in 1997, which was authorized in the 1998 Transportation Equity Act for 21st Century (TEA-21). The objectives of IVI were to: (1) prevent driver distraction, and (2) facilitate accelerated deployment of crash avoidance systems.[17] Intelligent vehicle technology included development of vehicle-based and infrastructure-cooperative assistance products that would help drivers operate more safely and effectively. The premise of the IVI program was "to develop and deploy intelligent vehicle systems that completely consider the driver's capabilities and limitations, rather than focus on developing highway infrastructure technology."[18]

In relation to the prevention of driver distraction, studies were conducted that examined the relationship between distraction and crashes; ways to measure distraction and driver

[16] Traffic Technology International, Whatever Happened to Automated Highway Systems (AHS)? (August-September 2001). See http://faculty.washington.edu/jbs/itrans/bishopahs.htm (last accessed Jan. 24, 2014).

[17] Saving Lives Through Advanced Vehicle Safety Technology, Intelligent Vehicle Initiative, Final Report, (September 2005, FHWA-JPO-05-057). See http://ntl.bts.gov/lib/jpodocs/repts_pr/14153_files/ivi.pdf (last accessed Jan. 24, 2014).

[18] An Overview of Automated Highway Systems (AHS) and the Social and Institutional Challenges they Face (Cheon). See www.uctc.net/papers/624.pdf (last accessed Jan. 24, 2014).

workload; and ways to assess the impact of in-vehicle information on distraction and safety.[19] The results of the driver distraction research suggested that the chaotic nature of crashes precluded the possibility of developing and validating a quantitative model to predict crashes as a function of workload measures.

IVI also developed prototype crash avoidance systems using vehicle-based and infrastructure cooperative technology. The initiative sought to identify the safety problem; develop the performance requirements and specifications for prototypes that would address the safety problem; and, using promising technologies, to prototype and test those avoidance systems. Prototypes that were developed and tested addressed rear-end, road departure, vehicle stability (heavy truck), and intersection crashes. The results of the tests and field operational tests of the prototype systems provided a foundation, e.g., requirements such as the range needed for radar sensors and camera object-detection performance, for further research and private development of crash avoidance safety technologies.

As the IVI research was concluding, new developments in telecommunications prompted a new direction in relation to the interaction of vehicles and infrastructure. The Vehicle Infrastructure Integration (VII) Initiative brought together the results of the IVI, the need for improved traffic operations, and the new developments in telecommunication technology. The focus of the VII initiative was to prove the concept that communications technology could be used to send information among vehicles and between vehicles and the infrastructure.[20]

At the 10th Intelligent Transportation Systems World Congress in Madrid, Spain, in November 2003, DOT announced the initiation of the VII initiative. This was made possible by the FCC allocating 75 MHz of spectrum at 5.9 GHz (where DSRC operates) for research purposes for improving transportation safety and use for other non-safety applications to improve transportation mobility.[21]

Using the spectrum and the foundation of crash avoidance research from past efforts, the vision for the VII initiative was to establish a small-scale implementation to test and evaluate the VII concept of operations. The basic VII concept of operations was that vehicle-to-vehicle and vehicle-to- infrastructure communication could support safety and mobility applications. To prove the concept, research and development needed to be conducted to establish the characteristics of the VII system (e.g., requirements and design specifications for vehicle and

[19] *See supra* note 17.

[20] Final Report: Vehicle Infrastructure Integration Proof of Concept Executive Summary–Vehicle (May 19, 2009). See http://ntl.bts.gov/lib/31000/31100/31135/14477.htm (last accessed Jan. 24, 2014).

[21] See http://apps.fcc.gov/ecfs/document/view;jsessionid=zJy8QddC2zQpvYt2fTQdJTp1qLL3rTmmVZvxb13HPtzwtfMphskN!-856245186!973241960?id=6009850553 (last accessed Jan. 24, 2014).

infrastructure communications devices, network communication, and security and privacy protocols). In December 2006, the DOT entered into a cooperative agreement with five automotive original equipment manufacturers to investigate whether DSRC, in combination with GPS relative positioning, could improve performance of autonomous onboard crash warning systems or enable new communication-based safety applications.[22]

The concept was broken down by two distinct components of the system: the roadside network and the on-board vehicle equipment (OBE). The roadside network supported the communication of information between the system through the road-side equipment (RSE) to the OBE and from the OBE back to the system. The VII research tested the communication on both sides of the RSE. The network connected the RSEs via the system. To prove the concept, prototypes of the roadside network (including RSEs) and the OBEs needed to be developed. Besides equipment, message protocols needed to be established that allowed time-constrained communications between OBEs and RSEs. The mobile communications would not have time to have devices establish a communication link between them in the way that current computers do with a wireless network, but messages still needed to be sent and received.

Laboratory and track tests were completed and the system was refined for an on-road proof of concept test. Data was collected to support analysis and the evaluation of the various components, including communications, the RSE, the network, and the OBEs. Key findings indicated that the VII concept was technically feasible; however, there were areas where the concept could be improved. Key areas that required more research included: (1) antenna placement for both OBEs and RSEs; (2) GPS positioning; (3) security for over the air communications; and (4) security systems operations.[23]

The VII Proof of Concept began with the vision that new telecommunication capabilities could be applied to transportation. It established DSRC as a means to connect vehicles and infrastructure via wireless communications. This foundation provided the information necessary to develop and plan the V2V Safety Application Research Plan and Safety Pilot. In addition, the success of the Proof of Concept provided the catalyst to create the Connected Vehicles Initiative.

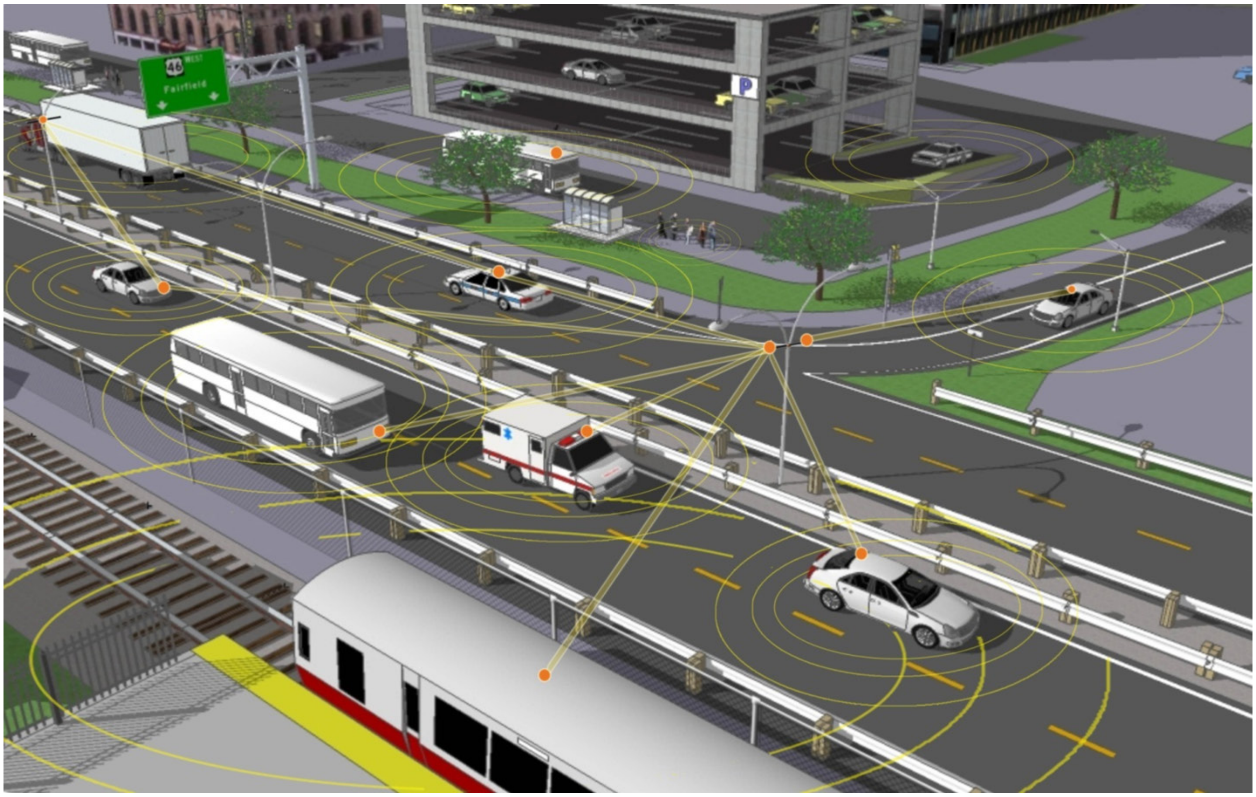
[22] Crash Avoidance Metrics Partnership (CAMP), Vehicle Safety Communications–Applications (VSC-A), Final Report at xi (September 2011, Report No. DOT HS 811 492A). See www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 24, 2014).
[23] Id.

3. The Connected Vehicle Safety Pilot Program

a) Introduction

The Connected Vehicle Safety Pilot Program is part of a major scientific research program run jointly by the DOT and its research and development partners in private industry. The program supports the development of safety applications based on V2V and V2I communications systems, using DSRC technology. The Safety Pilot Model Deployment was designed to inform the effectiveness estimates of these safety applications at reducing crashes and to show how real-world drivers respond to these safety applications in their vehicles. The test includes many vehicles with vehicle awareness devices, others with integrated safety systems, and others that use aftermarket safety devices to communicate with surrounding vehicles. All of these technologies are DSRC-based. The pilot includes multiple vehicle types—cars, trucks, and transit vehicles. The Safety Pilot has concluded for purposes of gathering information on light-duty vehicles, but it has been extended for additional data collection through late 2014.

Figure II-1 Visual Representation of V2V Communication



Note: Vehicles "talk" to each other exchanging information such as vehicle size, position, speed, heading, lateral/longitudinal acceleration, yaw rate, throttle position, brake status, steering angle, wiper status, turn signal status, enabling safety and mobility applications.

While the ITS-JPO within the OST-R is leading this research initiative, several agencies within DOT are supporting the Safety Pilot, including NHTSA, FHWA, Federal Motor Carrier Safety Administration, and Federal Transit Administration.

b) *Research vision*

The vision of the Safety Pilot Model Deployment was to test V2V safety applications in real-world driving scenarios to support estimation of their effectiveness at reducing crashes, and to ensure that the devices are safe and do not unnecessarily distract motorists or cause unintended consequences. The Model Deployment is evaluating everyday drivers' reactions, both in a controlled environment through driver clinics, and on actual roadways with other vehicles through the real-world model deployment.

c) *Research plan*

The two fundamental components of the Safety Pilot are:

Safety Pilot Driver Clinics: Driver clinics were conducted at six sites across the United States to assess user acceptance of the V2V technology. At each driver clinic, approximately 100 drivers tested in-vehicle wireless technology in a controlled environment, such as a race track. The goal was to determine how motorists responded to and benefitted from in-vehicle alerts and warnings. The driver clinics were conducted from August 2011 through January 2012.

Safety Pilot Model Deployment: The Model Deployment is being conducted in the 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 estimation of the effectiveness of V2V technology at reducing crashes. Approximately 2,800 vehicles – a mix of cars, trucks, and transit vehicles operating on public streets within a highly concentrated area – are 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.

The Safety Pilot Model Deployment, with 27 roadside units covering 75 miles of roadway, is also designed to test V2I applications, including:

- Signal priority for transit and emergency vehicles,
- Roadway maintenance,
- Density of pedestrian traffic, and
- Traffic signal timing.

Data from the model deployment is being archived and made available to researchers for evaluation and testing of applications beyond the testing period. The model deployment is the first test of this magnitude of V2V technology in a real-world, multimodal operating environment. UMTRI is leading a diverse team of industry, public agencies, and academia in supporting this effort.

d) Research goals

The goals of the Safety Pilot were to:

- Support the NHTSA agency decision by obtaining empirical data on user acceptance and system effectiveness;
- Demonstrate real-world connected vehicle applications in a data-rich environment;
- Establish a real-world operating environment for additional safety, mobility, and environmental applications development;
- Archive data for additional research purposes; and
- Identify prototype system characteristics that can be improved or that need to be corrected.

e) Research results

The planned outcomes of this research are:

- A determination of whether the system as designed, or somewhat modified, is viable
- Documentation of information helpful in estimating the potential benefits of connected vehicle technologies and evaluation of driver acceptance of vehicle-based safety systems
- Identification of any research needs and the steps to address them
- Analysis of Model Deployment data to support making the agency decision on how to proceed.

4. Studies related to V2V light-vehicle research

As this report focuses on the basis and potential of applying V2V technology to light vehicles, it important to note the agency is also heavily involved in V2V research related to heavy vehicles, pedestrians, and motorcycles.

a) Heavy vehicles

The agency intends to make a decision concerning the disposition of V2V technology concerning heavy vehicles in 2014. The heavy vehicle research is in parallel with the light vehicle research. The interoperability, security, and safety application research associated with light vehicles directly supports the heavy vehicle research. Interoperable devices (both integrated and retrofit) were installed on heavy trucks and run during the Safety Pilot Model Deployment. Heavy vehicle driver clinics were conducted to obtain feedback from professional drivers about V2V crash avoidance systems for heavy vehicles. Data collected during the Safety Pilot Model Deployment will be used to support an evaluation of the V2V technology, but meanwhile, the agency continues to conduct research to better understand the operational contrasts for these vehicles in terms of V2V technology and safety applications.

b) Pedestrians

Past investigation concerning preventing crashes with pedestrians has focused on vehicle-based sensors. The Pedestrian Crash Avoidance and Mitigation project studied the effectiveness of vehicle-based systems to detect a pedestrian in a possible crash situation with a vehicle and warn the driver. With V2V technology, pedestrians can carry devices (such as mobile phones) that can send out a safety signal using DSRC and communicate with DSRC devices that would be used in vehicles. We envision that both the driver and the pedestrian could both be warned if a possible conflict arises. However, there are many issues to be resolved concerning V2P safety applications. The agency is developing a research plan that will investigate issues relating to V2P communication, safety applications, and human factors, among other things. The initial research will identify the pre-crash scenarios involving pedestrians that can be addressed by V2P technology. That analysis will also provide information concerning the dynamics of each pre-crash scenario that will facilitate the prototyping of V2P safety applications.

c) Motorcycles

Motorcycle fatalities represent approximately 11 percent of all highway fatalities each year, and 80 percent of reported motorcycle crashes result in injury or death.[24] A small group of motorcycles were outfitted with Vehicle Awareness Devices and participated in the Safety Pilot Model Deployment. Using VADs on motorcycles enables the motorcycles to be “seen” by other V2V-equipped vehicles, enabling alerts to the driver if a motorcycle and the equipped vehicle are in a possible crash situation. Subsequent analysis of the Safety Pilot Model Deployment data will provide information that will assist in the development of a V2V motorcycle research program. V2V motorcycle research will likely entail investigating how to adapt safety applications to be used by motorcycles and addressing how to warn a motorcyclist of a possible crash situation, among other things.

5. Vehicle-to-infrastructure (V2I)

The same wireless technology that supports V2V safety applications (5.9 GHz DSRC) will also enable a broader set of safety and mobility applications when combined with

[24] Motorcycle Safety (Report No. DOT HS 807 709, revised December 2007). See www.nhtsa.gov/people/injury/pedbimot/motorcycle/motosafety.html (last accessed Jan. 9, 2014).

compatible roadway infrastructure; therefore V2V serves as the gateway for the broader intelligent transportation system program. The Connected Vehicle Core System Architecture[25] describes the overall anticipated system, including V2V and V2I capabilities. DSRC-based V2I communications are also being developed that involve the wireless exchange of critical safety and operational data between vehicles (including brought-in devices) and highway infrastructure, intended primarily to avoid motor vehicle crashes while enabling a wide range of mobility and environmental benefits. The program is funding V2V and V2I communications research within the Dynamic Mobility Applications (real-time traffic information to enhance mobility), Road Weather, Applications for the Environment: Real-Time Information Synthesis (AERIS), and V2I Safety programs.[26] V2I applications under development include applications for commercial freight operators and transit agencies. V2I applications complement the V2V safety applications by addressing crash scenarios that the V2V program cannot address or that could be addressed more efficiently with low levels of penetration of DSRC-equipped light vehicles. The following is a list of V2I potential safety applications:

- Red Light Violation Warning,
- Curve Speed Warning,
- Stop Sign Gap Assist,
- Reduced Speed Zone Warning,
- Spot Weather Information Warning,
- Stop Sign Violation Warning,
- Railroad Crossing Violation Warning, and
- Oversize Vehicle Warning.

Additional mode-specific applications are being developed in partnership with FHWA, FTA, FMCSA, and the Federal Railroad Administration.

The V2I safety research program also focuses on creating national interoperability to support infrastructure and vehicle deployments and facilitating cost-effective infrastructure deployment. DOT and State and local agencies are implementing test beds in Michigan, California, Arizona, Florida, New York, Virginia, and Minnesota to analyze V2I and V2V communications systems. The ITS-JPO created a group[27] for these entities to coordinate lessons learned, in particular related to the implementation of DSRC-based infrastructure.

[25] See www.its.dot.gov/research/systems_engineering.htm (last accessed Jan. 9, 2014).
[26] For detailed information on these programs, see www.its.dot.gov.
[27] For information about the affiliation of Connected Vehicle Test Beds, see www.its.dot.gov/testbed.htm (last accessed Jan. 24, 2014).

The ITS-JPO also awarded a contract with the American Association of State Highway and Transportation Officials to conduct a "National Connected Vehicle Field Infrastructure Footprint Analysis." This analysis was conducted to engage State and local departments of transportation in the development of concepts and scenarios for deployment of V2I systems that will be owned and operated by State and local DOTs. A final report, due later this year, will estimate costs for deployment and operations and maintenance of V2I. In addition to developing a concept for early deployments and a growing National Footprint for V2I systems, the analysis will serve as input to guidance that FHWA is preparing to release in late 2015. The FHWA Public Agency Guidance, currently under development, will initially focus on Federal-aid eligibility, use of right-of-way and infrastructure, innovative financing, procurement processes, and interoperability issues. This initial guidance is intended to address the needs of early demonstration site deployments, and to assist in planning for future investments and deployment of V2I systems. It is envisioned that deployment guidance will evolve as specific applications enter service.

The Basic Safety Message is the primary message set proposed to send data between vehicles and between vehicles and the infrastructure. While the BSM is mainly developed for safety applications, the data in the message may also be used by other connected vehicle applications, such as mobility, weather, and AERIS programs. Additional messages from vehicles or from the infrastructure may also be developed in the future. Some of the applications can also deliver significant safety benefits once implemented. Currently, DOT is developing the applications and planning for field testing, evaluation, and modeling analysis of the benefits.

Also, mobility, weather, and environment applications will benefit from vehicles storing certain limited types of data and, possibly, transmitting and receiving information over multiple communication media, such as DSRC and cellular. The NHTSA decision and market forces may have a role in encouraging vehicle manufacturers to provide storage and cellular capabilities that could facilitate mobility, weather, and environment applications. The following example describes why these capabilities are needed. DOT anticipates that few DSRC RSE units will be installed initially. In order to enable these applications, vehicles would need either to store data gathered along a trip and download it when reaching an RSE unit, or to transmit the information at regular intervals using cellular communications. Data may be used by the public sector to predict travel times along routes, as well as to identify incident locations or areas that may need salt treatments, in order to inform drivers about changes in traffic and road conditions. It will be important for vehicles to be able to receive V2I messages (e.g., Signal Phase and Timing, traveler information messages).

Enabling these capabilities could likely require additional elements in the BSM and could also cause more data to be broadcast to and processed by devices, potentially leading to communication congestion. It is critical that safety messaging not be compromised due to broadcasting more data for V2I. Fortunately, it is likely that mobility, AERIS and weather applications will not need data transmitted 10 times per second. It is expected that the DOT's

ITS-JPO will conduct additional channel congestion analysis to understand the implication of communicating V2I data in addition to V2V data. The ITS-JPO will fund more V2I and V2V modeling and field testing, to be completed within 24 months after a NHTSA decision. The ITS-JPO plans to perform the modeling and field tests and go through a peer review process with NHTSA to validate credibility of the methodology and results.

III. Safety Need

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 Highway Safety Act of 1966.[28] Among other things, NHTSA helps to reduce deaths, injuries and economic losses resulting from motor vehicle crashes by setting and enforcing safety performance standards for motor vehicles and motor vehicle equipment, and through grants to State and local governments to enable them to conduct effective local highway safety programs. Vehicle manufacturers respond to NHTSA's standards by building safer vehicles, and safety technology has developed rapidly since the 1970s – not only are air bags and ESC standard equipment now, but vehicles protect occupants better in the event of a crash due to advanced structural techniques propagated by more stringent crashworthiness standards. Combined with State and local government efforts, market effects, and driver behavior improvements, NHTSA's standards have contributed to a significant reduction in highway fatalities and injuries - from 52,627 fatalities in 1970,[29] to 32,479 fatalities in 2011.[30] Between existing crashworthiness and crash avoidance technologies, motor vehicles are safer than they have ever been.

Nevertheless, crashes continue to occur, with attendant property damage, injuries, and fatalities. Although continued improvements in vehicle crashworthiness will still help reduce fatalities and injuries, NHTSA believes the greatest gains in highway safety in coming years will result from broad-scale application of crash avoidance technologies.[31] Fortunately, the pace of technological development is picking up rapidly as advances in computers and electronics enable new crash avoidance technologies that may not only mitigate the remaining occurring crashes but avoid them entirely. By warning drivers of impending crash situations, V2V technology may be able to reduce the number and severity of motor vehicle crashes, thereby minimizing the costs to society that would have resulted from these crashes.

[28] NHTSA also carries out consumer programs established by the Motor Vehicle Information and Cost Savings Act of 1972.

[29] National Center for Health Statistics, HEW and State Accident Summaries (Adjusted to 30-Day Traffic Deaths by NHTSA).

[30] National Highway Traffic Safety Administration, Fatality Analysis Report System (FARS) final 2011 data. For more information, see www.nhtsa.gov/FARS (last accessed Feb. 12, 2014).

[31] For more information, see the agency policy statement on automated vehicles at www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf (last accessed Jan. 24, 2014).

A. Crashes potentially addressed by V2V technology

Calculating the target potential crashes that V2V-based safety applications could address helps provide a starting point for estimating the magnitude of the problem in terms of the number and severity of crashes and injuries, the number of fatalities, and the societal cost of vehicle crashes. Dividing up the potential target crashes by pre-crash scenario also helps us understand how different V2V-based safety applications can address different kinds of safety problems.

DOT conducted a preliminary analysis in 2009 of the annual number of crashes that could be addressed by V2V technology.[32] The identified applicable crashes are based on the DOT-[33]developed pre-crash scenario typology as shown in Table III-1, which is in turn primarily based on pre-crash variables recorded in the GES and Crashworthiness Data System.

Table III-1 37 Pre-Crash Scenario Typology

	Crash Scenario		Crash Scenario
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

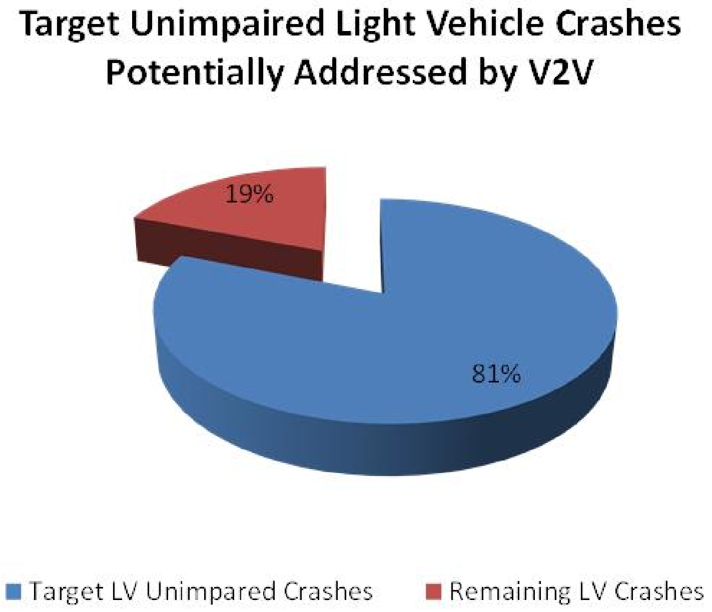
[32] Frequency of Target Crashes for Intellidrive Safety Systems (Najm, Koopman, Smith, and Brewer, October 2010, Report No. DOT HS 811 381). See www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print (last accessed Jan. 30, 2014).

[33] Analysis of Light Vehicle Crashes and Pre-Crash Scenarios Based on the 2000 General Estimates System (Najm, Sen, Smith, and Campbell, Nov. 2002, Report No. DOT HS 809 573). See www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print (last accessed Jan. 9, 2014).

17	Vehicle(s) Parking – Same Direction	37	Other
18	Vehicle(s) Changing Lanes – Same Direction		
19	Vehicle(s) Drifting – Same Direction		
20	Vehicle(s) Making a Maneuver – Opposite Direction		
Vehicle Action refers to a vehicle decelerating, accelerating, starting, passing, parking, turning, backing up, changing lanes, merging, or successful corrective action to a previous critical event.			
Vehicle Maneuver denotes passing, parking, turning, changing lanes, merging, or successful corrective action to a previous critical event.			

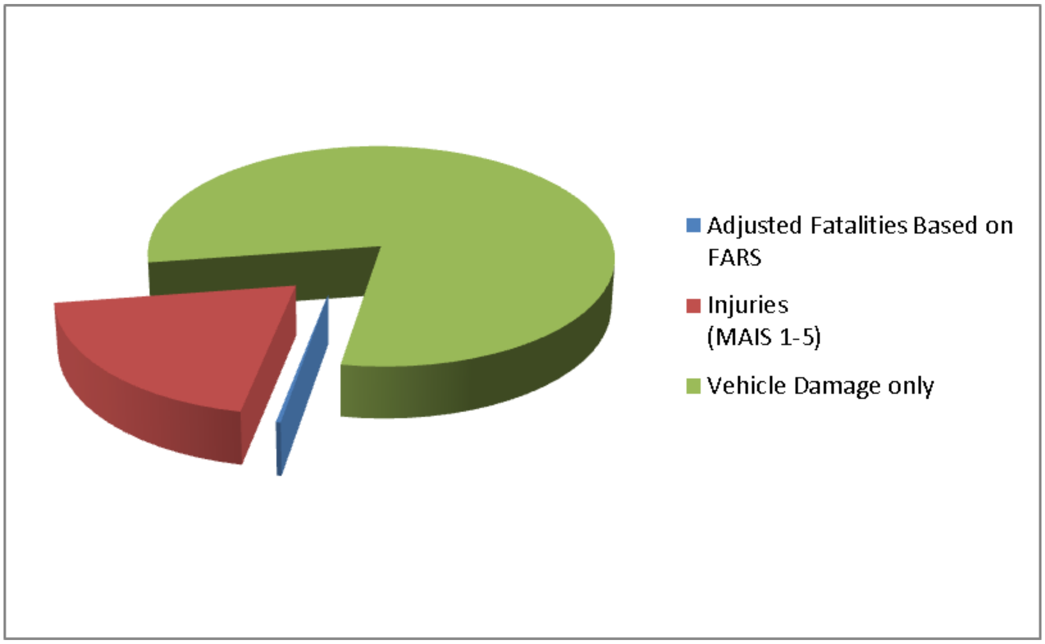
Of these 37 pre-crash scenarios, DOT determined that 15 represented either single vehicle crashes or crashes that would need to be addressed by V2I. That left 22 pre-crash scenarios remaining that could potentially be addressed by V2V technology. The 22 remaining crash scenarios, if the crashes they represent could be prevented, could address 81 percent of unimpaired light vehicle crashes, Figure III-1.

Figure III-1 Target Unimpaired Light Vehicle Crashes Potentially Addressed by V2V



Using 2004-2008 crash data, the approximate average number of fatalities, injuries, and property damage per year caused by these 22 target light-vehicle pre-crash scenarios are 27,000; 1,800,000; and 7,300,000, respectively, as illustrated in Figure III-2 below.

Figure III-2 22 Target Light-Vehicle Pre-Crash Scenario Crash Statistics

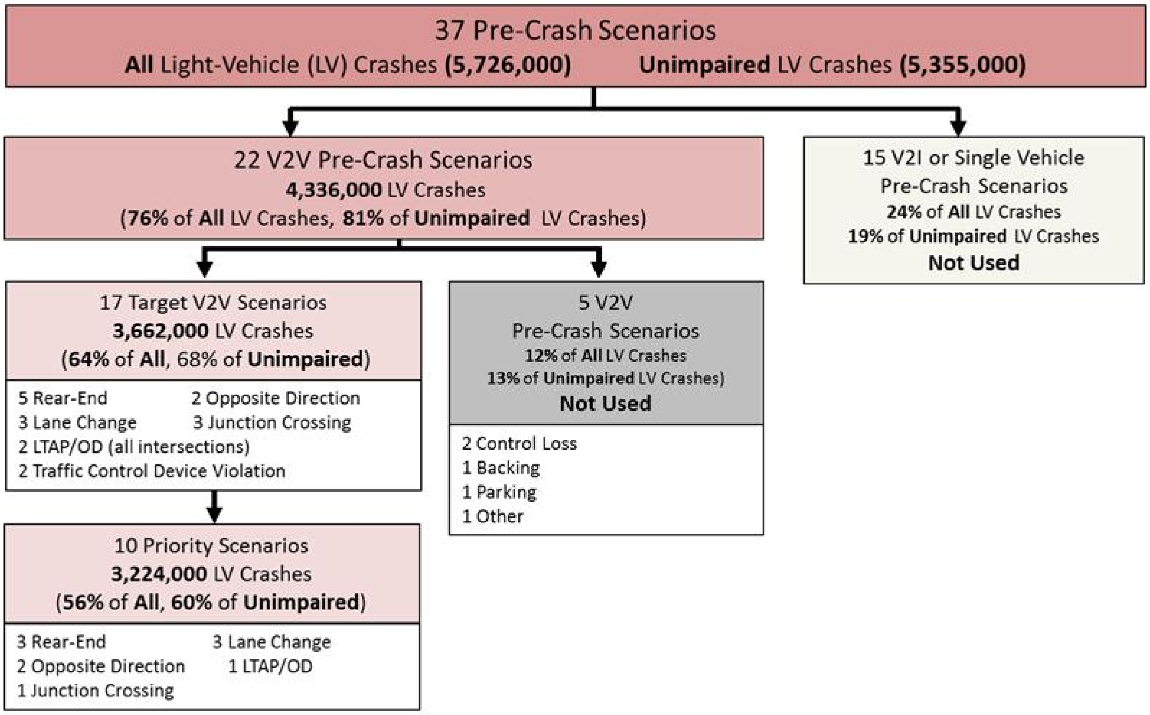


This analysis included the potential crashes that could be addressed by V2V technology only, V2I technology only, and combined. Overall, the DOT analysis concluded that, as a primary countermeasure, a fully mature V2V system could potentially address:

- about 4,409,000 police-reported or 79 percent of <u>all vehicle</u> target crashes,
- 4,336,000 police-reported or 81 percent of all <u>light-vehicle</u> target crashes, and
- 267,000 police-reported or 81 percent of all <u>heavy-truck</u> target crashes annually.

Figure III-3 provides a graphical representation of how the potential crashes that could be addressed by V2V technology only were derived.

Figure III-3 V2V Light-Vehicle Target Crashes Breakdown


37 Pre-Crash Scenarios
All Light-Vehicle (LV) Crashes **(5,726,000)**
Unimpaired LV Crashes **(5,355,000)**
22 V2V Pre-Crash Scenarios
4,336,000 LV Crashes
(**76%** of **All** LV Crashes, **81%** of **Unimpaired** LV Crashes)
15 V2I or Single Vehicle
Pre-Crash Scenarios
24% of **All** LV Crashes
19% of **Unimpaired** LV Crashes
Not Used
17 Target V2V Scenarios
3,662,000 LV Crashes
(**64%** of **All**, 68% of **Unimpaired**)
5 Rear-End
2 Opposite Direction
3 Lane Change
3 Junction Crossing
2 LTAP/OD (all intersections)
2 Traffic Control Device Violation
5 V2V
Pre-Crash Scenarios
12% of **All** LV Crashes
13% of **Unimpaired** LV Crashes)
Not Used
2 Control Loss
1 Backing
1 Parking
1 Other
10 Priority Scenarios
3,224,000 LV Crashes
(**56%** of **All**, **60%** of **Unimpaired**)
3 Rear-End
3 Lane Change
2 Opposite Direction
1 LTAP/OD
1 Junction Crossing

In addition, the analysis also indicated V2I systems could potentially address:

- about 1,465,000 police-reported or 26 percent of all-vehicle target crashes,
- 1,431,000 police-reported or 27 percent of all light-vehicle target crashes, and
- 55,000 police-reported or 15 percent of all heavy-truck target crashes annually.

And, finally, combined V2V and V2I systems could potentially address:

- about 4,503,000 police-reported or 81 percent of all-vehicle target crashes,
- 4,417,000 police-reported or 83 percent of all light-vehicle target crashes, and
- 272,000 police-reported or 79 percent of all heavy-truck target crashes annually.[34]

This preliminary analysis estimated the annual frequency of three different types of target crashes (i.e., light-vehicle, heavy-truck, and all-vehicle crashes) based on data from the General Estimates System (GES) crash database for 2005-2008, where: (1) Light-vehicle crashes are those that involve at least one light vehicle with gross vehicle weight rating (GVWR) of 10,000

[34] Id.

pounds or less; (2) Heavy-truck crashes are those that involve at least one heavy truck, single unit or multiple units, with GVWR over 10,000 pounds; and (3) All-vehicle crashes are those crashes involving both light vehicles and heavy trucks. The number of crashes reported by police for the crash types used in this analysis corresponds to the number of target crashes that might be addressed. The preliminary analysis also excluded drivers with physiological impairments (e.g., intoxication, drowsiness) because such driver conditions could be addressed by autonomous, vehicle-based, countermeasure systems.

This preliminary estimate of annual crash frequency is broader than the benefits estimates used in Section XII below. Those estimates focus only on the usage of two applications (IMA and LTA). These applications are currently viewed as only able to be implemented by V2V technology. The estimates in Section XII, also do not take into account any potential V2I or autonomous applications, given that the agency is evaluating the readiness of V2V and not V2I or autonomous applications.

Once the preliminary analysis of which crashes V2V could potentially address was complete, the agency then focused its research efforts to develop priority scenarios based on the 10 highest comprehensive cost and functional years lost values identified in Table III-2. The fatalities, injuries, and property damage caused by each of the crashes that occurred underlie the Comprehensive Costs and Functional Years Lost.

Table III-2 Societal Cost and Ranking of 22 Target Light-Vehicle Pre-Crash Scenarios

Pre-Crash Scenario	**Light Vehicle V2V Crashes**					
	Comprehensive Cost			Functional Years Lost		
	Total	Percent	Rank	Total	Percent	Rank
Control loss/no vehicle action	$64,744,000,000	23.5%	1	469,000	24.1%	1
SCP @ non-signal	$41,095,000,000	14.9%	2	292,000	15.0%	2
Rear-end/LVS	$29,716,000,000	10.8%	3	198,000	10.2%	4
Opposite direction/no maneuver	$29,558,000,000	10.8%	4	213,000	11.0%	3
Running red light	$18,274,000,000	6.6%	5	129,000	6.6%	5
LTAP/OD @ non-signal	$15,481,000,000	5.6%	6	111,000	5.7%	6
LTAP/OD @ signal	$14,777,000,000	5.4%	7	105,000	5.4%	7
Rear-end/LVD	$12,215,000,000	4.4%	8	82,000	4.2%	8
Rear-end/LVM	$10,342,000,000	3.8%	9	72,000	3.7%	9
Changing lanes/same direction	$8,414,000,000	3.1%	10	60,000	3.1%	10
Control loss/vehicle action	$7,148,000,000	2.6%	11	51,000	2.6%	11
Turning/same direction	$6,176,000,000	2.2%	12	43,000	2.2%	12
Opposite direction/maneuver	$3,500,000,000	1.3%	13	25,000	1.3%	13
Drifting/same direction	$3,483,000,000	1.3%	14	25,000	1.3%	14
Running stop sign	$3,075,000,000	1.1%	15	22,000	1.1%	15
Rear-end/striking maneuver	$2,381,000,000	0.9%	16	16,000	0.8%	16
Parking/same direction	$1,095,000,000	0.4%	17	8,000	0.4%	17

Turn @ non-signal	$930,000,000	0.3%	18	6,000	0.3%	18
Turn right @ signal	$908,000,000	0.3%	19	6,000	0.3%	18
Backing into vehicle	$874,000,000	0.3%	20	6,000	0.3%	18
Rear-end/LVA	$667,000,000	0.2%	21	5,000	0.3%	21
Other	$76,000,000	0.0%	22	-	0.0%	22
All	$274,929,000,000	100.0%		1,944,000	100.0%	

Comprehensive economic costs account for goods and services that must be purchased, or productivity that is lost, as a result of motor vehicle crashes. Comprehensive costs encompass medical, emergency medical service, market productivity, household productivity, insurance administration, workplace productivity, legal and court, travel delay, and property damage costs. In addition, comprehensive costs include the value of a statistical life, the value of quality-adjusted life-years, and pain and suffering.

Functional years lost is a non-monetary measure that sums the years of life lost to fatal injury and the years of functional capacity lost to nonfatal injury. This measure does not mirror the monetary economic cost. It assigns a different value to the relative severity of injuries suffered from motor vehicle crashes. Table III-2 provides the annual values of comprehensive costs and functional years lost for the 22 target pre-crash scenarios involving two or more light vehicles based on 2004-2008 GES crash statistics of injured persons. These cost estimates reflect the injury levels of persons involved in only police-reported crashes.

Based on the target light vehicle crashes that can be addressed by V2V technology, Table III-3 extracts the number of crashes, injuries, and fatalities that form the basis for the development of the Comprehensive Cost and Functional Year Lost measures. Additional information regarding this data is available in Section XII.

Table III-3 Light-Vehicle 2004-2008 GES Averages for V2V Target Pre-Crash Scenarios

Pre-crash Scenario Group	Pre-crash Scenario	Total No. Of crashes	MAIS Injury Code							Adj. Fatalities Based on FARS
			0 None	1 Minor	2 Moderate	3 Serious	4 Severe	5 Critical	6 Fatal	
Rear End	LVS	942,000	204,027	299,750	33,389	8,815	1,761	562	811	1,080
	LVD	398,000	77,805	115,948	13,082	3,542	720	230	397	528
	LVM	202,000	42,752	66,363	7,866	2,288	480	163	701	933
	Striking Maneuver	83,000	11,948	19,420	2,242	626	128	44	111	147
	LVA	21,000	4,465	6,320	750	223	47	16	14	19
Lane Change	Same Direction	336,000	34,501	53,356	6,677	2,118	464	163	504	672
	Turn - Same Direction	202,000	28,491	39,850	4,893	1,511	325	116	379	504
	Drift - Same Lane	105,000	12,530	18,208	2,260	706	155	51	222	295
Opposite Direction	Maneuver	11,000	2,519	6,433	1,036	435	106	41	417	556
	No Maneuver	118,000	25,589	58,025	9,035	3,660	875	344	3,501	4,663
LTAP/OD	@ Non Signal	184,000	50,160	89,482	11,644	3,830	853	296	970	1,293
	@ Signal	204,000	62,164	108,673	13,940	4,450	975	334	605	805
Junction Crossing	SCP@ Non Signal	647,000	149,611	245,533	31,290	10,045	2,214	762	2,641	3,517
	Turn Right @ Signal	31,000	3,474	5,388	603	153	29	9	77	103
	Turn @ Non Signal	45,000	5,408	7,811	925	263	54	18	38	50
	Total	3,529,000	715,444	1,140,560	139,632	42,665	9,186	3,149	11,388	15,165
Total All Light Vehicle Crashes		5,764,645	995,019	1,712,336	220,355	71,756	15,883	5,591	25,885	
% of Total Light Vehicle Crashes		61	72	67	63	59	58	56	44	

From the 10 pre-crash scenarios prioritized by the agency, CAMP identified five initial, prototype V2V safety applications that could address these scenarios. It was found that these prototype applications could also address seven other pre-crash scenarios that were included in the overall list of 22 addressable by V2V, as shown in Table III-4 (Note: acronyms used in tables are explained in the list of acronyms at the front of this report). This includes the V2I safety application Traffic Control Device Violation pre-crash scenarios that can be addressed by the V2V Intersection Movement Assist safety application.

Table III-4 Groups of Target Light-Vehicle V2V Pre-Crash Scenarios and Associated Societal Cost

		Light Vehicles V2V Crashes					
Pre-Crash Scenario/Safety Application		**Comprehensive Cost**			**Functional Years Lost**		
		Total	**Percent**	**Rank**	**Total**	**Percent**	**Rank**
Rear End/Forward Collision Warning	Rear-end/LVS	$ 29,716,000,000	10.8%	3	198,000	10.2%	4
	Rear-end/LVD	$ 12,215,000,000	4.4%	8	82,000	4.2%	8
	Rear-end/LVM	$ 10,342,000,000	3.8%	9	72,000	3.7%	9
	Rear-end/striking maneuver	$ 2,381,000,000	0.9%	16	16,000	0.8%	16
	Rear-end/LVA	$ 667,000,000	0.2%	21	5,000	0.3%	21
	Total	**$ 55,321,000,000**	**20.1%**		**373,000**	**19.2%**	
Lane Change/Blind Spot- Lane Change Warning	Changing lanes/same direction	$ 8,414,000,000	3.1%	10	60,000	3.1%	10
	Turning/same direction	$ 6,176,000,000	2.2%	12	43,000	2.2%	12
	Drifting/same direction	$ 3,483,000,000	1.3%	14	25,000	1.3%	13
	Total	**$ 18,073,000,000**	**6.6%**		**128,000**	**6.6%**	
Opposite Direction/Do Not Pass Warning	Opposite direction/no maneuver	$ 29,558,000,000	10.8%	4	213,000	11.0%	3
	Opposite direction/maneuver	$ 3,500,000,000	1.3%	13	25,000	1.3%	13
	Total	**$ 33,058,000,000**	**12.0%**		**238,000**	**12.2%**	
LTAP/OD/ Left Turn Assist Warning	LTAP/OD @ non signal	$ 15,481,000,000	5.6%	6	111,000	5.7%	6
	LTAP/OD @ signal	$ 14,777,000,000	5.4%	7	105,000	5.4%	7
	Total	**$ 30,258,000,000**	**11.0%**		**216,000**	**11.1%**	
Junction Crossing/Intersection Movement Assist	SCP @ non signal	$ 41,095,000,000	14.9%	2	292,000	15.0%	2
	Turn @ non signal	$ 930,000,000	0.3%	18	6,000	0.3%	18
	Turn right @ signal	$ 908,000,000	0.3%	19	6,000	0.3%	18
	Total	**$ 42,933,000,000**	**15.6%**		**304,000**	**15.6%**	
Traffic Control Device Violation	Running red light	$ 18,274,000,000	6.6%	5	129,000	6.6%	5
	Running stop sign	$ 3,075,000,000	1.1%	15	22,000	1.1%	15
	Total	**$ 21,349,000,000**	**7.8%**		**151,000**	**7.8%**	

The Safety Applications identified in Table III-4, except for the V2I safety application Traffic Control Device Violation, are represented by prototype applications in the Safety Pilot Model Deployment. These prototypes were developed by a consortium of OEMs working collaboratively in a pre-competitive environment. Data has been collected that provides information about the functional nature of these safety applications being used by regular drivers under real driving conditions. Analysis of the first 6 months of data identified the safety applications that most drivers experienced and for which the most data was collected. These safety applications were Forward Collision Warning, Intersection Movement Assist, Left Turn Assist, and Blind Spot Warning/Lane Change Warning. The amount of preliminary data collected on these four safety applications provided the information needed to estimate possible effectiveness and benefits these safety application may generate.

B. Potential for V2V to address vehicle crashes

The discussion up to this point has focused on determining the universe of crashes that V2V could address, and how a research program was developed and executed to prototype safety applications to address those crashes. The data collected during the Safety Pilot Model Deployment provide an indication of functional feasibility, along with information to evaluate the system – in effect, *whether* the prototypes and the system worked, but not necessarily *how well* they worked. Based on the information available to the agency at this time, Section XI starts to take the next step to analyze potential effectiveness and benefits that may accrue if these systems are implemented in the real world at production volumes.

In mass deployment, though, the agency would not expect benefits to accrue immediately. When V2V technology first begins to enter the fleet, it is possible (perhaps even likely) that vehicles equipped with the technology will encounter relatively few other vehicles also equipped with the technology – i.e., that V2V devices may not be able to "find" each other for a while. Even if the market drives faster uptake by consumers of aftermarket devices (if, for example, auto insurance companies offer discounts for installing the devices), which would increase the ability of V2V devices to find each other earlier on, it will still take 37 years before we would expect the technology to fully penetrate the fleet. As a result, full knowledge of how different aspects of the V2V system perform – the ability of the security system to manage certification revocation lists for the complete U.S. vehicle fleet, for example – may be delayed.

However, as explained in Section XII, benefits would begin to appear in the first year. On the other hand, costs for the security system would be lower during initial deployment because there would be fewer vehicles requiring certificates. Over the 37 years, costs would increase in parallel with increased fleet penetration. Section XI discusses this issue of gradual roll-out of V2V technology and its implications in more detail.

While a safety application as initially developed by an OEM or supplier may only address a subset of the pre-crash scenarios in the group, over time the safety application may be updated to include the other pre-crash scenarios as the technology and knowledge evolves.

Another factor affecting costs and benefits would be what combination of safety applications are deployed in various vehicles. V2V devices in various vehicles may not be able to support all the safety applications.[35] Depending on the type of device, different data elements may or may not be available, which may limit what safety applications can be supported. For example, a device that does not connect to a vehicle data bus may support forward collision warning, but without turn signal information, it may not support/implement left turn assist warning.

The agency notes that crashes that can be prevented and lives that can be saved depends on the effectiveness of the safety applications. This report evaluates effectiveness estimates for two potential applications, IMA and LTA, but not for other potential safety applications such as LCW, FCW, CSW, etc.

As such, the overall potential of V2V and the number of crashes prevented and lives saved is highly dependent on the number of safety applications deployed, the penetration of those applications in the fleet and the way in which the applications operate. For additional information on potential crashes prevented and lives saved using the IMA and LTA applications please refer to Section XII.

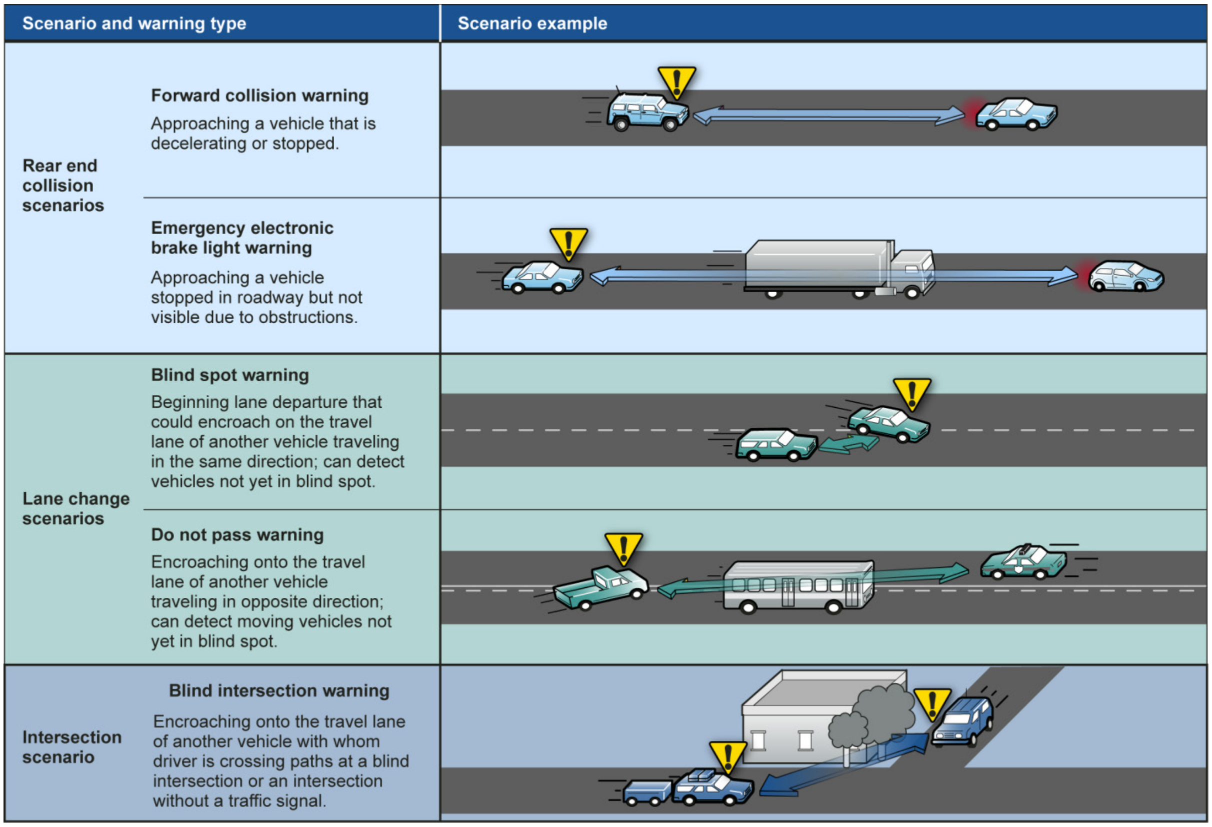
C. Ways of addressing the safety need

1. Scenarios addressed uniquely by vehicle-to-vehicle communications

V2V technology communicates via radio signals, which are omnidirectional (i.e., offer 360 degrees of coverage). Communicating via these signals allows two equipped vehicles to "see" each other at times when other vehicles that are only relying on their sensors are not able to detect the presence of another vehicle, let alone determine the other vehicle's heading, speed, or its operational status. Figure III-4 depicts examples of safety applications and the scenarios they can address.

[35] Description of Light-Vehicle Pre-Crash Scenarios for Safety Applications Based on Vehicle-to-Vehicle Communications (Report No. DOT HS 811 731, May 2013). See www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 27, 2014)

Figure III-4 Examples of Crash Scenarios and Vehicle-to-Vehicle Applications



Scenario and warning type		Scenario example
Rear end collision scenarios	**Forward collision warning** Approaching a vehicle that is decelerating or stopped.	
	Emergency electronic brake light warning Approaching a vehicle stopped in roadway but not visible due to obstructions.	
Lane change scenarios	**Blind spot warning** Beginning lane departure that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles not yet in blind spot.	
	Do not pass warning Encroaching onto the travel lane of another vehicle traveling in opposite direction; can detect moving vehicles not yet in blind spot.	
Intersection scenario	**Blind intersection warning** Encroaching onto the travel lane of another vehicle with whom driver is crossing paths at a blind intersection or an intersection without a traffic signal.	

Source: GAO analysis of Crash Avoidance Metrics Partnership information.

NOTE: Sensor-based crash avoidance technologies can, in some instances, provide warnings in forward collision, blind spot, and do not pass scenarios

V2V communications also offer an operational range of up to 300 meters between vehicles to facilitate identification of intersecting paths that may potentially result in a crash if no driver or vehicle action is taken. Additionally, a V2V system is not subject to the same weather, light, or cleanliness constraints associated with vehicle-resident sensors (e.g., cameras, lidar), although it is subject to other issues (e.g., urban canyons, GPS signal).[36]

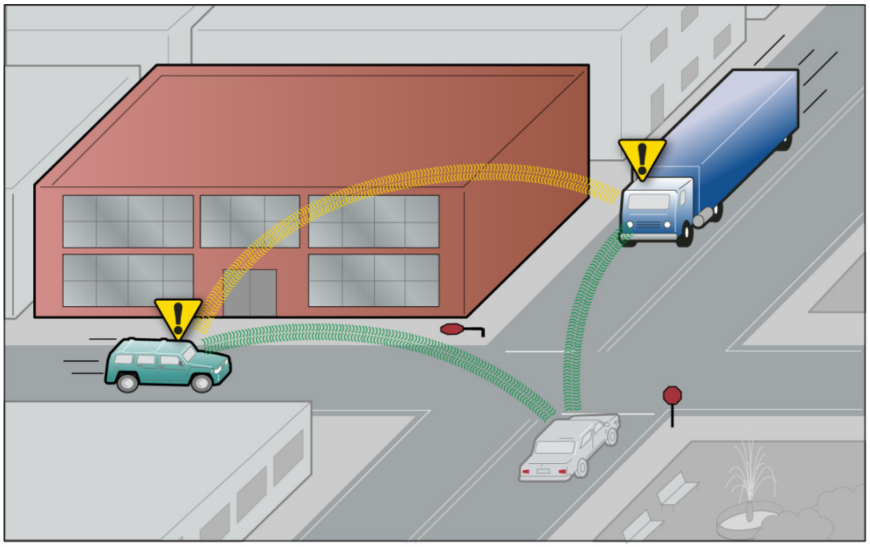
There are three V2V safety applications that the agency believes are enabled by V2V alone and could not be replicated by any current, known vehicle-resident sensor- or camera-based systems, as discussed below.

[36] A lidar device detects distant objects and determines the ir position, velocity, or other characteristics by analysis of pulsed laser light reflected from the ir surfaces. Lidar operates on the same principles as radar and sonar.

a) Intersection Movement Assist

IMA warns the driver of a vehicle when it is not safe to enter an intersection due to a high probability of colliding with one or more vehicles at intersections both where a signal is present (a "controlled" intersection) and those where only a stop or yield-sign is present (an "uncontrolled" intersection). Figure III-5 illustrates one possible IMA scenario.

Figure III-5 Example of V2V Intersection Movement Assist Warning Scenario



Source: GAO.

Note: In this scenario, the truck and sports utility vehicle are at risk of colliding because the drivers are unable to see one another approaching the intersection and the stop sign is disabled. Both drivers would receive warnings of a potential collision, allowing them to take actions to avoid it.

b) Left Turn Assist

LTA warns the driver of a vehicle, when they are entering an intersection, not to turn left in front of another vehicle traveling in the opposite direction.

c) Emergency Electronic Brake Light

Emergency Electronic Brake Light enables a vehicle to warn its driver to brake in a situation where another V2V-equipped vehicle decelerates quickly but may not be directly in front of the warning vehicle. The EEBL warning is particularly useful when the driver's line of sight is obstructed by other vehicles or bad weather conditions, such as fog or heavy rain.

2. Scenarios also addressed by vehicle sensor-based systems

Two of the applications being evaluated by the agency are already available in production vehicles using vehicle-resident sensors: FCW and BSW. These applications have been available in a small number of production vehicles for many years. They could be considered mature technologies, insofar as they have undergone multiple generations of sensor technologies and variations of sensing technology to achieve their implementation.

V2V technology, however, could enable these applications independent of any vehicle-resident sensors (e.g., cameras or lidar). At the same time, V2V could provide additional detection range for these applications, and/or detection agnostic to the weather, light or cleanliness constraints associated with vehicle-resident sensors such as cameras or lidar.

a) Forward Collision Warning

FCW warns the driver of the host vehicle in case of an impending rear-end collision with a remote vehicle ahead in traffic in the same lane and direction of travel.

The agency believes, based on current technology, that FCW systems using radar or cameras cannot provide a warning fast enough for very high speed rear end crashes. V2V, in contrast, has that capability based on its longer range (300 meters). Thus, fatal rear end crashes are one area where we believe V2V can provide some benefits not potentially covered by radar- and camera-based systems.

Radar and camera FCW systems also have a problem detecting stopped vehicles if the vehicle is stopped before coming into range of the radar and camera. Recently, dual radar and dual camera systems have been developed to provide detection of stopped vehicles. A V2V system could act as the redundant system and allow a single radar or single camera FCW system to detect stopped vehicles, thus reducing system cost as compared to dual radar or dual camera.

b) Blind Spot Warning + Lane Change Warning

Blind Spot Warning +Lane Change Warning warns the driver of the host vehicle during a lane change attempt if the blind spot zone into which the host vehicle intends to switch is, or will soon be, occupied by another vehicle traveling in the same direction. The application also provides the driver of the host vehicle with advisory information that a vehicle in an adjacent lane is positioned in a vehicle's "blind spot" zone when a lane change is not being attempted.

3. Scenarios possibly addressed by a combination of vehicle resident sensors and V2V communications

Other sensors such as radar, lidar, and cameras enable certain safety applications that are viewed by some as alternatives to V2V. While these systems might be more mature than V2V, they also have drawbacks when used alone; a combined or fused system using any of these other sensors along with V2V will take advantage of the benefits of DSRC. For example, detection of threat vehicles not in the sensors' field of view, and using a DSRC signal to validate a return from a vehicle-based sensor (i.e., a radar return off metal objects in the roadway, absent a DSRC signal identifying the sender as a vehicle, may be mistaken for a vehicle and cause a false warning).

A fused system would be able to use multiple sensors to augment accuracy, and could lead to improved warning timing and a reduction in the number of false positives. As stated in the agency policy statement on automated vehicles,[37] V2V technology could potentially also act as an additional sensor input that could augment data available.

D. Types of V2V devices

1. OEM devices

An OEM device is an electronic device built or integrated into a vehicle during vehicle production. An integrated V2V system is connected to proprietary data busses and can provide highly accurate information using in-vehicle information to generate the Basic Safety Message. The integrated system both broadcasts and receives BSMs. In addition, it can process the content of received messages to provide advisories and/or warnings to the driver of the vehicle in which it is installed. Because the device is fully integrated into the vehicle at the time of manufacture, vehicles with Integrated Safety Systems could potentially provide haptic warnings to alert the driver (such as tightening the seat belt or vibrating the driver's seat) in addition to audio and visual warnings provided by the aftermarket safety devices. It is expected that the equipment required for an integrated OEM V2V system would consist of a general purpose processor and associated memory, a radio transmitter and transceiver, antennas, interfaces to the vehicle's sensors, and a GPS receiver. Such integrated systems are capable of being reasonably combined with other vehicle-resident crash avoidance systems to exploit the functionality of both types of systems.

2. Aftermarket devices

a) Definition of an "aftermarket" device

Generally speaking, automotive aftermarket devices can be defined as any product with one or more functions in the areas of comfort, convenience, performance, or safety, which are added to a motor vehicle after its original assembly. An aftermarket V2V communication device provides advisories and warnings to the driver of a vehicle similar to those provided by an OEM-installed V2V device. These devices, however, may not be as fully integrated into the vehicle as an OEM device, and the level of connection to the vehicle can vary based on the type of aftermarket device itself. For example, a "self-contained" V2V aftermarket safety device could only connect to a power source, and otherwise would operate independently from the systems in the vehicle. Aftermarket V2V devices can be added to a vehicle at a vehicle dealership, as well as by authorized dealers or installers of automotive equipment. Some aftermarket V2V devices (e.g., cell phones with apps) are portable and can be standalone units carried by the operator, the passenger, or pedestrians.

[37] See www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf (last accessed Feb. 20, 2014).

b) Types of aftermarket devices used in Safety Pilot Model Deployment

In the Safety Pilot Model Deployment, three types of aftermarket devices were installed into vehicles: vehicle awareness devices, aftermarket safety devices, and retrofit safety devices.

The VAD is the simplest design, and it only transmits a BSM to nearby vehicles. A VAD does not have any safety applications or DVIs, and it cannot provide any advisories or warnings to a driver. Installing these devices on existing vehicles could be an attractive option for fleet operators, rental agencies, or vehicle owners who could see benefit in signaling the presence of their vehicles to V2V-equipped vehicles and thus potentially avoiding crashes. Installation of VADs could increase deployment of V2V systems across the fleet as a whole, and thus potentially could increase the benefits for early adopters of this technology.

The ASD (referred to as a "self-contained" device in this research report in contrast to the terminology used in the Safety Pilot Model Deployment), is similar to the VAD, but also has the ability to both receive and transmit a BSM to nearby vehicles. Also, it contains safety applications that can provide advisories or warnings to the driver. Three suppliers developed and tested self-contained devices for use with light vehicles in the Safety Pilot Model Deployment. All suppliers developed and tested the following safety applications:

- FCW
- EEBL
- CSW[38]

The safety applications and warning functionality in both the ASDs and the V2V vehicles were similar, but the three self-contained device suppliers implemented only audible warnings for their devices, with no visual or haptic advisories or warnings presented to the driver. The agency originally specified a visual display for these devices, but the display selected by the suppliers did not meet the distraction guidelines for the Safety Pilot Model Deployment and was, therefore, not implemented as part of that testing.

The RSD is more fully integrated than the ASD: it connects to the vehicle and receives information from the vehicle's data bus to support operation of various applications on the device. Although it is possible from a technical standpoint, light vehicles were not equipped with a RSD device in the Safety Pilot Modal Deployment, even though RSDs were deployed in heavy vehicles. The heavy truck RSDs demonstrated the following safety applications:

[38] Some self-contained devices also had IMA capabilities and were track tested outside of the Safety Pilot Model Deployment, but did not meet performance requirements for purposes of inclusion in Model Deployment.

- FCW
- EEBL
- CSW
- BSW
- IMA
- Bridge Height Information

The advantage to RSDs, as compared to the other types of aftermarket devices, is that they can potentially perform different or enhanced safety applications or execute more sophisticated applications because they can access a richer set of data (i.e., data from the data bus). For example, having information on the turn signal status from the vehicle provides the device and application an indication of possible driver intent to make a turn, which can help inform the LTA, DNPW, and BSW/LCW safety applications. Therefore, the RSD is considered to be the closest of all of the aftermarket devices to a V2V device integrated into a new vehicle. Table III-5 provides details on the three types of aftermarket safety devices employed in the Safety Pilot Model Deployment. The agency envisions these general types as models for potential commercial aftermarket devices that could be available to consumers.

Table III-5 Aftermarket Safety Device Types

Device Type	Definition	Method of Installation	Functionality
Vehicle Awareness Device	Device is able to be connected to the vehicle for power source. Device provides Basic Safety Message for surrounding vehicles.	Device would need to be installed by a certified installer on vehicles not equipped with V2V technology to ensure correct antenna placement and security. In the future, VADs might be mobile devices or stand-alone key fobs.	• Transmits BSM
Aftermarket Safety Devices (i.e., Self-contained)	Device is connected to the vehicle for power source, Device transmits BSM and receives BSMs to support safety applications for the driver of the vehicle in which it is installed.	This device only receives power from the vehicle; however, a certified installer would need to ensure correct antenna placement and security.	• V2V Safety applications • Receives and Transmits BSM • Driver-Vehicle Interface
Retrofit Safety Devices	Device is connected to the vehicle's data bus that provides BSM and safety applications for the driver of the vehicle in which it is installed.	This device needs to be connected to the vehicle's data bus, therefore would require an installer that can access this for the particular make of vehicle. Also, a certified installer would need to ensure correct antenna placement and security.	• V2V Safety applications • Receives and Transmits BSM • Driver Vehicle Interface • Integration into the vehicle data bus

3. Infrastructure-based devices

a) Infrastructure based devices that enable V2I

In addition to in-vehicle equipment, the Safety Pilot program is evaluating road side equipment with DSRC devices that allow vehicles to receive information from the infrastructure and allow vehicles to update their security certificates.[39]

This RSE can be co-located with infrastructure elements such as road signs, traffic signals, etc. The applications that the RSE is supporting in the Safety Pilot Model Deployment are signal phasing and timing (SPaT), and curve and curve speed warnings. There are twenty-six DSRC-equipped roadside units being used to support the program.

V2I communications involve the wireless exchange of critical safety and operational data between vehicles (including brought-in devices) and roadway infrastructure. V2I communications are intended primarily to avoid motor vehicle crashes while enabling a wide range of mobility and environmental benefits. The Connected Vehicle program is funding V2V and V2I communications research within the Dynamic Mobility Applications, Road Weather, AERIS, and V2I Safety programs.

b) What potential safety applications are enabled by V2I?

V2I applications complement the V2V safety applications by addressing crash scenarios that V2V applications cannot address and by more efficiently addressing some crash scenarios when there are low levels of penetration of DSRC-equipped light vehicles. The following is a list of contemplated, but not yet developed, V2I safety applications:

- Red Light Violation Warning: This technology will provide in-vehicle alerts to drivers about potential violations of upcoming red lights, based on vehicle speeds and distances to intersections.
- Curve Speed Warning: If a driver's current speed is unsafe for traveling through an upcoming road curve, this technology will alert the motorist to slow down.
- Stop Sign Gap Assist: This technology will assist drivers at STOP-sign-controlled intersections via vehicle gap detections, alerting motorists when it is unsafe to enter intersections.
- Reduced Speed Zone Warning: This technology will assist drivers in work zones, by issuing alerts to drivers to reduce speed, change lanes, and/or prepare to stop.
- Spot Weather Information Warning: This technology will provide in-vehicle alerts or warning to drivers about real-time weather events and locations, based upon information

[39] During the second phase of Safety Pilot, DSRC and cellular were used to provide vehicles with updated security certificates.

from Roadside Equipment connections with Transportation Management Center and other weather data collection sites/services.

- Stop Sign Violation Warning: Based on vehicle speeds and distances to intersections, this technology will provide in-vehicle alerts to drivers about potential violations of upcoming stop signs.
- Railroad Crossing Violation Warning: This technology will assist drivers at controlled railroad crossings via RSE connections with existing train detection equipment, alerting motorists when it is unsafe to cross the railroad tracks.
- Oversize Vehicle Warning: Drivers of oversized vehicles will receive an in-vehicle alert to take an alternate route or a warning to stop, based upon information from RSE connections to infrastructure at bridges/tunnels.

Implementation of these V2I applications would require additional data elements to be broadcast to, and processed by, vehicles. Since the broadcasting of additional data has the potential of leading to communication congestion, DOT's ITS JPO will conduct additional channel congestion analysis. It is critical that safety messaging should not be compromised due to broadcasting more data for V2I.

IV. Scope and Legal Authority

A. NHTSA's scope and legal authority and how it applies to vehicle to vehicle communication

The National Traffic and Motor Vehicle Safety Act (the "Safety Act") gives NHTSA broad statutory authority to regulate motor vehicles and items of motor vehicle equipment.[40] As applied in this context, the agency's authority includes all or nearly all aspects of a V2V system. Congress enacted the Safety Act in 1966 with the purpose of reducing deaths and injuries as a result of motor vehicle crashes and non-operational safety hazards attributable to motor vehicles.[41] The Safety Act, as amended, is now codified at 49 U.S.C. §§ 30101 et seq.

[40] For more discussion and analysis of NHTSA's authority to regulate advanced crash avoidance technologies, including V2V technologies, under the Safety Act, see the Potential Regulatory Challenges of Increasingly Autonomous Vehicles, 52 Santa Clara L. Rev. 1423 (Wood *et al*., 2012) at http://digitalcommons.law.scu.edu/lawreview/vol52/iss4/9/ (last accessed Mar. 4, 2014).
For example, the agency's authority to address the privacy and security of vehicle data associated with the operation of those technologies is discussed at length. Id., at pp. 1448, 1465-72. Addressing data security is necessary to safeguard the effectiveness of these technologies and promote the ir acceptance by vehicle users. Addressing privacy is similarly necessary to promote public acceptance. The views expressed in that article fairly encompass the agency's views of its regulatory authority.

[41] H.R. Rep. No. 89-1776, at 10 (1966).

The vehicle technologies that enable vehicles to talk to each other and to communicate with infrastructure are vastly different from those that existed when the Safety Act was enacted. Then, the vehicle operating systems were largely mechanical and controlled by the driver via mechanical inputs and linkages. Components and systems were either designed into the vehicle at the time of original manufacture or were later attached to or physically carried into the vehicle. Sensing of a vehicle's performance and the roadway environment was done solely by the driver. Today, an increasing number of vehicle functions are electronic. These functions can be activated and controlled automatically and do not necessarily require driver involvement, unlike the mechanical functions of previous generations of vehicles. As discussed in much more detail in Section V.D below, V2V technologies rely on dedicated short-range radio communications (DSRC), which themselves require no driver involvement whatsoever in order to send and receive information that can be used for vehicle safety functions. Other ways in which V2V technologies differ from the mechanical technologies prevalent when the Safety Act was first enacted include the fact that how they operate can be substantially altered by post-manufacture software updates, and that advances in communications technology make it possible for nomadic devices with vehicle-related applications to be brought into the vehicle.

The language of the Safety Act, however, is broad enough to comfortably accommodate this evolution in vehicle technologies. NHTSA's statutory authority over motor vehicles and motor vehicle equipment would allow the agency to establish safety standards applicable both to vehicles that are originally manufactured with V2V communications technologies and to aftermarket equipment that could be added to vehicles that were not originally manufactured as V2V-capable (i.e., to convert them into vehicles with various degrees of V2V-capability).

In the Safety Act, which gives NHTSA authority over new motor vehicles and motor vehicle equipment, "motor vehicle" is defined as a "vehicle driven or drawn by mechanical power and manufactured primarily for use" on public roads.[42] The definition of "motor vehicle equipment," as cited below, is broader and thus effectively establishes the limit of the agency's authority under the Safety Act:

> (A) any system, part, or component of a motor vehicle as originally manufactured;
> (B) any similar part or component manufactured or sold for replacement or improvement of a system, part, or component, or as an accessory or addition to a motor vehicle; or
> (C) any device or an article or apparel, including a motorcycle helmet and excluding medicine or eyeglasses prescribed by a licensed practitioner, that –
> i) is not a system, part, or component of a motor vehicle; and

[42] 49 U.S.C. § 30102(a)(6).

ii) is manufactured, sold, delivered, or offered to be sold for use on public streets, roads, and highways with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death.[43]

NHTSA's authority to issue safety standards that apply to new motor vehicles would enable the agency to establish standards applicable to vehicles that were originally manufactured with V2V capabilities.[44] This authority would also extend to the individual pieces of equipment that are installed in new vehicles to provide them with V2V capabilities.[45] Using the agency's authority over equipment, as described in (B) and (C) above, NHTSA could also establish safety standards that apply to equipment used to equip vehicles (not originally manufactured with V2V capabilities) with V2V capabilities.[46]

NHTSA's authority over these groups of items – (1) systems, parts, and components installed or included in a vehicle, (2) replacements and improvements to those systems, parts, and components, (3) accessories and additions to motor vehicles, and (4) devices or articles with an apparent safety-related purpose – is very broad. The status of these items as motor vehicle equipment does not depend on the type of technology or its mode of control (mechanical or electronic) or whether an item is tangible or intangible. The transition from mechanical to electromechanical systems has thus had no significant effect on the extent of NHTSA's authority over motor vehicle performance. NHTSA continues to have regulatory authority under the Safety Act over all the systems, parts, and components installed on new motor vehicles, even as motor vehicle control systems become increasingly electronic, and perhaps increasingly automated, in the future.

[43] § 30102(a)(7)(C); MAP-21, Pub. L. 112-141, § 31201, 126 Stat. 405. See www.gpo.gov/fdsys/pkg/PLAW-112publ141/pdf/PLAW-112publ141.pdf (last accessed Jan. 27, 2014). Congress added subparagraph (C) to the statutory definition of "motor vehicle equipment" in 1970 when it amended the definition in order to clarify the Department's authority over additional objects such as motorcycle helmets. See S. Rep. No. 91-559, at 5 (1970). However, Congress did not seek to limit the extension of the Department's authority only to motorcycle helmets and instead utilized the broad terms "device, article, and apparel" to describe the universe of objects that are within the agency's authority. *See id*. Acknowledging the concerns of those who authored the House version of the amendatory language that utilizing the terms "device, article, and apparel" might unduly extend the Department's authority to objects that have only a tangential relation to motor vehicle safety, the conference committee added a use restriction. *See id*. Congress relaxed this use restriction in the statutory definition of "motor vehicle equipment" as part of the amendments to the Safety Act in MAP-21. *See* MAP-21, Pub. L. 112-141, § 31201, 126 Stat. 405. Thus, the Department's regulatory authority under subparagraph (C) is limited to those devices, articles, or apparel that are used for "*the apparent purpose* of safeguarding users of motor vehicles against risk of accident, injury, or death." See id. (Emphasis added.)

[44] 49 U.S.C. §§ 30102(a)(6), 30111.

[45] 49 U.S.C. § 30102(a)(7)(A).

[46] 49 U.S.C. § 30102(a)(7)(B).

Put in the context of V2V-related motor vehicle equipment, NHTSA considers the following items subject to the agency's regulatory authority:

(1) Any integrated original equipment (OE) used for V2V communications or safety applications reliant on V2V communications
(2) Any integrated aftermarket equipment used for V2V communications or safety applications reliant on V2V communications[47]
(3) Some non-integrated aftermarket equipment, depending on its nature and apparent purpose[48]
(4) Software that provides or aids V2V functions, and software updates to all of this equipment[49]
(5) Some roadside infrastructure (V2I), to the extent it relates to safety[50]

We describe the agency's specific authority over these V2V-related items of motor vehicle equipment in more detail below.

1. Integrated OEM V2V technologies

Integrated OE V2V technologies, in this case, refer to all items of equipment that function as part of a V2V system and are built into the vehicle when it is produced for sale. As explained above, 49 U.S.C. § 30102(a)(7)(A) defines "motor vehicle equipment," in relevant part, as including all systems, parts, and components that are installed in or accompany a motor vehicle as it is originally manufactured. Again, "system, part, or component" is broad language that encompasses a large universe of items that can be considered motor vehicle equipment.[51]

[47] § 30102(a)(7)(B), if the equipment "improves" an already-existing function of the vehicle or is an "addition" to the vehicle.

[48] § 30102(a)(7)(B), if we interpret the equipment as constituting a motor vehicle "accessory" (something to be used while the vehicle is in operation, that enhances that operation), or § 30102(a)(7)(C), if we interpret the equipment as constituting a device used for the apparent purpose of traffic safety (purpose would be clearly observable from the characteristics of the object and the context of its use, rather than necessarily defined by the manufacturer's intent for the equipment).

[49] § 30102(a)(7)(B), because updates can be replacements, improvements.

[50] § 30102(a)(7)(B) and (C), if its apparent purpose is safety, it may be an "accessory" or a "device…manufactured…with the apparent purpose of safeguarding users of motor vehicles against accident, injury, or death." We note that there will certainly be roadside infrastructure that would not fall within this category. A stop sign, for example, may be provided by a municipality for safety reasons, and it may even be manufactured with the apparent purpose of safeguarding users of motor vehicles against accident, injury, or death, but NHTSA would not consider the stop sign to be motor vehicle equipment.

[51] As last accessed in Merriam Webster on Mar. 4, 2014: (1) A system is "a regularly interacting or interdependent group of items forming a unified whole . . . : a group of devices or artificial objects or an organization forming a network especially for distributing something or serving a common purpose." See www.merriam-webster.com/dictionary/system ; (2) A part is "one of the often indefinite or unequal subdivisions into which

The agency has already given some consideration to the application of subparagraph (A) of the definition of "motor vehicle equipment" to technologies that include both mechanical and electromechanical/tangible and intangible aspects. A recent example of such a technology that the agency has considered to be an item of motor vehicle equipment is the OnStar in-vehicle communications system.[52] OnStar is available on many new General Motors vehicles, and is also offered as an aftermarket option for certain other vehicles.[53] As an item that is built into the vehicle in a way that cannot easily be un-integrated, for the purposes of providing various functions such as emergency notification and turn-by-turn navigation, OnStar is considered by the agency to be a system, part, or component installed in motor vehicles as originally manufactured, when present on the vehicle prior to initial sale. Similarly, DSRC and other equipment that allow V2V-based safety applications to function would be considered "motor vehicle equipment" by virtue of these items being installed in a new motor vehicle at the time of manufacture, in the same manner as OnStar.

2. Integrated aftermarket equipment

The broad definition of "motor vehicle equipment" also covers equipment and devices purchased by motor vehicle users in the aftermarket, i.e., after the vehicle's initial sale.[54] The agency's jurisdiction over aftermarket equipment is important in regard to V2V-related technologies because consumers may be interested in obtaining equipment for their used vehicles to give them V2V capabilities and help them be seen by other vehicles on the roads. Further, any aftermarket software updates to V2V-related systems or software enabling other devices to connect to the V2V system would be considered "motor vehicle equipment" under this part of the definition, as discussed further below.

The statutory language in 49 U.S.C. § 30102(a)(7)(B) separates the items covered by this part of the definition into two groups: (1) those that are a "replacement or improvement," and (2) those that are an "accessory or addition." We note that even though these groups are different from the criteria that govern NHTSA's regulation of original motor vehicle equipment in § 30102(a)(7)(A), both statutory provisions essentially refer to "systems, parts, or components" – we interpret the additional terms in § 30102(a)(7)(B) simply as describing *when* the equipment becomes part of the vehicle (at some point after first sale, rather than prior to first sale). As all parts of a vehicle can need replacement, it does not seem accurate to consider the

something is or is regarded as divided and which together constitute the whole." See www.merriam-webster.com/dictionary/part?show=0&t=1366224315; and (3) A component is "a constituent part: INGREDIENT." See www.merriam-webster.com/dictionary/component.

[52] Letter from Anthony M. Cooke, Chief Counsel, NHTSA to Ashley G. Alley, Office of General Counsel, Government Accountability Office (Jul. 19, 2007). See http://isearch.nhtsa.gov/files/GAO%20telematics%20Sept%2013.htm (last accessed Jan. 27, 2014).

[53] See https://www.onstar.com/web/fmv/home?g=1 (last accessed Jan. 27, 2014).

[54] 49 U.S.C. § 30102(a)(7)(B) (covering replacements, improvements, accessories, and additions).

"replacements," "improvements," "accessories," or "additions" in part (B) as a narrower set of objects than in part (A). Thus, NHTSA interprets its authority over aftermarket equipment installed in used vehicles as at least as comprehensive as its authority over original equipment installed in new vehicles.

Items that are considered to be accessories or additions are not necessarily closely related to the systems, parts, and components originally installed in new motor vehicles (in the sense that these items potentially do not duplicate the functions of original equipment), as a "replacement" or "improvement" might be. The dictionary definition of "addition" seems to imply that an "addition" to the motor vehicle is an item that becomes united or joined with a motor vehicle.[55] In other words, it is not an item that can be freely carried into and out of the vehicle.

Section III.D.2 describes a wide range of aftermarket V2V equipment items that fall within NHTSA's authority to regulate. Integrated aftermarket V2V equipment is referred to in this document as a "retrofit safety device," and is defined as a V2V system purchased and installed in a vehicle after first sale, which can transmit and receive the BSM, run safety applications, and provide alerts/warnings to the driver through an in-vehicle display (likely the center console DVI). Another noteworthy feature of the RSD is its integration into the vehicle's data bus, so that it can obtain information from the vehicle about the vehicle's operation in use to maximize its effectiveness – such as having access to the vehicle's actual speed rather than attempting to estimate it through GPS coordinates, which helps determine the imminence of a potential crash event and could therefore improve timing for need to warn. Thus, the integrated aftermarket RSD is scarcely different from the integrated OE V2V system, with similar if not identical components, which can either "improve" the vehicle or be an "addition" to it under § 30102(a)(7)(B). Non-integrated aftermarket V2V equipment (i.e., that which can be removed from a vehicle relatively easily, like a navigation-system-type device or a smartphone application) will be covered in Section IV.A.3.

3. Non-integrated aftermarket equipment

It is difficult to predict at this point how wide the potential future range of aftermarket V2V equipment might be. If we take as an example all of the electronic tools that drivers now have at their disposal to aid in navigation, there are integrated OE services like GM's OnStar mentioned above, which is also available for certain vehicles as an aftermarket option; there are "dedicated" navigation devices sold by companies like Garmin or TomTom, which can be installed in a vehicle simply by mounting it in a cradle and can be as easily removed and

[55] As last accessed in Merriam Webster on Jan. 27, 2014: (1) An addition is "a part added (as to a building or residential section)." See www.merriam-webster.com/dictionary/addition; and (2) To add means "to join or unite so as to bring about an increase or improvement." See www.merriam-webster.com/dictionary/add.

installed in another vehicle; and there are smartphone applications, such as Google Navigation or Apple Maps, which use the phone's GPS (and often a connection to the Internet) to determine where a vehicle is and where it needs to go to reach a certain destination, all the while allowing full or nearly-full access to all of the phone's other features. It seems plausible that future aftermarket V2V devices will span a similar range of forms and functions. Depending on their design and apparent purpose, non-integrated or "nomadic" devices, which can be carried into and out of vehicles at the driver's whim, may still be covered by the Safety Act.

§ 30102(a)(7)(B) and (C) allow the agency to regulate "accessories" as well as "devices or articles … manufactured [or] sold … with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death." As with the other portions of the definition of motor vehicle equipment, we interpret these words to cover both mechanical and electronic "accessories," "devices," and "articles."

The dictionary definition of "accessory" states that an accessory is a secondary item which adds some value or function (such as additional convenience or effectiveness) to the original item.[56] While such a definition does not contemplate that item's becoming a part of (or physically attached to) the motor vehicle in order to be regarded as an accessory (as such an interpretation would make "accessory" duplicative of the term "addition"), this definition does seem to imply some sort of use of the item in conjunction with the motor vehicle. Thus, an item could be an "accessory" under § 30102(a)(7)(B) if a substantial portion of its expected use were in conjunction with motor vehicles.

A dedicated handheld aftermarket V2V device would fall comfortably under any of these definitions – it could be an "accessory," or it could be a "device or article…manufactured or sold with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death" because a substantial portion of its expected use is reasonably in conjunction with a motor vehicle. Moreover, the anticipated basic trait of any V2V device purchased for installation in a vehicle is that it emits the BSM, whether or however it provides safety information to the driver. Emitting a BSM will necessarily protect the driver from incidents that might occur with other V2V-equipped vehicles, which are able to detect the BSM and alert their own drivers accordingly. This is fundamentally a safety purpose.

For mobile devices, like a smartphone, a tablet, a tablet computer or other mobile platform, in which V2V-enabled applications and related technology are only one of several functions, the Safety Act authorizes the agency to regulate the V2V-enabled applications to the extent that they are an accessory to a motor vehicle or that they are "manufactured or sold with

[56] As last accessed in Merriam Webster on Jan. 27, 2014: (1) An accessory can be "a thing of secondary or subordinate importance: ADJUNCT" or "an object or device not essential in itself but adding to the beauty, convenience, or effectiveness of something else." See www.merriam-webster.com/dictionary/accessory.

the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death."[57] Consider the example of an application that a vehicle owner can download for a smartphone to enable the smartphone to transmit and receive BSMs. This application on the smartphone could gather information on surrounding vehicles that are transmitting BSMs and use this information to alert a driver of a potential crash. In this situation, the application is an accessory to the motor vehicle (by way of its use with the motor vehicle) and also a "device or article manufactured or sold with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death."

In addition to the software application itself, the performance of safety applications could be affected by characteristics of the mobile platform (i.e., hardware) on which they are run. Hardware attributes such as data processing speed, GPS accuracy, screen size, contrast ratio, image resolution, camera resolution, and sound/voice quality could affect the application's ability to perform its safety function. For example, the processor on the mobile platform might not have the necessary computational power to process incoming BSMs quickly enough so that a warning could be issued to the driver in a timely manner. This possibility could be taken into account by establishing criteria for the application to ensure that it could be run only on devices with sufficient technical hardware capability to enable the application to function at a level of minimum performance necessary for safety.

The aftermarket V2V device designs examined in this paper that are most likely related to future nomadic aftermarket V2V devices include "self-contained" devices, which we assume would connect to the vehicle only for a power source (i.e., not connect to the data bus) and would both emit/receive a BSM and provide safety applications for the driver, and "vehicle awareness devices" or VADs, which simply emit a BSM. Both of these types of devices are discussed in more detail in Section III.D.2, and as explained above, fall comfortably within the definition of motor vehicle equipment under the Safety Act.

4. Software that aids or updates the V2V system

We discussed above that NHTSA's Safety Act authority covered not only tangible mechanical and electronic motor vehicle equipment, but also reasonably extended to cover *intangible* electronic motor vehicle equipment. Depending on their character, software and algorithms that aid or update V2V technologies may be OE, and thus covered under § 30102(a)(7)(A); or those that are part of aftermarket devices or are updates to either OE or

[57] The agency notes that its regulatory authority with respect to mobile devices extends beyond V2V applications and technologies. Examples of more general capabilities or features that may cause mobile devices, insofar as they are used in conjunction with motor vehicles, to fall within the ambit of "motor vehicle equipment" include the following: the capability of being paired with a vehicle's electronics, whether through wired or wireless connection; the "driver mode" on unpaired devices; and the capability of the devices and the vehicle to distinguish automatically whether a device is located in the driver's position or a passenger's position.

aftermarket devices, may be covered under § 30102(a)(7)(B) as "replacements," "improvements," or "additions." Software could also be an "accessory" as long as a substantial portion of its expected use is in conjunction with a motor vehicle. For example, a software application that could be installed on a cell phone for the purpose of enabling the phone user to perform such vehicle-related functions as starting/stopping or locking/unlocking a motor vehicle through manipulating the controls on the phone would be considered an accessory to the motor vehicle even if the cell phone itself is not.[58] Other applications can perform functions related to on-road vehicle operation. An example is a software application that uses the camera function on a smartphone placed on a vehicle's dashboard to detect and recognize vehicles on the road ahead and provide forward collision warnings.[59] Regardless of where the software is located (i.e., on what type of hardware), the software itself would be subject to the Safety Act and could be subject to a safety standard or other exercise of NHTSA's authority (e.g., a recall for a defective condition).

5. Roadside infrastructure (V2I)

There are a couple of types of roadside infrastructure that may be involved in facilitating DSRC-based V2V, as discussed in Section III.D.3. Communications infrastructure physically helps get the messages from the vehicles to and from the SCMS (as at first usage, when the

[58] Our conclusion that software can be an item of motor vehicle equipment is reinforced by the recent enactment of MAP-21. In that Act, Congress implicitly recognized this fact when it directed NHTSA to examine the need for safety standards with regard to electronic systems in passenger motor vehicles. See Pub. L. No. 112-141, §§ 31401-02, 126 Stat. 405.
Separately, NHTSA is not the only agency that has concluded its statutory authority applies to software. For example, the Food and Drug Administration (FDA) has adopted an interpretation of its statutory authority that would subject software installed on mobile devices to regulation under the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301 et eq. (2006). See Guidance for Industry and Food and Drug Administration Staff; Mobile Medical Applications; Availability, 78 Fed. Reg. 59038 (Sept. 25, 2013) [hereinafter FDA Guidance] (announcing the availability of the FDA's application of the agency's regulatory authority to software applications installed on mobile devices) at www.fda.gov/downloads/MedicalDevices/../UCM263366.pdf (last accessed Feb. 6, 2014). The FDA stated that it was issuing the guidance to inform manufacturers, distributors, and other entities about how the FDA intends to apply its regulatory authorities to select software applications intended for use on mobile platforms (mobile applications or "mobile apps"): Consistent with the FDA's existing oversight approach that considers functionality rather than platform, the FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended. FDA Guidance, *supra*. The term "device" is defined in the Federal Food, Drug, and Cosmetic Act as:

> an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is . . . recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them, [ ] intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary Intended purpose.

21 U.S.C. § 321(h) (2006).

[59] E.*g*., see www.ionroad.com/ (last accessed Jan. 28, 2014).

vehicle is self-reporting a malfunction, or when it is reporting on another vehicle's perceived malfunction), and helps get new certificates and the CRL from the SCMS to the V2V-equipped fleet. The communications infrastructure includes roadside equipment (RSE) units, which contain a DSRC radio or a cellular modem, a processor, connection ports, antennas, and software. The RSE uses wireless DSRC to send messages/materials to on-board equipment (OBE). The RSE also connects to the SCMS via a wired connection (i.e., through the Internet), in order to support the transmission of reports from OBE through the RSE to the SCMS and the transmission of certificates from the SCMS through the RSE to the OBE. Security infrastructure helps ensure that the messages sent are trustworthy, and helps remove malfunctioning devices from the system and protect against outside threats. Physically speaking, security infrastructure will include computer hardware, software, and a physical location for all of the components of the SCMS, which will be connected via the Internet to the RSEs, which then connect to the V2V-equipped vehicles' OBE.

It could, therefore, end up being important for NHTSA to regulate some aspects of infrastructure as a way to avoid regulatory gaps that could critically compromise the overall system. Given that certain elements of infrastructure are just as related to safety as on-board equipment, and equally intended for safety, the next question becomes *how*, if possible, to regulate that infrastructure. Fitting these infrastructure pieces under NHTSA's Safety Act authority as items of motor vehicle equipment depends on their nature and apparent purpose. If, as discussed above, we consider "accessories" as items that are used concurrently with one vehicle, then many pieces of roadside infrastructure, which can be used concurrently with many vehicles at once, are probably not "accessories." However, if the apparent purpose of the roadside equipment is safety, then it is arguably a device "manufactured … with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death," and therefore motor vehicle equipment under § 30102(a) (7)(C). For example, an RSE at an intersection could provide Signal Phase and Timing information and an intersection map to vehicle OBE to support the safety applications that might be triggered to help drivers avoid intersection collisions; this would arguably be a safety purpose, even if the RSE could also be providing that SPaT information and map for other purposes as well. For that matter, any RSE that communicates with vehicles in a way that promotes V2V or V2I communications would potentially appear to be doing so for a safety purpose. On the other hand, an RSE that might receive data from a vehicle, but cannot communicate with vehicles, would be unlikely to affect vehicle safety and, accordingly, would likely not be considered motor vehicle equipment.

Policy Need IV-1 Road Side Equipment Authority

Policy Need:	Determination of Authority for NHTSA to regulate Road Side Equipment
Description:	NHTSA will thoroughly evaluate the need to regulate aspects of RSE operation and assess its authority for doing so.

Even if NHTSA decided not to exercise authority directly over roadside infrastructure, NHTSA can still significantly influence its design and operation through our Safety Act authority to establish safety standards. As will be discussed in more detail below when we explain what a V2V system practicable and consistent with our legal authority might include, the Safety Act states, among other things, that motor vehicle safety standards must be: (1) practicable, (2) meet the need for motor vehicle safety, and (3) be stated in objective terms.[60] As one hypothetical example, in order to meet the need for motor vehicle safety, a safety standard for DSRC-enabled FCW might include provisions to ensure that all messages received from other vehicles that could trigger the FCW: (1) Come with some kind of authentication to verify message is from a trusted source; and (2) Include provisions covering checking the accuracy of the information from the outside source. RSE would need to be interoperable in order to ensure that they functioned correctly within the system – meaning that the messages they send have to be able to be read by the OBE in order for the OBE to act on it.

Many aspects of the V2V system, then, can qualify as motor vehicle equipment under the Safety Act, which means that NHTSA can regulate them and mandate their installation in new motor vehicles (as appropriate) per 49 U.S.C. § 30111 (NHTSA may prescribe motor vehicle safety standards for motor vehicles and motor vehicle equipment) and § 30102(a)(9) ("motor vehicle safety standard" means a minimum standard for motor vehicle or motor vehicle equipment performance). For the other parts of the V2V system that NHTSA cannot regulate directly under the Safety Act, we can influence how they develop to a significant extent through the manner in which we regulate, as in the infrastructure example above.

Under both the Vehicle Safety Act and the Highway Safety Act, NHTSA has other ways of affecting the parts of the V2V system that cannot be regulated directly. For example, 49 U.S.C. § 30182 provides NHTSA authority to enter into contracts, grants, and cooperative agreements with a wide range of outside entities to conduct motor vehicle safety research and development activities, including activities related to new and emerging technologies. Separately, the Highway Safety Act (23 U.S.C. § 401 et seq.) authorizes NHTSA to enter into contracts, grants, cooperative agreements, and other transactions for research and development activities with a similarly wide range of outside entities in "all aspects of highway and traffic safety systems … relating to [ ] vehicle, highway, [and] driver … characteristics" (§ 403(b)), as well as collaborative research and development, on a cost-shared basis, to "encourage innovative solutions to highway safety problems" and "stimulate the marketing of new highway safety related technology by private industry" (§ 403(c)). Because issues related to V2V are cross-cutting, spanning both the Vehicle Safety Act and the Highway Safety Act, these separate authorities provide the agency with sufficient flexibility to enter into a variety of agreements

[60] 49 U.S.C. § 30111(a).

related to the development of a V2V security system (although the agency currently lacks sufficient appropriations to incur any significant Federal expenditures for these purposes).

A principle of appropriations law known as the "necessary expense doctrine" allows NHTSA to take the next step of entering into contracts or agreements to ensure the existence of sufficient communications and security systems to support deployment of V2V technologies, if V2V communications are mandated or otherwise regulated by a Federal Motor Vehicle Safety Standard or other NHTSA regulation. According to that principle, when an appropriation is made for a particular purpose, it confers on the receiving agency the authority to incur expenses necessary to carry out the purpose of the appropriation.[61] Under the necessary expense doctrine, the spending agency has reasonable discretion to determine what actions are necessary to carry out the authorized agency function. Here, the deployment and operation of the SCMS is necessary in order for V2V technology and on-board equipment to function in a safe, secure and privacy-protective manner. As designed, V2V technology cannot operate without a sufficient security system, and absent such a security system, misbehavior by hackers or others could compromise V2V functionality and participant privacy. If the problem of "misbehavior" were sufficiently widespread, it might even cause widespread disregard of or delayed response to V2V warnings. Hence, a robust SCMS is imperative in the V2V regulatory environment.

For these reasons, in addition to NHTSA's research, development, and collaboration authority under the Vehicle Safety Act and the Highway Safety Act, if the agency issues a V2V FMVSS or other V2V-related regulation, the necessary expense doctrine provides sufficient authority under the Vehicle Safety Act to take the next step of entering into agreements or contracts, either for cost or no-cost, with the goal of ensuring the existence (i.e., the development and operation) of sufficient communications and security systems to support the reliability and trustworthiness of V2V communications. As is the case under the agency's research and development authority, discussed above, the current limiting factor is the absence of sufficient appropriations to incur any significant expenses in this regard.

[61] Under the necessary expense doctrine, an expenditure is justified if it meets a three-part test: (1) the expenditure must bear a logical relationship to the appropriation sought to be charged (i.e., it must make a direct contribution to carrying out either a specific appropriation or an authorized agency function for which more general appropriations are available); (2) the expenditure must not be prohibited by law; and (3) the expenditure must not be otherwise provided for (i.e., it must not be an item that falls within the scope of some other appropriation or statutory funding scheme. See U.S. Gen. Accounting Office, Principles of Federal Appropriations Law 4–22 (3d ed.2004) (the "GAO Redbook") at www.gao.gov/special.pubs/3rdeditionvol1.pdf.

B. Agency actions that are practicable and consistent With its legal authority

1. Elements of the Safety Act that would apply to potential future agency actions

A V2V system, as currently envisioned, is a compilation of many elements. Essentially, DSRC units in vehicles send out BSMs to alert other vehicles to their presence and receive BSMs from other vehicles in order to determine whether to warn their drivers of impending risk; BSMs must be accompanied by security certificates so that the receiving vehicle can trust their source; and the receiving vehicle receives the BSM through its DSRC unit and triggers safety applications (at this point, we are only discussing applications that would provide warnings), if necessary, depending on what the message received indicates about the sending vehicle's behavior. In order for the entire system to function effectively, each vehicle or aftermarket device participating in the system may need periodic updates to its security certificates, and may need information about vehicles or devices that are malfunctioning or have been otherwise compromised (so that they know not to trust the BSMs received from those vehicles or devices). In addition, the system also needs: (1) An overarching security manager to provide those updates and that information; and (2) A communications network to get those updates and information to the devices. How, then, would NHTSA exercise its legal authority from a central source to bring these elements into existence?

As explained above, NHTSA may establish Federal Motor Vehicle Safety Standards (which would be codified in 49 CFR Part 571) for new motor vehicles and motor vehicle equipment. NHTSA could establish FMVSSs for DSRC units in vehicles (requiring that all new vehicles be equipped with DSRC) and in aftermarket equipment, and also for the safety applications enabled by those DSRC units. As part of those FMVSSs, NHTSA could include requirements for content of the BSM, content of the security certificates (including how up-to-date they need to be), and so on.

NHTSA has general authority to prescribe regulations that help to carry out the duties and the powers of the Secretary, including, for example, the overarching purpose of 49 U.S.C. Chapter 301, to reduce traffic accidents and deaths and injuries resulting from traffic accidents.[62] There are fewer substantive requirements for a non-FMVSS regulation,[63] which can be helpful,

[62] Under the Safety Act as originally written, NHTSA had express authority to issue, amend, and revoke such rules and regulations as deemed necessary to carry out the Safety Act. See Safety Act, Sec. 119, previously codified at 15 U.S.C. § 1407. That language was not included in the recodification of the Safety Act in 1994, but the Department of Transportation Act continues to include similar language, currently codified at 49 U.S.C. § 322, giving the Secretary authority to prescribe regulations to carry out the duties and powers of the Secretary, and allowing that authority to be delegated.

[63] A regulation not promulgated as an FMVSS must still comply with Administrative Procedure Act requirements to be reasonable and contain a rational connection between the factual support for the rule and the requirements of the

for example, if the agency is concerned about fulfilling one or some of the requirements discussed below for FMVSSs; but the agency also has more enforcement tools available for dealing with non-compliance with a safety standard as compared to non-compliance with a non-FMVSS regulation.[64] Additionally, the preemptive effect of an FMVSS is clear from the Safety Act.[65]

We will concentrate the rest of this discussion on the requirements for FMVSSs. A future V2V program would likely be more comprehensively successful if DSRC and DSRC-based safety applications are required through FMVSSs than if NHTSA issued non-FMVSS regulations that merely set out how DSRC must work if provided. Without a requirement that all new vehicles be equipped with DSRC, it would likely take far longer for DSRC to penetrate a substantial portion of the nation's vehicle fleet, thus delaying V2V's benefits and making security system needs hard to predict.

Under the Safety Act, NHTSA's motor vehicle safety standards are generally performance-oriented.[66] Further, the standards are required to be practicable, objective, and meet the need for safety.[67] The following section will discuss briefly the meaning of each of these requirements, and then explore what the agency might do in order to ensure that safety standards for DSRC and DSRC-enabled safety applications reasonably meet those requirements.

a) What does "performance-oriented" mean?

In the Safety Act, the Secretary is directed to issue motor vehicle safety standards. "Motor vehicle safety standards" are defined as "minimum standard[s] for motor vehicle or motor vehicle equipment *performance*."[68] One point to note at the outset is the party of whom performance is required: NHTSA's safety standards apply to manufacturers of new motor

rule itself, and it must also carry out the powers and duties of the Secretary, by doing things like facilitating the agency's performance of its statutory functions or providing additional assurance that regulated parties will properly perform their statutory and regulatory obligations.

[64] NHTSA generally has three enforcement tools relevant to standards and regulations: notification and remedy (recalls) of noncompliant vehicles (49 U.S.C. §§ 30118, 30119, 30120), injunctions (49 U.S.C. § 30163(a)), and civil penalties (49 U.S.C. § 30165). While NHTSA can order recalls and assess civil penalties, only a court can order an injunction; additionally, NHTSA's orders for recalls or civil penalty assessments are themselves enforceable only in court.

[65] 49 U.S.C. § 30103(b).

[66] 49 U.S.C. § 30102(a)(8) (defining "motor vehicle safety" as "the performance of a motor vehicle . . . in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle"); *and* § 30102(a)(9) (defining "motor vehicle safety standard" as "a minimum standard for motor vehicle or motor vehicle equipment performance"). See also: S. Rep. No. 89-1301, at 2713-14 (1966) (stating that motor vehicle standards issued by NHTSA should specify a minimum level of safety performance).

[67] 49 U.S.C. § 30111(a) (establishing requirements for NHTSA to follow when issuing motor vehicle safety standards).

[68] Id.; see also: § 30102(a)(9) (emphasis added).

vehicles and motor vehicle equipment. It therefore falls to those "manufacturers" – from vehicle OEMs to OE suppliers to aftermarket device manufacturers to creators of V2V safety applications for smartphones – to certify compliance with any safety standards established by NHTSA, and to conduct recalls and remedy defects if NHTSA finds them.[69] Vehicle owners are generally not required to comply with NHTSA's safety standards, which means that for vehicles already on the roads, participation in the V2V system would be entirely voluntary: NHTSA can regulate how aftermarket devices function, but it cannot force manufacturers or drivers to add them to used vehicles. The one exception to this rule against retrofit is that NHTSA has authority to require retrofit of commercial heavy-duty vehicles,[70] but that is not part of this research paper on light-duty vehicles, and will be examined in more detail in the agency's decision in 2014 with reference to heavy-duty vehicles.

While NHTSA is directed to establish performance standards, the case law and the legislative history indicate that when necessary to promote safety, NHTSA can be quite specific in drafting its performance standards and may require or preclude the installation of certain equipment. The cases have reinforced this concept by determining that NHTSA is "generally charged"[71] with setting performance standards, instead of becoming directly involved in questions of design.[72] The legislative history further illustrates that NHTSA's standards are to "[specify] the required minimum safe performance of vehicles but not the manner in which the manufacturer is to achieve the specified performance."[73] An example cited in the legislative history points to "a building code which specifies the minimum load-carrying characteristics of the structural members of a building wall, but leaves the builder free to choose his own materials and design."[74] In that example, the agency could require the wall to be built (analogous to requiring certain equipment in vehicles) but would be expected to measure the wall's regulatory compliance by its performance rather than its design.

Although the Safety Act directs NHTSA to issue performance standards, however, Congress understood that the agency may preclude certain designs through these performance standards. "Motor vehicle safety" is defined in the Safety Act as the performance of a motor

[69] 49 U.S.C. § 30115(a), "Certification of compliance; In general"; § 30116, "Defects and noncompliance found before sale to purchaser"; § 30117(a), "Providing information to, and maintaining records on, purchasers; Providing information and notice"; § 30118, "Notification of defects and noncompliance"; § 30119, "Notification procedures"; § 30120, "Remedies for defects and noncompliance."

[70] Per 49 CFR 1.95, which delegates to NHTSA the Secretary's authority under Sec. 101(f) of the Motor Carrier Safety Improvement Act of 1999 (Pub. L. 106-159; Dec. 9, 1999) to promulgate safety standards for "commercial motor vehicles and equipment subsequent to initial manufacture." NHTSA's retrofit authority is coextensive with FMCSA's.

[71] *Washington v. Dept. of Transp.,* 84 F.3d 1222, 1224 (10th Cir. 1996) (citations omitted).

[72] Id. at 1224 (citations omitted).

[73] S. Rep. No. 89-1301, at 2713-14 (1966).

[74] Id.

vehicle in a way that protects the public from unreasonable risks of accident due to (among other things) the design of a motor vehicle.[75] The legislative history indicates that this language is not intended to afford the agency the authority to promulgate design standards, "but merely to clarify that the public is to be protected from inherently dangerous designs which conflict with the concept of motor vehicle safety."[76] This clarification is evidence that Congress recognized that performance standards inevitably have an impact on the design of a motor vehicle.[77]

The courts have further elaborated on the framework established by Congress and have recognized that, when necessary to achieve a safety purpose, NHTSA can be quite specific in establishing performance standards even if certain designs will be precluded. For example, the Sixth Circuit found that an agency provision permitting rectangular headlamps, but only if they were of certain specified dimensions, was not an invalid design restriction and "serve[d] to ensure proper headlamp performance," reasoning that "the overall safety and reliability of a headlamp system depends to a certain extent upon the wide availability of replacement lamps, which in turn depends upon standardization."[78] Thus, the court found it permissible for the agency to establish very specific requirements for headlamps even though it would restrict design flexibility.[79]

Further, the cases indicate that NHTSA can establish standards to require the installation of certain specific equipment on vehicles and establish performance standards for that equipment. For example, the Tenth Circuit found in *Washington v. DOT* that "NHTSA's regulatory authority extends beyond the performance of motor vehicles *per se*, to particular items of equipment."[80] In that case, the validity of NHTSA's FMVSS No. 121 requiring ABS systems on air-braked vehicles was challenged as "imposing design specifications rather than performance criteria."[81] The court's conclusion was based not only on the fact that prior courts had upheld NHTSA's standards requiring particular equipment,[82] but also on the fact that

[75] § 30102(a)(9).

[76] H.R. Rep. No. 89-1919, at 2732 (1966).

[77] Courts have also recognized this fact. See *Chrysler Corp. v. Dept. of Transp.*, 515 F.2d 1053, 1058-59 (6th Cir. 1975); see also*:* Washington, 84 F.3d at 1224 (stating "the performance-design distinction is much easier to state in the abstract than to apply definitively-so …. . This is particularly true when, due to contingent relationships between performance requirements and design options, specification of the former effectively entails, or severely constrains, the latter.").

[78] Chrysler Corp., 515 F.2d at 1058-59.

[79] Id.

[80] Washington, 84 F.3d at 1222, 1225 (citations omitted).

[81] Id. at 1223.

[82] Id. at 1225 (citing *Chrysler Corp. v. Rhodes*, 416 F.2d 319, 322, 322 n. 4) (1st Cir. 1969) ("motor vehicles are required to have specific items of equipment . . . These enumerated items of equipment are subject to specific performance standards," including lamps and reflective devices requiring "specific items of equipment")); *Wood v. Gen. Motors Corp.*, 865 F.2d 395, 417 (1st Cir. 1988) ("requiring seat belts or passive restraints . . . has elements of

Congress had recognized NHTSA's former rulemakings and left NHTSA's authority unchanged when it codified the Safety Act in 1994.

Thus, in summary, NHTSA is required to issue performance standards when regulating motor vehicles and motor vehicle equipment. However, NHTSA is able to be quite specific in establishing performance standards and may preclude certain designs that are contrary to the interests of safety. Further, NHTSA may require the installation of certain equipment and establish performance standards for that equipment.

b) Standards "meeting the need for motor vehicle safety"

As required by the Safety Act, standards issued by the agency must "meet the need for motor vehicle safety."[83] As "motor vehicle safety" is defined in the statute as protecting the public against "unreasonable risk" of accidents, death, or injury,[84] the case law indicates that there must be a nexus between the safety problem and the standard.[85]

However, a standard need not address safety by direct means. In upholding NHTSA's authority to issue a safety standard requiring standardized vehicle identification numbers, the Fourth Circuit Court of Appeals found that an FMVSS requiring VINs met the need for motor vehicle safety by such indirect means as reducing errors in compiling statistical data on motor vehicle crashes (in order to aid research to understand current safety problems and support future standards, to increase the efficiency of vehicle recall campaigns, and to assist in tracing stolen vehicles).[86]

c) "Objective" standards

A standard is objective if it specifies test procedures that are "capable of producing identical results when test conditions are exactly duplicated" and performance requirements whose satisfaction is "based upon the readings obtained from measuring instruments as opposed to subjective opinions."[87] The requirement that standards be stated in objective terms matches

a design standard"); Automotive Parts & Accessories Ass'n v. Boyd, 407 F.2d 330, 332 (D.C. Cir. 1968) ("factor equipped . . . head restraints which meet specific Federal standards").

[83] 49 U.S.C. § 30111(a).

[84] 49 U.S.C. § 30102(a)(8).

[85] e.g.,: *National Tire Dealers Ass'n v. Brinegar*, 491 F.2d 31, 35-37 (D.C. Cir. 1974) (stating that the administrative record did not support a significant nexus between motor vehicle safety and requiring retread tires to have permanent labels because there was no showing that a second-hand owner would be dependent on these labels and no showing as to how often such situations would arise); See also *H&H Tire Co. v. Dept. of Transp*., 471 F.2d 350, 354-55 (7th Cir. 1972) (expressing doubt that the standard met the need for safety because there was little evidence that the required compliance tests would ensure that retreaded tires would be capable of performing safely under modern driving conditions).

[86] *Vehicle Equip. Safety Comm'n v. NHTSA*, 611 F.2d 53, 54 (4th Cir. 1979).

[87] *Chrysler Corp. v. Dept. of Transp*., 472 F.2d 659, 676. See also *Paccar, Inc., v. Nat'l Highway Traffic Safety Admin.,* 573 F.2d 632, 644 (9th Cir. 1978).

the overall statutory scheme requiring that manufacturers self-certify that their motor vehicles or motor vehicle equipment comply with the relevant FMVSSs.[88] In order for this statutory scheme to work, the agency and the manufacturer must be able to obtain the same result from identical tests in order to objectively determine the validity of the manufacturer's certification.[89]

Using those two elements of objectivity (capable of producing identical results and compliance based on measurements rather than subjective opinion), the Sixth Circuit Court of Appeals found that the test procedure in question in an early version of FMVSS No. 208 was not objective because the test dummy specified in the standard for use in compliance testing did not give consistent and repeatable results.[90] The court in this case was unconvinced that the standard met the objectivity requirements even though NHTSA based its test procedure on a test dummy in a voluntary automotive industry standard (Society of Automotive Engineers Recommended Practice J963). The court rejected NHTSA's explanation that, although J963 "may not provide totally reproducible results," "dummies conforming to the SAE specifications are the most complete and satisfactory ones presently available."[91] Further, the court rejected NHTSA's reasoning that, in the event that the agency's test results were different from those of the manufacturers because of the difference in the test dummies, NHTSA's test results would not be used to find non-compliance, stating that "there is no room for an [ ] agency investigation [ ] in this procedure" that enable the agency to compare results of differing tests.[92]

Other courts have also reached similar conclusions. The Ninth Circuit Court of Appeals, relying on the same reasoning adopted by the Sixth Circuit, found that a compliance road test specifying the use of surfaces specifically rated with quantifiable numbers (defining the "slickness" of the surfaces) was objective despite "[t]he fact that it is difficult to create and thereafter maintain a road surface with a particular coefficient of friction does not render the

[88] 49 U.S.C. § 30115(a).

[89] Chrysler Corp., 472 F.2d at 675.

[90] As the court stated,

> The record supports the conclusions that the test procedures and the test device specified . . . are not objective in at least the following respects: (1) the absence of an adequate flexibility criteria for the dummy's neck; the existing specifications permit the neck to be very stiff, or very flexible, or somewhere in between, significantly affecting the resultant forces measured on the dummy's head. (2) Permissible variations in the test procedure for determining thorax dynamic spring rate (force deflection characteristics on the dummy's chest) permit considerable latitude in chest construction which could produce wide variations in maximum chest deceleration between two different dummies, each of which meets the literal requirements of SAE J963. (3) The absence of specific, objective specifications for construction of the dummy's head permits significant variation in forces imparted to the accelerometer by which performance is to be measured.

Id. at 676-78.

[91] Id. at 677.

[92] Id. at 677-79.

specified coefficient any less objective."[93] In this case, both NHTSA and the manufacturer would perform road tests on surfaces with identically rated friction coefficients.[94] In a later case, the Sixth Circuit upheld NHTSA's decision not to incorporate a test suggested by a commenter for wheelchair crashworthiness performed with a "test seat" that "shall be capable of resisting significant deformation" during a test as not sufficiently objective.[95] In the absence of language quantifying how much deformation is significant, terms such as "significant deformation" do not provide enough specificity to remove the subjective element from the compliance determination process.

d) *"Practicable" standards*

In general, the practicability of a given standard involves a number of considerations. The majority of issues concerning the practicability of a standard arise out of whether the standard is technologically and economically feasible. An additional issue is whether the means used by manufacturers to comply with a standard will be accepted and correctly used by the public.

e) *"Technologically practicable" standards*

Significant technical uncertainties in meeting a standard might lead a court to find that a standard is not practicable. For example, the Sixth Circuit Court of Appeals upheld NHTSA's decision to amend FMVSS No. 222 to include requirements for wheelchair securement and occupant restraint on school buses with a static[96] compliance test instead of a dynamic test,[97] noting that the administrative record showed that this particular dynamic test was underdeveloped and had many unresolved technical problems.[98] The court noted that it is not

[93] *Paccar, Inc. v. Nat'l Highway Traffic Safety Admin.*, 573 F.2d 632, 644 (9th Cir. 1978), *cert. denied*, 439 U.S. 862 (1978).

[94] Id. (stating that the "skid number method of testing braking capacity meets the [objectivity] definition. Identical results will ensue when test conditions are exactly duplicated. The procedure is rational and decisively demonstrable. Compliance is based on objective measures of stopping distances rather than on the subjective opinions of human beings.").

[95] *Simms v. Nat'l Highway Traffic Safety Admin*., 45 F.3d 999, 1007-08 (6th Cir. 1995).

[96] Static testing tests the strength of individual components of the wheelchair separately, while dynamic testing subjects the entire wheelchair to simulated real-world crash conditions. See *Simms*, 45 F.3d at 1001.

[97] Id. at 1006-08. Petitioners argued that NHTSA had acted unlawfully in promulgating standards for the securement of wheelchairs on school buses based only on "static" instead of "dynamic" testing. Id. Static testing tests the strength of the individual components of a securement device. Id. Dynamic testing is a full systems approach that measures the forces experienced by a human surrogate (test dummy) in a simulated crash that replicates real-world conditions and assesses the combined performance of the vehicle and the securement device. Id.

[98] Id. at 1005-07. NHTSA agreed that dynamic testing is the preferred approach (because it more fully and accurately represents the real-world conditions in which the desired safety performance is to be provided), but explained that it was not practicable at that time to adopt dynamic testing because there was:

> (1) [N]eed to develop an appropriate test dummy; (2) need to identify human tolerance levels for a handicapped child; (3) need to establish test conditions; (4) need to select a "standard" or surrogate wheelchair; (5) need to establish procedures for placing the wheelchair and test dummy in an effective test

practicable "[t]o attempt to fashion rules in an area in which many technical problems have been identified and no consensus exists for their resolution …. ."[99] In another example, the Ninth Circuit Court of Appeals found a compliance test procedure using a specified friction (slickness) coefficient to be impracticable due to technical difficulties in maintaining the specific slickness test condition. As mentioned above, the Ninth Circuit found the specified coefficient test condition to be objective.[100] However, simply being objective did not also make the test condition practicable. Thus, the cases show that when significant technical uncertainties and difficulties exist in a standard promulgated by NHTSA, those portions of the standard can be considered impracticable under the Safety Act.

However, the requirement that a standard be technologically feasible does not include the additional requirement that the agency show that the technology to be used to comply with the standard is already fully developed and tested at the time that the standard is promulgated. The Sixth Circuit upheld a NHTSA standard requiring "Complete Passive Protection," that required the installation of airbags as standard equipment, by a future date, rejecting petitioner's contention that NHTSA may only establish performance requirements which can be met with devices which, at the time of the rulemaking, are developed to the point that they may be readily installed.[101] Relying on the legislative history of the Safety Act, the court found that the agency "is empowered to issue safety standards which require improvements in existing technology or which require the development of new technology, and is not limited to issuing standards based fully on devices already developed."[102] Thus, the requirement that standards be technologically feasible is sufficiently broad that it can be satisfied by showing that new technology can be developed in time to comply with the effective date of the standard. A corollary of the agency's authority to issue technology-driving standards is that the agency can rely on data other than

> condition; and (6) need to develop an appropriate test buck to represent a portion of the school bus body for securement and anchorages.
>
> Id. at 1005.

[99] Id. at 1010-11.

[100] *Paccar, Inc. v. Nat'l Highway Traffic Safety Admin.,* 573 F.2d 632, 644 (9th Cir. 1978).

[101] See *Chrysler Corp. v. Dept. of Transp.,* 472 F.2d 659, 666, 671-75 (6th Cir. 1972). Stages one and two required vehicle manufacturers to provide "Complete Passive Protection" or one of two other options on vehicles manufactured between January 1, 1972 and August 14, 1973 (for stage one) and after August 15, 1973 (stage two). See id. at 666-67. Stage three, requiring solely "Complete Passive Protection," was required by August 15, 1975. Id. at 667.

[102] Id. at 673. In making its decision, the court stated

> [I]t is clear from the Act and its legislative history that the Agency may issue standards requiring future levels of motor vehicle performance which manufacturers could not meet unless they diverted more of the ir resources to producing additional safety technology than they might otherwise do. This distinction is one committed to the Agency's discretion, and any hardships which might result from the adoption of a standard requiring . . . a great degree of developmental research, can be ameliorated by the Agency under . . . The section [that] allows the Secretary to extend the effective date beyond the usual statutory maximum of one year from the date of issuance, as he has done [here].

Id. at 673.

real-world crash data in justifying those standards. Technology that is not yet either fully developed or being installed on production vehicles cannot generate real-world performance data. Thus, in justifying the issuance of technology-driving standards, it is permissible, even necessary, for the agency to rely on analyses using experimental test data or other types of non-real world performance information in determining whether such standards "meet the need for vehicle safety."

f) "Economically practicable" standards

A standard can be considered impracticable by the courts due to economic infeasibility. This consideration primarily involves the costs imposed by a standard.[103] In the instances in which a court has been called upon to assess whether a standard is economically feasible, typically with respect to an industry composed largely of relatively small businesses, the courts have asked whether or not the cost would be so prohibitive that it could cause significant harm to a well-established industry. In essence, this consideration generally establishes a non-quantified outer limit of the costs that can be reasonably imposed on regulated entities. If compliance with the standard is so burdensome, i.e., costly, so as to create a significant harm to a well-established industry, courts have generally found that the standard is impracticable in its application to that industry.

g) Standards that encourage "public acceptance and use"

Finally, a standard might not be considered practicable if the public were not expected to accept and correctly use the technologies installed in compliance with the standard. When considering passive restraints such as automatic seatbelts, the D.C. Circuit stated that "the agency cannot fulfill its statutory responsibility [in regard to practicability] unless it considers popular reaction."[104] While the agency argued in that case that public acceptance is not one of the statutory criteria that the agency must apply, the court disagreed. The court reasoned that "without public cooperation there can be no assurance that a safety system can 'meet the need for motor vehicle safety.'"[105] Thus, as a part of the agency's considerations, a standard issued by the agency will not be considered practicable if the technologies installed pursuant to the standard are so unpopular that there is no assurance of sufficient public cooperation to meet the safety need that the standard seeks to address.[106]

[103] E.g., *Nat'l Truck Equip. Ass'n v. Nat'l Highway Traffic Safety Admin.*, 919 F.2d 1148, 1153-54 (6th Cir. 1990); *Ctr. for Auto Safety v. Peck,* 751 F.2d 1336, 1343 (D.C. Cir. 1985) (panel opinion by Circuit Judge Scalia).

[104] *Pac. Legal Found. v. Dept. of Transp.,* 593 F.2d 1338, 1345-46 (D.C. Cir.), *cert. denied*, 444 U.S. 830 (1979).

[105] Id.

[106] Pursuant to concerns about public acceptance of various seat belt designs, NHTSA issued a final rule in 1981 adding seat belt comfort and convenience requirements to Standard No. 208, Occupant Crash Protection. Federal Motor Vehicle Safety Standards; Improvement of Seat Belt Assemblies, 46 Fed. Reg. 2064 (Jan. 8, 1981) (codified at 49 CFR Part 571).

The discussion in this section thus far has presented the requirements under the Safety Act for establishing motor vehicle and motor vehicle equipment safety standards; the following discussion will cover how theoretical safety standards for DSRC and DSRC-based safety applications might go about fulfilling those requirements.

2. Safety standards for DSRC

NHTSA would theoretically establish an FMVSS for DSRC in order to enable safety applications such as IMA, FCW, LTA, DNPW, and others. As discussed above, we are assuming here that the FMVSS for DSRC would require DSRC equipment in all new vehicles. For purposes of this discussion, we assume that DSRC would have its own FMVSS rather than have all of its requirements incorporated into FMVSSs for DSRC-based safety applications – this would appear to be preferable to avoid duplication of requirements if multiple safety applications were going to be DSRC-based – although any or all of these FMVSSs could certainly be established simultaneously. This would also permit OEMs to comply with at least some of the safety application FMVSSs using non-V2V technology (e.g., sensor-based FCW technology).

An FMVSS for DSRC must include minimum standards for DSRC performance. This requires a determination of what tasks DSRC must be able to perform. NHTSA has certain performance measures already available as developed for the Safety Pilot,[107] and is also currently working to develop a comprehensive list of DSRC use cases as a basis for developing performance measures that may be more appropriate for an eventual FMVSS, but at its most basic, the DSRC likely must be capable, among other things, of sending and receiving BSMs to other vehicles and to infrastructure; of *not* sending or receiving certain types of information that might be harmful to the vehicle or to the V2V system (including BSMs, if the system recognizes or the DSRC recognizes itself to be somehow compromised); and of receiving new certificates and software updates. Each of those tasks, in turn, has sub-tasks in order to ensure effective performance. For example, when a DSRC unit sends out a BSM, the BSM needs to:

- Contain the relevant elements and describe them accurately (e.g., vehicle speed; GPS position; vehicle heading; DSRC message ID, etc.);
- Be received quickly enough for the receiving DSRC unit to interpret the message and respond accordingly by triggering safety applications or not;
- Contain something to indicate that it should be trusted by the receiving DSRC unit and that the message has not altered (e.g., a signed security certificate that is up-to-date).

[107] E.g., System Requirements Description, 5.9 GHz DSRC Vehicle Awareness Device Specification, Version 3.6 (Jan. 25, 2012) at www.its.dot.gov/newsletter/VAD%20Specs.pdf (last accessed Jan. 28, 2014).

In the interest of brevity, this discussion does not contain every current anticipated task and sub-task that would likely be included among minimum standards for DSRC performance – those can be found in Section V.E. For purposes of helping to ensure legal sufficiency, relevant tasks must be identified and minimum standards for DSRC units performing those tasks must be specified. SAE J2945.1, developed in large part through DOT funds, contains minimum performance requirements for BSM communication, but SAE has not yet developed any requirements for message accuracy, test procedures, or how the data and message would be used (such as message transmission rate or optional data usage in various situations), nor is it certain that they will do so in the future. DOT and its research partners have developed performance requirements for the BSM and DSRC to use in the Safety Pilot[108] that the agency believes are adequate for that purpose. SAE has yet to incorporate any of this work, however, in order to develop comprehensive voluntary consensus standards that NHTSA could consider to ensure full DSRC interoperability.[109] SAE's work is still ongoing, but it is likely reasonable to assume that it would be completed prior to a potential future proposal to establish an FMVSS for DSRC. In order to determine the performance requirements for the BSM and DSRC that would be needed to support interoperability on a larger scale, NHTSA will likely rely on the results of the Safety Pilot and other ongoing research, and examine whatever voluntary consensus standards are available at that time and seem applicable. Section V.E discusses the status of the voluntary consensus standards under development that are relevant to DSRC.

A future DSRC standard may also need to include requirements to ensure that messages are able to be received even as more vehicles and infrastructure are broadcasting more often – "message congestion" has not come up in the Model Deployment due to the relatively low density of DSRC-equipped vehicles and infrastructure in Ann Arbor, but may become an issue going forward, especially in heavily populated areas. DOT is sponsoring research to evaluate the capacity of the spectrum and mitigate the effects of channel congestion on DSRC performance; CAMP has also conducted testing, but has been unable to create a situation of channel saturation.[110] Depending on the findings of that research, the agency may want to consider requiring manufacturers to use a particular congestion mitigation algorithm so that the safety applications can continue to work as the broadcast channel approaches capacity. As discussed above, the case law reasonably supports the agency specifying certain design aspects if necessary to ensure proper operation of safety systems.

[108] Please see: System Requirements Description, 5.9 GHz DSRC Vehicle Awareness Device Specification, Version 3.6 (Jan. 25, 2012) at www.its.dot.gov/newsletter/VAD%20Specs.pdf (last accessed Jan. 28, 2014) and System Requirements Description, 5.9 GHz DSRC Vehicle Awareness Device Specification, Version 3.6 (Dec.26, 2011) at www.its.dot.gov/meetings/pdf/T2-05_ASD_Device_Design_Specification_20120109.pdf (last accessed Feb. 20, 2014).

[109] See http://standards.sae.org/wip/j2945/ (last accessed Jan. 28, 2014).

[110] For more information, see Section V.E.1.c).

A safety standard for DSRC also needs to meet the need for safety, which means, as discussed above, that there needs to be some nexus between DSRC and the safety problem that a DSRC standard is trying to resolve, but does *not* mean that DSRC must directly create more safety itself, as long as it is enabling other safety applications. On the second point, the case law supports this view – if VINs could be upheld as meeting the need for motor vehicle safety simply by virtue of the fact that they aid research in understanding safety problems and supporting future standards, as well as aiding recall campaigns and tracking of stolen vehicles, then DSRC, which would directly enable half a dozen safety applications at its inception and perhaps many more eventually, seems even more likely to meet the need for safety in that respect.

If the agency decides to issue an FMVSS, we will want to be sure to explain carefully the nexus between DSRC and the safety problems that we are trying to address, depending on the order in which the agency issues FMVSSs for safety applications. There is no doubt that there is *a* nexus – DSRC *can* enable all of the safety applications under consideration by the agency, which means that DSRC can help to address the safety problems of, e.g., intersection collisions, collisions with forward stopped or slowing vehicles, collisions that occur because a driver chose to pass a forward vehicle without enough room to do so safely, etc. As far as we know currently, DSRC is the only technology that can enable Intersection Movement Assist, Left Turn Assist, and Electronic Emergency Brake Light. For some of the other safety applications, which can also be enabled by other technologies besides DSRC, such as on-board sensors, radar, or cameras, DSRC can add robustness to an on-board system. The agency may nonetheless want to develop evidence that a DSRC mandate represents a reasonable technological solution for addressing the safety problems at issue. In sum, DSRC will either be the sole enabler of some safety applications or present a possible enhancement to on-board systems with regard to other applications. In either case, DSRC will address safety needs.

A DSRC standard also needs to be objective. It is likely to be objective, according to the case law, if exact duplication of test conditions yields identical results, and if compliance is based on measurements rather than on subjective opinion. As explained above, while there are test procedures for DSRC performance that were used in the Safety Pilot,[111] test procedures for DSRC performance, survivability, etc. that might be appropriate for an FMVSS have yet to be developed, and research continues. Testing for DSRC will likely require procedures to establish both that the DSRC unit itself is able to receive and transmit the needed messages as timely as needed and without being compromised (recognizing that in the current design, one radio will be used exclusively for sending and receiving BSMs, while the other will be used to communicate with infrastructure and the security system), and that the BSM elements are accurate. Some

[111] E.*g*., Safety Pilot Model Deployment, Deliverable: Interoperability Stage II Test Report, Task 5. See Docket No. NHTSA-2014-0022

examples of tests that could be needed for DSRC message transmission/reception might include tests for:

- Range,
- Latency,
- Ability to transmit,
- Ability to receive,
- Accuracy of GPS,
- Accuracy of information on vehicle speed and heading, and
- BSM performance in a degraded state when GPS is not available.

Some examples of tests that could help to determine the accuracy of the BSM elements might include, among other things:

- Sending an instrumented vehicle through a set of maneuvers and checking whether the BSM is reporting vehicle conditions/activity consistently with what the instruments are reporting;
- Setting up an array of DSRC receivers at a certain distance from the vehicle to test the directional range of the vehicle's broadcast capability;
- Sending a vehicle through a set of maneuvers and checking whether BSMs from that vehicle are received with the required frequency to support particular safety applications; and
- Checking the vehicle's relative reported GPS position against a GPS receiver with a known bias to determine the accuracy of the vehicle's reported relative position.

The agency will have to carefully assess any compliance test that tests the accuracy of GPS to ensure that the test is objective. As one example, atmospheric conditions influence the accuracy of GPS receivers and can cause the same receiver to produce different results, even when the receiver is tested at different times on the same day. Atmospheric and weather conditions also influence the range of radio broadcast capabilities. The agency could adjust the tolerances of the compliance tests to account for factors like this that introduce uncertainty, but this strategy could end up reducing the stringency of the requirements. We also know that there are conditions under which the GPS will not be able to work, such under bridges and in "urban canyons" that exist between tall buildings in urban and city environments. Compliance tests will need to account for these situations, and we are researching methods to compensate for these degradations in performance. These examples help to illustrate the uncertainty that exists in trying to assess the objectivity of potential compliance tests at this time.

And finally, a DSRC FMVSS would need to be practicable – as defined by technological practicability, economic practicability, and public acceptance of the technology.

Technologically, DSRC has existed for over a decade, and is currently being used in Japan to support V2I applications and electronic toll collection. While DSRC may be widely used for some purposes and in some regions, however, ensuring interoperability between vehicles remains an issue needing further research. While comprehensive DSRC performance requirements and test procedures, such as those that would be included in an FMVSS, have yet to be established, it seems reasonably likely that an FMVSS would be technologically practicable assuming that objective tests to ensure interoperability are developed.

In terms of economic practicability, NHTSA currently assumes that the cost of a DSRC standard would include costs for device hardware and software, as well as costs for the security and communications system that would be necessary in order for DSRC to function properly. As discussed in Section XI, we estimate the likely total cost for a V2V system to the consumer (vehicle equipment costs, fuel economy impact, SCMS costs, and communication costs) at approximately $341- $350 (7% to 3% discount rate) per new vehicle in 2020. Economic practicability requires that compliance with the standard should not be so burdensome as to create a significant harm to a well-established industry. It does not seem likely that a court would find the standards economically impracticable either for the auto industry, or for any small business interests potentially implicated, since those would more likely be in the context of aftermarket devices (phone apps and so forth), which are entirely voluntary and do not represent a mandate.

For the question of public acceptance, the main concerns with regard to a DSRC FMVSS likely relate to security and privacy. In order to avoid risk that a DSRC standard is not accepted by the public, the standard could likely benefit from security and privacy requirements for message transmission/receipt – for example, that the message does not contain information that could create an unreasonable privacy risk; that the unit is resistant to tampering, hacking; etc. Another requirement related to security that could create public acceptance issues is when and how updates to the DSRC occur. DSRC units will likely need periodic software upgrades and patches, and may need additional security certificates to be uploaded over the course of their lifetimes. If driver action is needed to make those updates successful – for example, if the driver must take the vehicle to a dealership for the work to be done – it is possible that some drivers simply will forgo the effort, leaving themselves less safe and possibly impairing the entire V2V system. NHTSA could try to develop driver alerts as part of a potential FMVSS to help ensure that drivers take that action, but would have to consider how to balance the need to warn drivers against possible public acceptance issues. At this point, NHTSA is optimistic that updates will be able to be performed automatically. Section V.E.4 provides additional discussion on how device updates could be managed so that this can be avoided, but the agency will continue to research this issue going forward.

Policy Need IV-2 V2V Device Software Updates

Policy Need:	V2V Device Software Updates
Description:	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. V2V devices may become inoperable over time or potentially out of date with system needs as upgrades are implemented. One possible route to address this issue is via terms of use required by the SCMS in connection with providing security services necessary to support V2V communications.

Excessive false warnings may create another public acceptance issue, in that they may annoy drivers and cause them to ignore true warnings if false warnings are too numerous. False warnings may be caused through inaccuracies in a vehicle's reported position, speed or predicted path information: preventing these false warnings will require test procedures to reduce these inaccuracies and mitigation techniques have already been implemented in the Safety Pilot Model Deployment to minimize false positives discovered thus far. Initial analysis of data collected during the second phase of Model Deployment indicates that the false positive mitigation techniques associated with the IMA safety application has reduced the amount of certain false positive alerts observed in the Model Deployment. Additionally, consumer acceptance and practicability of the system is currently dependent on the existence of a security system. If the agency is not able to identify an entity to manage the security system, then that may affect the practicability of any FMVSS mandating DSRC-based V2V, as the security system is currently needed to ensure that messages are trustworthy.

3. Safety standards for DSRC-enabled safety applications

As discussed in more detail in Section VI, the agency is currently investigating six safety applications that could be enabled by DSRC: IMA, FCW, DNPW, EEBL, BSW/LCW, and LTA. We may decide to mandate some or all of these applications, and perhaps also future applications yet to be developed. If we do mandate them, it seems likely that (1) in the interests of stronger enforcement options, they would be incorporated into NHTSA's regulations as an FMVSS, and (2) in the interests of clarity, each would have its own FMVSS. An FMVSS for each of these safety applications must include minimum standards for its performance. This first requires a determination of what tasks the safety applications need to perform, which varies based on the types of safety risks/crash scenarios that the application is intended to address. As further discussed in Section VI, the agency is examining the currently available (research-stage) performance and test metrics associated with each application. Further, the agency is analyzing these metrics against the available safety data to determine whether these metrics cover the applicable safety problem. We envision that each FMVSS for one of these safety applications would set performance requirements that could be met by any technology. For example, FCW might be met through use of radar or cameras, or through use of DSRC. However, if DSRC performance requirements made it reasonable to require more robust performance, we could require that performance when DSRC is mandated. As discussed above, for some applications, like IMA, performance requirements can likely be met *only* with DSRC-based technologies due to their ability to detect crossing-path vehicles, but for others, a variety of technologies could potentially be used.

It would seem clear-cut that FMVSSs for the V2V safety applications meet the need for safety, insofar as we would issue them to address safety problems that continue to cause crashes in the absence of regulation or market forces driving their adoption. The safety applications are clearly intended to relate to safety – they warn drivers of dangerous conditions and are intended to promote safety by triggering a response to avoid the danger.

There are several things that the agency could do to help solidify the nexus of safety application warning and driver response. For example, from a technological perspective, research continues at this point to develop driver-vehicle interfaces for each of the safety applications. We will need to be able to demonstrate how effective the DVIs we may eventually mandate are at warning the drivers and inducing them to avoid the dangerous situation. We currently have reason to believe that the V2V safety applications will meet the need for safety, but our evidence needs to be stronger.

FMVSSs for V2V safety applications also need to be objective, meaning that they specify test procedures that are “capable of producing identical results when test conditions are exactly duplicated” (meaning that the agency and the manufacturer must be able to obtain the same result from identical tests) and performance requirements whose satisfaction is “based upon the readings obtained from measuring instruments as opposed to subjective opinions.” As discussed above, test procedures and performance requirements for the V2V safety applications are still being developed, but NHTSA would ensure that any test procedures it may require would meet the criteria of being objective.

In terms of technological practicability, because test procedures and requirements (including those for DVIs) are still being developed for the V2V safety applications, it could be advisable to provide additional lead time to meet eventual standards in order to ensure that manufacturers have the opportunity to work out how to comply depending on timing for a future potential regulatory action.[112] More research will be helpful in informing future assessments of technological practicability.

In terms of economic practicability, NHTSA currently assumes using preliminary cost estimates that the cost of standards for the V2V-based safety applications would primarily include costs for software that would be used by the vehicle to interpret DSRC signals and make decisions about whether to warn the driver, as well as costs for any hardware that would be necessary to make those warnings happen via the DVI. As discussed above, it seems unlikely that economic practicability would be an issue for potential safety application FMVSSs, but more research to determine costs more precisely would be beneficial to this assessment.

Based on the research we have so far from the Safety Pilot, driver enthusiasm for the V2V safety applications appears mixed – *see* Section VII for more information. Given that DVI requirements remain under development, and given that the algorithms currently being analyzed as part of the Model Deployment have a relatively high false positive rate, more work needs to be done before we can be confident that eventual FMVSSs for V2V safety applications will not have public acceptance risks.

The discussion in this section has focused so far on what it would take to establish FMVSSs to facilitate a V2V system, but a V2V system is not complete without communications and security components that NHTSA cannot mandate fully under its Safety Act authority. As discussed at much greater length in Section IV.A, NHTSA has authority under the “necessary expense” doctrine to enter into agreements or contracts to ensure the existence of sufficient communications and security systems to support deployment of V2V technologies as required by FMVSSs. As part of that authority, an SCMS agreement or contract could be designed with adequate government oversight to ensure that the SCMS is supporting V2V communications in a secure, privacy-appropriate way. Some of the likely primary areas covered in an SCMS agreement or contract might include the nature of the services provided, both on an initial and on an ongoing basis; requirements for system access; requirements to foster user/data privacy; requirements for system security; user fees; data ownership and access; liability; enforcement; and what to do in the event of default or termination.

However, if private industry does not establish the required communications infrastructure without government intervention (which is possible), NHTSA will need to exercise its authority to enter into a contract or agreement to establish the necessary communications and security pieces of a V2V system and will need someone on the other end of that contract or agreement. With no appropriations (i.e., no ability to pay the entity performing this role)

[112] See discussion above regarding the Sixth Circuit’s finding in *Chrysler*, 472 F.2d at 659, 666, and 671-75 (6th Cir. 1972).

currently anticipated for this purpose, the likelihood of success in finding entities willing to take on these considerable tasks will depend on the extent to which private entities can create financial models[113] to support development and operation of the communications and security infrastructure that are consistent with the Department's V2V principles (i.e., no recurring fees for consumers, appropriate privacy and security protections and extensibility to V2I and V2X applications). Thus, having authority is not a guarantee of success in system implementation – the V2V system model is unlikely to work unless private industry moves forward with developing the security and communications infrastructure required for the V2V system or NHTSA is able to reach agreement with the entities who will eventually manage the security and communications systems in a way that encourages their performance but does not create unintended consequences. Potential privacy issues associated with this will be discussed in Section VIII.

4. Discussion of need for additional legal authority prior to taking regulatory actions regarding vehicle to vehicle communication

The agency already has the legal authority between the Safety Act and the necessary expense doctrine to create the pieces needed for a V2V system. We believe that a viable V2V system can be established and maintained under our current authority. However, some have suggested that a system could potentially be better protected if NHTSA had sufficient appropriations to develop the capacity itself to manage the security and communications components of the system, and did not have to rely on contracts/agreements with other parties. NHTSA has no current plans to seek additional funding for this purpose.

C. Non-regulatory actions required to stand up V2V communications

The largest non-regulatory actions needed to create a V2V system, as discussed above, include the possible need to enter into contracts/agreements required to ensure the existence of the communications and security portions of the system (both of which will fall to the security system manager/owners to put in place). These could range in nature from Federal procurement and management of the entities making up the security and communications portion of the system, to procurement solely of the security and communications services themselves, via for cost or no-cost contracts covered by the Federal Acquisition Regulations (FAR), to one or more binding agreements not covered by the FAR with private entities that voluntarily 'stand up' the security and communications parts of the system.

The agency would also need to conduct a number of analyses as part of a potential future regulatory action to establish FMVSSs for DSRC and the V2V safety applications, such as

[113] A possible financial model identified by some stakeholders involves charging fees to motor vehicle and ASD equipment manufacturers that the n can be passed on to consumers via equipment costs.

evaluating the potential effect of standards on small businesses, small organizations, and small governmental jurisdictions under the Regulatory Flexibility Act; consulting with State, local, and tribal governments as appropriate and evaluating the preemptive effect of standards under Executive Order 13132 (Federalism); assessing the costs and benefits of the standards and evaluating whether we have selected the most cost-effective alternative under the Unfunded Mandates Reform Act of 1995 (UMRA); determining and disclosing whether we are imposing requirements to collect information under the Paperwork Reduction Act (PRA); and evaluating whether we could have used technical standards developed by voluntary consensus bodies as required by the National Technology Transfer and Advancement Act (NTTAA), among others. Requirements for the agency's analysis under the Privacy Act will be discussed in Section VIII.

Optionally, we may also decide to conduct a consumer education campaign to raise consumer awareness of the benefits of V2V technologies and help address potential concerns about security and privacy. The agency is aware of public concerns regarding the issue of privacy generally, and a campaign could be developed and shaped to provide clear messaging on the many components and operation of the V2V system specifically developed to protect consumer privacy. Additionally, the campaign could also provide clear messaging on the basic operation of V2V, along with the benefits and potential plans for a rollout.

D. Authority for the spectrum in which V2V will operate, and how it could affect the development of a V2V system

DSRC communications are currently designed to travel in a specific band of the electromagnetic spectrum – specifically, around 5.9 GHz, as allocated by the Federal Communications Commission (FCC) in 1999. The FCC has the authority to allocate sections of the spectrum to various uses within the United States,[114] and is currently considering whether to "share" the 5850-5925 MHz bands with "Unlicensed-National Information Infrastructure" (U-NII) devices.[115] This could potentially have serious consequences for the viability of V2V communications. Existing authorizations for U-NII devices allow them to operate only on a non-interfering basis with licensed services. Issues regarding spectrum will be discussed further in Section V.D.2.

U-NII devices provide short-range, high-speed unlicensed wireless connections in the 5 GHz band for, among other applications, Wi-Fi-enabled radio local area networks, cordless telephones, and fixed outdoor broadband transceivers used by wireless Internet service providers. On April 10, 2013 the FCC published in the Federal Register, a Notice of Proposed Rulemaking

[114] 47 U.S.C. § 303.
[115] FCC docket for this issue. See http://apps.fcc.gov/ecfs/proceeding/view?name=13-49 (last accessed Jan. 28, 2014).

to revise Part 15 of its Rules to permit U-NII devices in the 5.580-5.925 GHz band.[116] DOT submitted comments to the FCC NPRM to the National Telecommunications and Information Administration and NTIA filed those comments with the FCC June 10, 2013.[117] The June 10, 2013 comments indicated DOT's technical concerns related to spectrum sharing with U-NII devices in the 5.9 GHz band, that identified the absence of (1) any proposed technical sharing solution with U-NII devices that would definitively maintain the channel (or medium) access required to guarantee interference-free operation of the critical safety applications; or (2) an assessment of the technical risk to Connected Vehicle safety operations of potential interference from U-NII devices. DOT plans to remain actively involved in the ongoing discussions and technical analyses relating to the FCC rulemaking proceeding and will continue working with NTIA on this spectrum issue.

[116] 78 Fed. Reg. 21320, at 21321(Apr. 10, 2013).

[117] DOT's comments, as submitted by NTIA. See: http://apps.fcc.gov/ecfs/comment/view;jsessionid=hGpQRykFTJLGq48qstFl7wBR2RvJbHBFhCbt470V7ykR1fTvQ2Wy!-528136363!-1469015862?id=6017448690 (last accessed Jan. 28, 2014).

V. Technical Practicability

A. Technical practicability and its importance to an agency decision

Technical practicability is a measure of how feasible a standard is given the technology options that are available to meet it. Significant technical uncertainties in meeting a standard might lead a court to find that a standard is not practicable. V2V technology is currently fairly mature – certainly mature enough to function in the Safety Pilot – and we anticipate that future research will address any lingering uncertainty with how either DSRC or the safety applications should function. The following discussion covers the current state of the agency's knowledge of the different pieces and parts necessary for a V2V system, their technological readiness, and what research may be appropriate going forward. This section does not discuss the security of V2V communications nor the system contemplated to ensure that security, both of which are addressed in Section IX.

B. Overview of hardware components enabling system operation

In general, two sets of components are needed for V2V communications to operate. The first set of components are those required for a device to transmit an accurate and trusted basic safety message and the second are the components needed for a device to receive and interpret a BSM transmitted from another entity.

To *generate and send* a BSM, a device needs to know its own position (such as via a GPS antenna and receiver). Once its position is known, the device needs a computer processing unit that can take its location and combine this with other onboard sensors (e.g., speed, heading, acceleration) to generate the required BSM data string. Once the BSM is generated, a device is needed to transmit this message wirelessly to another vehicle. As the onboard processor is generating the BSM, a security module is processing and preparing the security information and certificates for transmission to provide the receiving vehicle assurance that the message is valid. This security information needs to be transmitted wirelessly as well.

To *receive and interpret* a BSM, a device must be capable of receiving the BSM that is transmitted from a nearby device and it must match the method of BSM transmission (i.e., if the message is transmitted via DSRC, the receiving device must have a DSRC receiver). It also must have a computer processing unit that can decode the BSM properly. A GPS antenna and receiver are needed to verify the relative distance between the sending device and the receiving device. Lastly, the device that is receiving the BSM must also have a security module that is capable of receiving and processing the security credential information as well.

Lastly, to operate the safety applications adequately to warn drivers, a driver-vehicle interface is needed to display critical advisories and imminent alerts. This DVI may take the form of a visual heads-up display or infotainment screen displays, LEDs and blinkers located strategically around the driver's field of view, audible noises, and/or haptic feedback peripherals.

1. Components used in testing

DOT has conducted a significant amount of research on DSRC-based vehicle-to-vehicle communications. In 2012, building on this research, the Department initiated the Safety Pilot Program in Ann Arbor, Michigan, in order to collect data to be used to evaluate V2V technology in relation to light vehicle operations. The different types of DSRC-based devices, used in the vehicles that were deployed in Ann Arbor, are: (1) Integrated Vehicle Devices (OEM devices) , which were installed (integrated by OEMs) into 64 new vehicles (8 per the 8 OEMs participating in the Safety Pilot); (2) Aftermarket Safety Devices (elsewhere called "self-contained" devices), which were installed into 270 light vehicles supplied by volunteer subjects; (3) Vehicle Awareness Devices, which were installed in over 2,400 volunteer private vehicles and various fleet vehicles such as schools buses; and (4) Integrated and Retrofit Safety Devices, which were also installed in heavy trucks (19) and transit buses (3) to support later evaluation of heavy truck and transit bus safety applications.

These DSRC-based devices had varied characteristics and served different purposes in being included in the Program. The main device, an integrated vehicle device, is an electronic device that is inserted into a vehicle during its manufacture. This type of device is connected to proprietary data buses and can provide highly accurate information using in-vehicle sensors to generate the BSM. It can both broadcast and receive BSMs, as well as process the content of received messages to provide warnings and/or alerts to the driver of the vehicle in which it is installed.

As described in Section III.D.2.a), an aftermarket safety device, as used in the Safety Pilot context, is an electronic device installed in a vehicle after its original manufacture, which is capable of both sending and receiving safety messages over a DSRC wireless communications link. This type of device has a driver interface, can run V2V and V2I safety applications, and can issue audible advisories or warnings to the driver of the vehicle. Some of the devices are integrated into the vehicle's existing computer systems and are referred to as Retrofit Safety Devices (RSDs).[118] They can receive information from the vehicle data buses and on-vehicle sensors. Other devices are not connected to the vehicle's data bus. They receive the information needed to form the BSM from the device's GPS, and they can also be equipped with additional sensors to provide more accurate information for the BSM.

[118] Retrofit devices that are connected to the vehicle computer system are being used in the safety pilot on transit vehicles and trucks. See Safety Pilot Information Sheet at www.its.dot.gov/factsheets/safety_pilot_factsheet.htm (last accessed Jan. 28, 2014).

A VAD is an aftermarket electronic device installed in a vehicle without connection to vehicle systems, which is only capable of sending the BSM over a DSRC wireless communications link to alert other DSRC-equipped vehicles to its presence. Because VADs are not connected to the vehicle's computer systems, all of the information for the BSM is derived from the device's GPS.[119] Additional sensors in these devices such as accelerometers or gyros can be used to provide more accurate information for the BSM. Because VADs are not equipped with a driver interface, they are not capable of generating warnings. VADs may be used in any type of vehicle, regardless of the vehicle's age or onboard electronic systems.

2. Components required for V2V system operation

A V2V communication system requires components located in vehicles and along roadways to enable complete system operation. For a V2V system, this includes both the vehicle-based components and road side equipment (RSE) units to provide security updates and communication to the security management system. A V2I system would expand capabilities by embedding additional RSEs, potentially, in traffic signals, signs, and other infrastructure-related components. The following sections provide details on vehicle and non-vehicle based components.

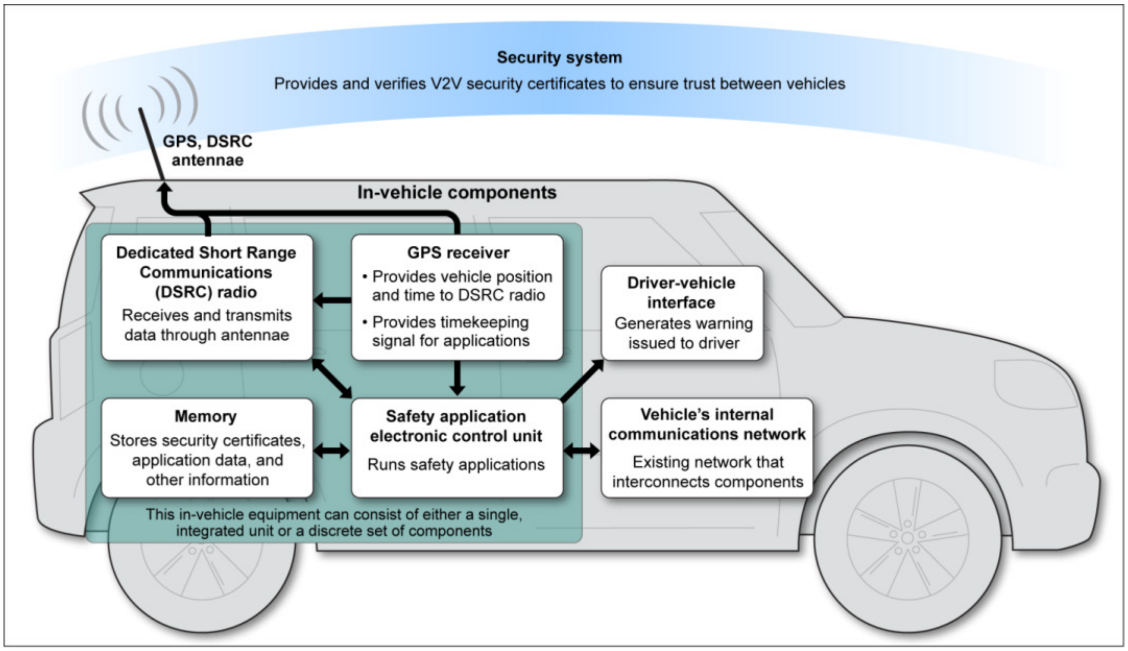
3. Vehicle-based hardware

At a minimum, V2V devices would require two DSRC radios[120] and a GPS receiver with a processor to derive information such as vehicle speed and predicted path from the device's GPS data. To improve the quality of the data that vehicle-based components could use to issue warnings, an inertial measurement unit to detect acceleration forces would be needed. In addition, a driver-vehicle interface would be essential for issuing warnings to the driver. Such warnings could be audial or visual (with the corresponding required hardware), or, for devices fully integrated into the vehicle at the time of manufacture (i.e., vehicles with Integrated Safety Systems), the warnings could potentially be haptic warnings (e.g., tightening of the seat belt, vibrating the driver's seat).

NHTSA also foresees the potential for V2V safety systems to be integrated into an existing electronic control unit(s) during large-scale production of vehicles equipped with these systems. Figure V-1 illustrates the vehicle-based components needed for an integrated V2V system that uses integrated vehicle devices. (A V2V system with ASDs would only differ in its lack of connection to the vehicle's internal communications network.)

[120] See Section V.D.2 below for more information on why NHTSA believes two DSRC radios would be necessary.

Figure V-1 In-Vehicle Components of a V2V System


Security system
Provides and verifies V2V security certificates to ensure trust between vehicles
GPS, DSRC antennae
In-vehicle components
Dedicated Short Range Communications (DSRC) radio
Receives and transmits data through antennae
GPS receiver
• Provides vehicle position and time to DSRC radio
• Provides timekeeping signal for applications
Driver-vehicle interface
Generates warning issued to driver
Memory
Stores security certificates, application data, and other information
Safety application electronic control unit
Runs safety applications
Vehicle's internal communications network
Existing network that interconnects components
This in-vehicle equipment can consist of either a single, integrated unit or a discrete set of components

Sources: Crash Avoidance Metrics Partnership and GAO.

a) Production feasibility of vehicle-based components

The Safety Pilot Model Deployment hardware consists of pre-competitive, prototype components—some that would be required for a production implementation and others that would not. For example, the extensive data acquisition systems, which are used to log driver behavior and vehicle information, collect information that is used only for the needed post-test analysis. Most likely, they would not be needed by the agency if the V2V system was deployed in mass production.

However, many components being used in the Model Deployment could be leveraged to develop products further for full scale production. In some cases, prototype components used in the Safety Pilot have the appearance and packaging of what could be a regular production device. NHTSA's current understanding, based on discussions with industry OEMs and suppliers, is that securing and preparing manufacturing facilities is the major factor to transitioning from building prototype components to ramping up to produce mass market components, and that the device in its current form is nearly production-feasible today.

A minor condition for production feasibility is the need for automotive-grade DSRC microchips for devices that would be permanently mounted in a vehicle (e.g., integrated OEM or aftermarket retrofit devices). Automotive grade components are usually certified to more stringent environmental conditions and quality (defects per parts per million) requirements than consumer electronics. Each vehicle manufacturer has its own set of specifications for the components it purchases for the vehicles it produces. Automotive grade components must be able to operate in more extreme conditions such as temperature, vibration, and electro-magnetic interference that go beyond the conditions for typical consumer grade components. The Safety Pilot employs prototype DSRC microchips that are based on consumer grade components that are custom-modified to be DSRC-capable. Actual DSRC chips will need to be developed for production and qualified as automotive grade components. As the prototype microchips are based on existing consumer grade wireless microchips with minimal modification, the agency believes feasibility for these components moving to production should not be an issue to move forward.

b) Projected availability of vehicle-based components

Discussions with equipment suppliers have indicated that there is the potential to have an adequate supply of readily available, mass-produced, internal components for a V2V device approximately 2.5 to 3 years after NHTSA moves forward with some type of regulatory action.[121]

4. Non-vehicle-based hardware

In addition to the vehicle-based V2V components, a V2V system also requires equipment to be located along roadsides and, if expanded V2I capabilities are sought, to be embedded in other infrastructure support equipment such as traffic signals or stop signs.

Roadside equipment is the term used to refer to the physical wireless communications infrastructure that supports communication between the vehicle and the SCMS, and between the vehicle and V2I applications. There are two types of RSEs with which a vehicle can communicate: RSEs that serve as a wireless communications link between the vehicle and the SCMS so that the vehicle can receive new security certificates, report misbehavior, and receive CRL updates, and RSEs that broadcast messages needed to support V2I applications. The equipment necessary to support both functions can be located within one RSE device. RSEs could employ DSRC, or could potentially use some other communications medium such as existing 3G/4G cellular networks or Wi-Fi.

a) External equipment used in Safety Pilot

There are 26 DSRC-equipped roadside units being used to support the Safety Pilot Model Deployment program. The DSRC RSEs used in the Model Deployment are all technically capable of both storing and forming messages to support V2I applications and to support communications between OBE and the SCMS.[122] Specifically, the Model Deployment program

[121] Preliminary estimates are based on confidential information provided by two suppliers.
[122] All RSEs used in the Safety Pilot Model Deployment conformed to "5.9GHz DSRC Roadside Equipment" Device Specification Version 3.0. See www.its.dot.gov/safety_pilot/pdf/T-10001-T2-05_RSE_Device_Design_Specification_v30.pdf (last accessed Feb. 7, 2014).

is evaluating DSRC RSE devices that allow vehicles to receive updated security certificates[123] and messages to support V2I applications (SPaT, curve warnings, and curve speed warnings). The Model Deployment is also evaluating the use of existing 3G/4G cellular networks to provide vehicles with updated security certificates, because DOT wanted to examine the feasibility of supporting communications between vehicles and the SCMS though an existing communications infrastructure. While it is important to note that a nationwide network of RSE DSRC devices does not exist at this time and Congress has yet to allocate funds to build such a network, existing 3G/4G cellular networks could potentially be used to support communications between vehicles and the SCMS in the event that a nationwide network of RSE devices is not available.

b) External equipment needed for widespread deployment

In a widespread deployment scenario, NHTSA expects much more communication between vehicles and the SCMS than has occurred in the context of the Safety Pilot. For communications to support the security system, the data will be exchanged between the OBE and the SCMS using the well-known Internet Protocol (IP). The basic transaction will be that the OBE will send a request message bearing the SCMS IP address to the RSE, and the RSE will forward this to the backhaul,[124] where it will eventually be routed to the SCMS following the conventional Internet routing process. It is estimated that around 19,000 roadside DSRC units would be needed to support communications between vehicles and the SCMS under the current security framework.[125]

C. Overview of software enabling system operation

V2V communications is based on the wireless exchange of messages between vehicles. The messages provide information that a device can then use to provide a warning about potential danger through a safety application. Fundamentally, the basic hardware of a DSRC device is analogous to a common radio that not only receives information but transmits data as well. As a result the "core" of a DSRC device will be the software that gives devices the "intelligence" needed to determine and transmit current vehicle conditions and perform the necessary evaluations to potentially issue a warning. At the most basic level, a device will require low-level components to both transmit and receive the basic safety message; a relatively simple operating system; connection to a driver-vehicle interface; and algorithms to control the issuance of warnings (along with continual device diagnosis).

[123] The security system used in Safety Pilot Program did not involve distribution of a CRL but used a "test" CRL to prove transmittal, receipt, and action.

[124] "Backhaul" is a term used to refer to all telecommunications infrastructure, such as fiber optic cables and routing switches, needed to support IP protocol transactions.

[125] Communications Data Delivery System Analysis for Connected Vehicles: Revision and Update to Modeling of Promising Network Options, at 31 (Booz Allen Hamilton, Inc., May 2013). [Hereafter, "BAH CDDS Final Report"]. See Docket No. NHTSA-2014-0022.

Overall, both vehicle manufacturers and consumer electronic device manufacturers have years of significant experience developing similar software for the myriad devices and products they produce. They are skilled at managing suppliers to develop these components or, in some cases, developing device software in-house as part of their core intellectual property.

V2V devices present a new challenge to the agency regarding software and potential regulatory action. NHTSA's FMVSSs are generally performance-based, but the agency has not yet attempted to regulate software using performance tests, and software is increasingly pervasive in today's vehicles. The agency will need to consider carefully how to develop appropriate tests to regulate the software-based aspects of V2V communications and safety applications. NHTSA's research program concerning vehicle automation includes research into how the agency might regulate safety-critical software.

D. Interoperability

1. Interoperability and its importance

In order for the information in a V2V communication to be useful, it must be received timely, it must be reliable, and it must be transmitted in a standard format. Vehicles participating in the V2V communications network communicate with other connected vehicles using standardized DSRC message types broadcast on a standardized network, IEEE 1609.4, over a standardized wireless layer, IEEE 802.11p.[126] DSRC provides local-area, low-latency[127] network connectivity, and is generally intended to support broadcast messaging between vehicles and between vehicles and roadside access points. It is a variant of Wi-Fi that allows nearly instantaneous network connections, as well as broadcast messaging that requires no network connection. It uses 75 MHz of spectrum located in the 5.85 to 5.925 GHz frequency band.[128] Vehicles currently use channel 172 to transmit messages that support safety of life applications. Interoperability, in short, is the ability for different devices using V2V systems sourced, manufactured, and installed by various OEMs and aftermarket retailers to communicate with each other in a reliable and timely manner. If devices from different sources fail to "speak the

[126] See Section V.D.1.c) below for more information on these standards.

[127] Latency is a measure of the time delay experienced in a system, usually between the sending, and subsequent reception, of information. In communications, the lower limit of latency is determined by the physics of transmitting a message, where the medium (radio, fiber optics, copper wiring, etc.) being used for communications can affect transmission speed. In addition, delays can also be incurred by the addition of data handling protocols, message routing and switching, and a few other smaller factors. For more information, see www.o3bnetworks.com/media/40980/white%20paper_latency%20matters.pdf (last accessed Feb. 25, 2014). DSRC can be considered to be low latency because it consists of point to point communication over very short distances (less than 300 m) with relatively few messaging protocol requirements using radio (in air, radio transmits information at approximately light speed).

[128] This is usually referred to as the 5.9 GHz band.

same language," then the system as a whole will not be "interoperable," and will consequently degrade and break down.

a) Communication between vehicles

V2V communications consists of two types of messages: safety messages and certificate exchange messages. The safety messages are used to support the safety applications, and the certificate exchange messages ensure that the safety message is from a trusted source. The safety messages are transmitted in a standardized format so that they can be read by all other vehicles participating in the network. To satisfy this requirement, each DSRC-equipped vehicle would need to broadcast and receive safety messages in a standardized format and specified performance level in terms of characteristics like accuracy and range.[129] Additional details on standards related to V2V can be found in Section V.D.1.c). The safety messages include information about the vehicle's behavior such as the vehicle's GPS position, its predicted path, its lateral and vertical acceleration, and its yaw rate. The messages are time-stamped so the receiving vehicle knows when the message was sent. This information can be used by other vehicles for a variety of crash avoidance applications.

NHTSA's current research is based on the assumption that the V2V system will use a Public Key Infrastructure (PKI) to authenticate messages, so that other vehicles will trust the m.[130] PKI uses certificates to inform a receiving device that the message is from a trusted source, and it uses cryptography to send encrypted message content. For V2V communications, BSM messages are trusted but not encrypted, while messages that contain security information (e.g., certificates) are trusted and the contents encrypted.[131]

The security system currently being researched for V2V would use a type of cryptography known as "asymmetric cryptography."[132] In asymmetric cryptography, there are two keys that are mathematically linked in such a way that what is encrypted with one key can only be decrypted with the other. Although the keys are mathematically linked, it is extremely difficult to derive one key based on knowledge of the other. This property allows one key, the "public key," to be widely distributed while the other key, the "private key," is held only by the owner. Asymmetric cryptography (both encryption and decryption) is computationally harder

[129] Such as, for example, the parameters as defined in SAE J2735.

[130] BAH CDDS Final Report, at 9.

[131] Certificates decrease latency as compared to encrypting the BSM itself; encrypting the BSM, sending it, and the n the other vehicle receiving, decrypting, and translating it could take longer than what would support effective functioning of the safety applications.

[132] Also known as public key encryption.

than symmetric cryptography and is one of the reasons many security experts believe asymmetric cryptography to be more secure.[133]

Many Internet security protocols use asymmetric cryptography as the basis for their infrastructure. Secure socket layers/transport layer security (SSL/TLS),[134] the protocol used in most secure online transactions, uses asymmetric encryption to authenticate the server to the client, and optionally the client to the server. Asymmetric cryptography is also used to establish a session key. The session key is used in symmetric algorithms to encrypt the bulk of the data. This combines the benefit of asymmetric encryption for authentication with the faster, less processor-intensive symmetric key encryption for the bulk data.[135] The secure form of Hypertext Transfer Protocol is HTTPS, which operates as a PKI system and uses SSL. SSL\TLS also operates on its own as a PKI system, independently of HTTPS. For a further discussion of symmetric and asymmetric cryptography, please see Section IX.

b) Vehicle-to-Vehicle Message Sets

For vehicle communication to succeed among OEM-installed in-vehicle devices and aftermarket devices, communication messages must be standardized so that the devices speak the same language. SAE J2735 is intended to help address this purpose so that all V2V safety applications are built around a common framework. SAE J2735 defines the design specifications for the safety messages, including specifications for the message sets,[136] data frames,[137] and data elements.[138]

[133] Symmetric encryption is a very common encryption scheme that many use routinely, possibly without knowing the exact name for it. In fact, before 1973, all known encryption algorithms were symmetric. If the reader has ever "password protected" a .zip file, where the same passphrase (key) is used to both lock and unlock the .zip file, then symmetric encryption was used. Similarly, a "Secret Decoder Ring," where a ring containing 2 sets of alphanumeric strings (located on different halves of the ring) can be rotated relative to each other to develop an encryption scheme, is another example of symmetric cryptology, as the orientation of the two sides of the ring used to encrypt a message is also needed to decode the secret message. One challenge with symmetric cryptography is controlling key distribution so that the key does not fall into unintended hands.

[134] Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a protocol primarily used to encrypt confidential data sent over an insecure network, such as the Internet.

[135] For an overview of SSL/TLS encryption, see http://technet.microsoft.com/en-us/library/cc781476(v=ws.10).aspx (last accessed Jan. 28, 2014).

[136] As defined in SAE J2735, a message is a well-structured set of data elements and data frames that can be sent as a unit between devices to convey some semantic meaning in the context of the applications. A message set is a collection of messages based on the ITS functional-area to which they pertain.

[137] As defined in SAE J2735, from a computer science perspective, data frames are viewed as logical groupings of other data frames and of data elements to describe "structures" or parts of messages used in SAE J2735 and other standards. A data frame is a collection of two or more other data concepts in a known ordering. These data concepts may be simple (data elements) or complex (data frames).

[138] As defined in SAE J2735, a data element is a syntactically formal representation of some single unit of information of interest (e.g., a fact, proposition, observation) with a singular instance value at any point in time,

(1) The Basic Safety Message

The currently-published version of SAE J2735, published in November 2009, is the second version of the standard. It specifies 15 message sets, with Basic Safety Message the most important one.[139]

As explained above, the BSM is used to exchange safety data regarding vehicle state. The message is broadcast routinely to surrounding vehicles with a variety of data content. The BSM is split into two parts to guarantee that the core information for vehicle safety (Part I) has priority and is transmitted more often. It also minimizes the amount of data communicated (most of the time) between devices, helping to reduce channel congestion.

BSM Part I contains the core data elements, such as vehicle position, speed, heading, brake system status, and vehicle size. Details of the BSM Part I content are found in Table V-1.

about some entity of interest (e.g., a person, place, process, property, object, concept, association, state, event). A data element is considered indivisible.

[139] For more information on the other message sets defined in SAE J2735, see www.sae.org/standardsdev/dsrc/ (last accessed Jan. 28, 2014).

Table V-1 Contents of BSM Part I[140]

Part I	
Data Frame (DF)	**Data Element (DE)**
Position (DF)	
	Latitude*
	Elevation*
	Longitude*
	Positional accuracy*
Motion (DF)	
	Transmission state*
	Speed
	Steering wheel angle
	Heading*
	Longitudinal acceleration*
	Vertical acceleration
	Lateral acceleration
	Yaw rate*
	Brake applied status
	Traction control state
	Stability control status
	Auxiliary brake status
	Brake status not available
	Antilock brake status
	Brake boost applied
Vehicle size (DF)	
	Vehicle width
	Vehicle length
	*Required in Safety Pilot Model Deployment

BSM Part II contains a set of data elements that can vary by vehicle model. Part II data are only broadcast when an event happens that changes the Part II data content. Part II is then appended to Part I data and broadcast; otherwise, only Part I data is transmitted in the BSM. The content of Part II data depends on the triggering events – not all Part II data will be transmitted simply because *some* Part II data is transmitted. For example, when a vehicle activates ABS, a

[140] Based on SAE 2735-2009. For more information, see "Vehicle Information Exchange Needs for Mobility Applications: Version 2.0, Revised Report (Aug. 1, 2012, FHWA-JPO-12-021) at http://ntl.bts.gov/lib/46000/46000/46089/Final_PKG_FHWA-JPO-12-021_508_PDF.pdf (last accessed Jan. 28, 2014).

data element named "ABS activated" is set and the vehicle's BSM transmissions include a Part II message indicating that its ABS is active.[141] This event type data is being used in the Safety Pilot Model Deployment to support the EEBL safety application. Consequently, Part II data are transmitted less frequently. Details of the BSM Part II content are found in Table V-2.

Table V-2 Contents of BSM Part II[142]

Part 2 (all elements optional, sent according to criteria to be established)	
Data Frame (DF)	**Data Element (DE)**
Vehicle safety extension (DF)	
	Event flags (DE) – A data element consisting of single bit event flags:
	Hazard lights
	Intersection stop line violation
	ABS activated
	Traction control loss
	Stability control activated
	Hazardous materials
	Emergency response
	Hard braking
	Lights changed
	Wipers changed
	Flat tire
	Disabled vehicle
	Air bag deployment
Path history (DF)	
	Full position vector (DF)
	Date and time stamp (DE)
	Longitude (DE)
	Latitude (DE)
	Elevation (DE)
	Heading (DE)
	Transmission and speed (DF) – same as in Part 1
	Positional accuracy (DE)
	Time confidence (DE)
	Position confidence set (DF)
	Position confidence (DE)
	Elevation confidence (DE)
	Speed and heading and throttle confidence (DF)

[141] For the same event, the traction control loss, stability control activated, and the hard braking flags may be set as well depending on the event type and causation.

[142] *See supra* note 140.

	Speed confidence (DE)
	Heading confidence (DE)
	Throttle confidence (DE)
	GPS status (DE)
	Count (DE) – number of “crumbs” in the history
Crumb data – set of one of 10 possible path history point set types, consisting of various combinations of:	
	Latitudinal offset from current position (DE)
	Longitudinal offset from current position (DE)
	Elevation offset from current position (DE)
	Time offset from the current time (DE)
Accuracy (DF) – See J2735 standard for more information	
	Heading (DE) – NOT an offset, but absolute heading
Transmission and speed (DF) – same as in Part 1, NOT an offset	
Path Prediction (DF)	Radius of curve (DE)
	Confidence (DE)
RTCM Package (DF) – RTCM (Radio Technical Commission for Maritime Services) is a standardized format for GPS messages, including differential correction messages.	
Full position vector (DF) – see full contents above under Path history	
RTCM header (DF)	
	GPS status (DE)
	Antenna offset (DE)
	GPS data – see SAE J2735 and RTCM standards for more information
Vehicle status (DF)	
	Exterior lights (DE)
	Light bar in use (DE)
Wipers (DF)	
	Wiper status front (DE)
	Wiper rate (front) (DE)
	Wiper status rear (DE)
	Wiper rate (rear) (DE)
Brake system status (DF) – same as in Part 1	
	Braking pressure (DE)
	Roadway friction (DE)
	Sun sensor (DE)
	Rain sensor (DE)
	Ambient air temperature (DE)
	Ambient pressure (DE)
Steering, sequence of:	
	Steering wheel angle (DE)
	Steering wheel angle confidence (DE)
	Steering wheel angle rate of change (DE)
	Driving wheel angle (DE)

Acceleration set (DF) – same as in Part 1	
	Vertical acceleration threshold (DE)
	Yaw rate confidence (DE)
	Acceleration confidence (DE)
Confidence set (DF)	
	Acceleration confidence (DE)
Speed confidence (speed, heading, and throttle confidences (DF)	
	Time confidence (DE)
Position confidence set (DF)	
	Steering wheel angle confidence (DE)
	Throttle confidence (DE)
Object data, sequence of:	
	Obstacle distance (DE)
	Obstacle direction (DE)
	Time obstacle detected (DE)
Full position vector (DF) – see contents under path history	
	Throttle position (DE)
Speed and heading and throttle confidence (DF) – same as above under "Full position vector"	
	Speed confidence (DE) – same as above under "Speed and heading and throttle confidence"
Vehicle data (referred to as a "complex type" in J2735, rather than an element or frame)	
	Vehicle height (DE)
	Bumper heights (DF)
	Bumper height front (DE)
	Bumper height rear (DE)
	Vehicle mass (DE)
	Trailer weight (DE)
	Vehicle type (DE)
Vehicle identity (DF)	
	Descriptive name (DE) – typically only used for debugging
	VIN string (DE)[143]
	Owner code (DE)[144]
	Temporary ID (DE)
	Vehicle type (DE)

[143] SAE J2735 is a data dictionary that defines potential data elements for a number of messages (e.g., V2V, V2I, I2V, probe messages). Data elements are currently defined within the standard for a broad range of future safety and non-safety application messages. The vehicle identification data elements are defined for communication between emergency and fleet vehicles for applications such as traffic signal preemption, in which the road side equipment (traffic signal controller) requires confirmation of the identity of the vehicle.

[144] Id.

Vehicle class (drawn from ITIS code standard)	
J1939 data (DF)	
Tire conditions (DF) – see J2735 standard for list of data elements	
Vehicle weight by axle (DF) – see J2735 standard for list of data elements	
	Trailer weight (DE)
	Cargo weight (DE)
	Steering axle temperature (DE)
	Drive axle location (DE)
	Drive axle lift air pressure (DE)
	Drive axle temperature (DE)
	Dive axle lube pressure (DE)
	Steering axle lube pressure (DE)
Weather report, defined as a sequence of the following:	
	Is raining (DE) – defined in NTCIP standard
	Rain rate (DE) – defined in NTCIP standard
	Precipitation situation (DE) – defined in NTCIP standard
	Solar radiation (DE) – defined in NTCIP standard
	Mobile friction (DE) – defined in NTCIP standard
	GPS status (DE)

The SAE J2735-2009 standard contains only technical design specifications for the BSM, so in order to specify the usage of the BSM as defined in J2735, such as the transmission rate, power level, data integrity, etc., another set of standards for the minimum communication performance requirements for the BSM must be developed. The SAE DSRC Technical Committee is currently in the process of developing minimum performance requirements for BSM communication, named SAE J2945-1, based on the knowledge gained through the CAMP VSC-A project, the V2V-Interoperability project and the Safety Pilot Model Deployment.

Standards Need V-1 SAE Standards Maturity

Standards Need:	SAE J2945 & SAE J2735
Description:	Currently these standards are in development. Timeframe for completion and impact on future regulatory is to be determined by outside organizations

(2) Other options besides the BSM

The BSM is developed specifically for vehicle-to-vehicle communication, to allow devices from different OEMs and suppliers to interact in the system. This dedicated message was cooperatively developed as a standard involving both U.S. and EU representatives. Currently there is no planned alternative to using the collaboratively-developed BSM to transmit and receive vehicle information for use in safety applications. The BSM has been developed and refined over the course of the last decade specifically to support common V2V communication.

(3) Current maturity level of V2V message sets

The BSM is developed for vehicle-to-vehicle communication to allow devices from different OEMs, suppliers, and aftermarket device manufacturers to communicate with each other for V2V and V2I applications. The preliminary design specifications for the BSM are contained in the current version of SAE J2735 and preliminary minimum performance requirements will be contained in SAE J2945 when finalized.

Over the course of the Safety Pilot, it was identified that the current published J2735-2009 will not support interoperability as a stand-alone document, due to ambiguities in the standard that were causing OEMs and suppliers to interpret the standard and define the BSM inconsistently. During the V2V-I project, future revision items were identified for various DSRC standards for further improvement for interoperability.

Nevertheless, the vehicles in the Safety Pilot Model Deployment program are transmitting BSMs to each other and using those BSMs to activate safety applications. Results from the Safety Pilot and the CAMP Interoperability project will be used to further develop performance requirements for the BSM.

c) *Technical Standards related to V2V*

(1) Development and use of technical standards related to V2V

To support wireless communication between two or more vehicles and/or between vehicles and fixed or nomadic devices, a set of ITS V2X Cooperative System Standards are needed. These standards ensure that vehicles are interoperable and can interpret messages received from these other sources. The current set of cooperative system standards is found in Table V-3.

Table V-3 Cooperative System Standards for V2V Communications

Cooperative System Standards
IEEE 802.11p-2010
IEEE P1609.0/D5.8
IEEE 1609.2-2013
IEEE 1609.3-2010
IEEE 1609.4-2010
IEEE 1609.12-2012
SAE J2735, Version 2
SAE J2945.1, Version 1

These cooperative system standards were developed specifically to support V2V and V2I wireless interfaces. They establish a wireless link for V2V and V2I communications (IEEE 802.11p), establish protocols for information exchange across the wireless link (IEEE 1609.x), and define message content for communicating specific information to and from equipment and devices via DSRC (SAE J2735 and SAE 2945.x) or other communications media.

OST-R's Intelligent Transportation Systems Joint Program Office's Standards Program funds and manages ITS cooperative system standards efforts in support of V2V and V2I technologies. The content of these standards is developed collaboratively with contributions from diverse stakeholders. The VSC-A and CAMP projects have made significant contributions to many of the standards described above.[145]

The cooperative system standards are, to be clear, consensus standards voluntarily followed by industry, as compared with regulations issued by a government agency like NHTSA. NHTSA has no authority to enforce standards that it does not promulgate. However, if NHTSA eventually decided, for example, to mandate DSRC (in order to enable certain safety applications), part of that mandate would likely include requirements that DSRC devices be interoperable in order to ensure that they function properly. Part of ensuring interoperability is making sure that DSRC works, exchanges information the same way every time, and uses standardized messages. Each of the cooperative system standards discussed in this section facilitates some part of DSRC operation, so NHTSA may look to these standards and incorporate elements of them if the agency decides to pursue a DSRC mandate.

(2) SAE J2735 - DSRC Message Set Dictionary

The SAE J2735 standard specifies message sets, data frames, and data elements that make up messages/dialogs specifically for use by applications intended to use the 5.9 GHz DSRC for WAVE communications systems. The messages for V2V safety applications are defined in SAE J2735 as the BSM parts 1 and 2 (detailed information for BSM part 1 and 2 can be found in Section V.D.1.b) other parts of SAE J2735 define the message sets for other ITS applications, such as weather and mobility.

SAE's DSRC Technical Committee issued the current published version of J2735 in November 2009, as version 2 of the standard (referred to as J2735-2009 or version 2 of J2735). At present, the SAE J2735-2009 standard has been implemented for testing and experimental

[145] Specifically, VSC-A and CAMP have contributed to the development of SAE J2735 (DSRC Message Set Dictionary); SAE J2945.1 (DSRC BSM Minimum Performance Requirements); IEEE 1609.0 (Architecture); IEEE 1609.2 (Security Services); IEEE 1609.3 (Networking Services); IEEE 1609.4 (Multi-Channel Operation); IEEE 1609.12 (Identifier Allocations); and IEEE 802.11p (Wireless Access in Vehicular Environments (WAVE)).

purposes only, with no wide-scale deployment. As indicated in the discussion on maturity of the BSM message sets, revisions will be necessary to the J2735-2009 standard to support widespread deployment of a V2V system. Current expectations are that a revised standard will be published in late 2014.

(3) SAE J2945 - DSRC Minimum Performance Requirements

The SAE J2945.1 standard specifies the minimum communication performance requirements of the DSRC Message sets and the necessary BSM data elements to support V2V safety applications. The J2945.1 standard is part of a future family of J2945.x standards.[146] The current draft standard consists of multiple sections with each section describing the specific requirements for using the BSM for V2V safety applications. The content of the current draft J2945.1 is listed in Table V-4. To date, an early rough draft version of J2945.1 exists and it only includes the minimum communication performance requirements for the BSM message. It is anticipated the published version of J2945 will be available in late 2014.

Table V-4 Contents of Draft J2495.1 Standard[147]

Section	Section Title
1	Scope
2	References
3	Common Section
3.1	PSID Assignment
3.2	SSP (Service Specific Priority)
3.3	Message Priority Mapping
4	DSRC BSM Minimum Performance Requirements
4.1	Power option
4.2	DSRC Communication Channel Operation for BSM (or V-V Safety)
4.3	BSM Transmission Interval Requirements
4.4	Transmission Power Requirements
4.5	Security and Privacy Requirements
4.6	GPS configuration Requirements
4.7	Data Frame/Elements Requirements
5	Future Consideration
6	Application-level Requirements?
7	Other stuff*

*Note: [sic], per the current draft form of the standard

[146] Each J2945.x standard will provide the critical interface information needed to support one or more applications. Associated design specifications for data frames and data elements for the respective J2945.x standards are defined in the SAE J2735-2009 (DSRC Message Set Dictionary standard) and will also be included in future published versions of J2735.

[147] This outline is from the current draft J2945.1, and will likely change as the standard is further developed.

(4) IEEE 1609 - Standard for Wireless Access in Vehicular Environments (WAVE)

The IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) define an architecture and a complementary, standardized set of services and interfaces that collectively enable secure V2V and V2I wireless communications. Together these standards are designed to provide the foundation for a broad range of applications in the transportation environment, including vehicle safety, automated tolling, enhanced navigation, traffic management, and others.

(5) IEEE 1609.0 - Guide for Wireless Access in Vehicular Environments (WAVE) Architecture

IEEE 1609.0 is not a standard, but an architecture guide. It provides the descriptions of each of the full-use IEEE 1609 standards and their relationships to other relevant standards (such as IEEE 802.11), and includes guidance on how they should work together. The protocol architecture, interfaces, spectrum allocations, and device roles are all described. The guide is intended for organizations that will implement DSRC, such as State departments of transportation, automobile and original equipment manufacturers, aftermarket equipment makers, application developers, and standards developers. The guide describes the history of the development of the IEEE 1609 standards that includes the ITS architecture, the FCC allocation of the spectrum, and the original standards activity in the development of ASTM 2213-03. Also described are the IEEE 1609 trial use standards and IEEE 802.11. There is also a summary of the deployment history of DSRC devices in an annex to the guide. Overall WAVE system operations are described and an example system configuration is provided based on the published full use standards. The protocol architecture is described, including a description of the data plane,[148] the management plane,[149] and how WAVE messages and IPv6 messages are treated. Internal and external interfaces are described. The channel configurations, channel types and allowed operations are detailed according to the current FCC rules as well as a description of how the control channel and the service channels can be configured. The guide also explains channel coordination, channel switching, and time synchronization.

(6) IEEE 1609.2 - Security Services for Applications and Management Messages

The safety-related content of WAVE applications, and particularly vehicle safety applications, makes it necessary to protect messages from attacks such as eavesdropping, spoofing, alteration, and replay. Recipients of safety messages have to be assured that the messages they receive are authentic and are sent by a source authorized to transmit those

[148] The data plane, also known as the user plane, forwarding plane, carrier plane, and/or bearer plane, is the part of a network architecture that handles user traffic.
[149] Part of a network architecture which provides an administrative interface to the system.

messages. Additionally, the fact that the WAVE technology may be implemented in communication devices in personal vehicles as well as in other portable devices whose owners may have some expectation of privacy means that the security services may need to be designed to avoid, for example, revealing personal, identifying, or linkable information to unauthorized parties in systems where PII may be involved. This standard describes security services for WAVE management messages and application messages designed to meet these goals. This standard was intended to be used primarily for DSRC.

(7) IEEE 1609.3 - Networking Services

IEEE 1609.3 specifies how various message types (e.g., WAVE Short Messages, WAVE Service Advertisements, and WAVE Routing Advertisements) are assembled, packaged, and handled between an application and IEEE 1609.4 for transmission or upon reception. It describes how to build, route, process, and interpret WAVE low latency messages, as well as messages based on other well-known protocols such as the User Datagram Protocol and Internet Protocol Version 6 (IPv6). The standard includes information on what messages go on the control channel, what messages go out on the service channels, advertising specific services, authenticating the messages, accessing applications hosted on an external network (e.g., the Internet) and methods for how this can be accomplished.

(8) IEEE 1609.4 - Multi-Channel Operations

This standard describes multi-channel radio operations for WAVE. It is used in conjunction with other IEEE 1609 standards and IEEE 802.11-2012 to implement DSRC communications in the 5.9 GHz frequency band. WAVE operates using IEEE 802.11 outside the context of a basic service set. In order to implement functions such as user priority access to the media, routing data packets on the correct channel with the desired transmission parameters, and the ability to coordinate switching between the control channel and service channels, additional functions are required between the IEEE 802.11 medium access control and the Logical Link Control. This standard specifies how these functions are implemented.

(9) IEEE 1609.12 - Identifier Allocations

WAVE is specified in the IEEE 1609 family of standards, within which a number of identifiers are used. IEEE 1609.12 describes the format and use of the provider service identifier, and indicates identifier values that have been allocated for use by WAVE systems.

(10) IEEE 802.11p-2012 - Medium Access Control and Physical Layer Specifications for WAVE

IEEE 802.11 is a set of standards that specify the physical layer for implementing wireless local area network using Wi-Fi bands. The base version of the standard was released in 1997 and has had subsequent amendments. IEEE 802.11 is approximately 2,800 pages long, but only certain parts of the standard are required for implementing DSRC operating at 5.9 GHz for

V2V communications. IEEE 802.11p is an approved amendment to 802.11 standards to add WAVE that is required to support ITS applications. In March 2012, IEEE published the latest version of this standard, 802.11p-2012, which includes all the amendments to this standard published prior to 2012.

The purpose of this standard is to describe the operation of what are commonly known as Wi-Fi devices, including devices such as the wireless routers and the transceivers in computers. To accommodate the rapid exchange of trajectory information between vehicles traveling at high speed, IEEE 802.11p was amended to enable operation without setting up a basic service set. It allows security services, such as authentication, to be provided by other standards. It describes adjacent channel and alternate adjacent channel interference criteria and transmission masks corresponding to requirements of the FCC rules for DSRC. The entire standard applies to V2V and V2I communications, because it defines the structure for how devices should communicate using the 5.9 GHz frequency band but there are no performance criteria or test procedures described in this amendment.

(11) Maturity of the standards

Table V-5 describes the standards representing the core cooperative system standards, in particular those that support V2V and V2I. While versions of these standards have already been developed and published, some are currently undergoing revision to support evolving needs such as the current Safety Pilot Model Deployment activity.

Table V-5 ITS V2X Cooperative System Standards Latest Publication and Current Status

Standard	V2V Relevance	Latest Publication Date	Current Status
IEEE 802.11p-2010	DSRC-specific Wi-Fi device operations	July 2010	Finalized and published.
IEEE P1609.0/D5.8	Guide to other 1609 standards	Not yet published.	In sponsor ballot[150]
IEEE 1609.2-2013	Security	April, 2013	Finalized and published.
IEEE 1609.3-2010	Data exchange/message structure	December, 2010	Finalized and published.
IEEE 1609.4-2010	Channel switching modes	February, 2011	Finalized and published.
IEEE 1609.12-2012	Message identification	September, 2012	Finalized and published.
SAE J2735, Version 2	Basic safety message elements	November 19, 2009	Revision underway and expected to be published in late 2014.
SAE J2945.1, Version 1	Basic safety message requirements		No published version yet. Expected to be published in late 2014.

d) Relative Positioning

Relative positioning is a critical system function/element used to enable V2V safety applications. The essential function of the safety applications, their ability to warn the driver of an impending collision, depends on the ability of the automobiles within DSRC range to report their GPS positions to each other with confidence in their accuracy. GPS positioning matters because two interacting devices need to understand where they are in relation to each other.

Relative positioning is calculated by the difference in the reported GPS position between two vehicles in close proximity. The quality of a relative positioning solution between two cars depends on how accurate the two separate GPS positioning were.[151]

[150] For a description of the IEEE ballot process, see http://standards.ieee.org/develop/balloting.html (last accessed Jan. 9, 2014).

[151] Several different modes of absolute positioning have been investigated in the positioning research performed by CAMP, including standalone GPS, Wide Area Augmentation System (WAAS), and Real Time Kinematic (RTK). WAAS is an augmented GPS that uses ground reference stations to measure deviations from ground truth in the GPS signal and provide corrections to the geostationary WAAS satellites over the continental United States. Although WAAS specifications call for a position accuracy of 7.6 m or better 95 percent of the time, actual accuracy performance has typically been better than 1.0 m lateral accuracy and 1.5 m vertical accuracy. RTK functions on the principle of examining the difference in the phase of the carrier wave of the GPS signal between two reference stations (fixed or mobile). This difference is used to improve the raw GPS calculated distance between the stations. While RTK has the potential of high accuracy with errors measured down to a few centimeters, it comes in as more

Absolute positioning by itself might seem more useful to V2V communications, insofar as one might think that V2V-based safety applications would have the best chance of warning a driver correctly given the most precise information possible about the driver's location and the location of other vehicles. However, relative positioning has an inherent benefit as applied to V2V communications, as it relieves the burden of correcting for absolute positioning that would require additional communication with a RSE for each GPS location transmission, which would in turn require a comprehensive infrastructure network.

Error/biases in GPS raw measurements exist and are caused by natural effects and are almost identical over a geographic area. These natural biases are cancelled out in a relative positioning scheme performed over DSRC ranges. Using the relative positioning approach allows vehicles to calculate their position in relation to each other with a high degree of confidence, assuming that they have the same bias. The ability of a vehicle to determine its position in relation to other vehicles, rather than to determine its absolute position on the Earth, together with the other information transmitted in the BSM, is what is necessary to support the safety applications.

2. Current maturity level of V2V wireless communication channels

a) Securing a dedicated spectrum

It is widely accepted that V2V communications have a specific home in the wireless spectrum, but whether that home is sufficiently protected against intrusion that might impair the effectiveness of safety applications enabled by V2V is less clear at present. In 1999 the FCC allocated 75 MHz in support of the Intelligent Transportation Systems[152] on a primary basis. While this is referred to as a dedicated spectrum, it should be noted there are other allocations in this band, including the Fixed Service Satellite (co-primary) and Amateur Radio (secondary). Additionally, the lower 25 MHz overlaps the Industrial, Scientific, and Medical (ISM) band. Government Radiolocation is authorized on a primary basis as well. In February of 2004, the FCC released another Report and Order setting forth licensing and service rules for DSRC services. In 2006, the FCC released an Amendment of the Commission's Rules[153] that, among

costly in terms of computational and bandwidth requirement. S*ee:* VSC 2 Consortium, "Vehicle Safety Communications – Applications (VSC-A) Final Report: Appendix Volume 2 Communications and Positioning," Report No. DOT HS 811 492C, September 2011, at www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 28, 2014). [Hereafter, "VSC-A Final Report: Appendix Volume 2"].

[152] Amendment of Parts 2 and 90 of the Commission's Rules to Allocate the 5.850-5.925 GHz Band to the Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Services (ET Docket No. 98-95) at http://transition.fcc.gov/oet/dockets/et98-95/ (last accessed Jan. 9, 2014).

[153] Federal Communications Commission, Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz band (71 Fed. Reg. 52747, Sept. 7, 2006) at www.gpo.gov/fdsys/pkg/FR-2006-09-07/pdf/FR-2006-09-07.pdf (last accessed Feb. 18, 2014).

other things, designated channel 172 exclusively for vehicle-to-vehicle safety communications for accident avoidance and mitigation, and safety of life and property applications. The amendment also designated Channel 184 exclusively for high-power, longer-distance communications for public safety applications involving safety of life and property, including road intersection collision mitigation. These FCC decisions established DSRC as the incumbent in the band on a co-primary basis with the Fixed Service Satellite, and the FCC's continued recognition of this highlights the allocation of this spectrum for ITS.

In 2003, DOT announced the VII Proof of Concept initiative. At this point efforts shifted slightly from R&D into Test and Evaluation (T&E). This has continued for a number of years, culminating in the Safety Pilot. Data from the V2V Safety Application Research and the Safety Pilot will support a decision concerning the DSRC technology and if the technology can be used to address motor vehicles crashes.

The importance of DSRC has not been lost over the many years it has taken to develop and test it. In the latest 5 GHz NPRM, the FCC again notes the need to protect DSRC when they asked "what types of sharing technology or techniques could be used to protect non-radar systems, such as the DSRCS which includes both road side units (RSU-fixed) and on board units (OBU-mobile) operating under a primary allocation."[154]

b) Existing signal interference issues

Signal interference can pose challenges to V2V communication if other devices are operating at the same frequency as DSRC devices and preclude the transmission or reception of messages that could impact the effectiveness of safety applications. Existing signal interference deals with what devices are already using the signal and how the addition of devices using the same frequency (signal) would disrupt the signals of any existing devices operating at the same frequency. Early in the development of DSRC, the Institute for Telecommunication Sciences, the research arm of the National Telecommunication and Information Administration, was contracted to perform analysis work on signal interference by the Federal Highway Administration. Two reports are notable. The first report tested European and Japanese DSRC devices against DOD radar systems in a laboratory setting (the United States had nothing to test at that point in time).[155] The second examined the occupancy of the DSRC band as well as adjacent bands, meaning what other users and/or existing services occupy the band or nearby

[154] Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) devices in the 5 GHz Band (ET Docket 13-49) at http://apps.fcc.gov/ecfs/comment/view?id=6017164516 (last accessed Jan. 9, 2014).

[155] Electromagnetic Compatibility Testing of a Dedicated Short-Range Communication (DSRC) System that Conforms to the Japanese Standard (Nov. 1998, NTIA Technical Report TR-99-359) at www.its.bldrdoc.gov/publications/details.aspx?pub=2390 (last accessed Jan. 28, 2014).

adjacent bands that could leak into the 5.9 GHz band.[156] The testing with European and Japanese devices showed that "when combined with the additional isolation achieved by antenna alignment (estimated to be 40 dB), the engineers found that all of the existing 5-GHz radars (other users/services in the 5 GHz band)[157] should be compatible with the DSRC system that was tested [in a worst case scenario] for extremely small separation distances (several meters or less)." Based on these findings, the agency believes interference should be minimal and not present a major impact on the effectiveness of the system.

The second report noted that interference from the Fixed Service Satellite (FSS)[158] to DSRC is possible. Typically, the FSS uplinks are in remote and rural locations. These earth-based facilities use a high-powered uplink to transmit data to geostationary satellites, predominantly over the eastern Atlantic or mid to eastern Pacific Oceans. Their primary function is trans-ocean communications and there are relatively few around the country. An in-band sharing agreement was developed and submitted to the FCC several years ago. In essence, it calls for new sites to be coordinated such that incumbents have priority. This is a standard approach for co-primary allocations. The FCC has not yet acted on the agreement.

c) Current status of the spectrum

On June 28, 2010, President Obama directed the Secretary of Commerce to work with the FCC to identify and make available 500 megahertz of spectrum over the next 10 years for wireless broadband use. On February 22, 2012, the President signed the Middle Class Tax Relief and Job Creation Act of 2012 into law. The Act requires the Assistant Secretary of Commerce (through NTIA), in consultation with the Department of Defense (DoD) and other impacted agencies, to evaluate spectrum-sharing technologies and the risk to Federal users if Unlicensed-National Information Infrastructure (U-NII) devices were allowed to operate in these bands.

The most common types of U-NII devices include those that use Wi-Fi communication. These devices, in general, operate without a license, but are not supposed to interfere with licensed devices, and have no interference protection.[159] The NTIA was required to issue a report eight months after enactment (October 22, 2012) on the portion of the study on the 5.350-5.470

[156] Measured occupancy of 5850-5925 MHz and adjacent 5-GHz spectrum in the United States (Dec. 1999, NTIA Technical Report TR-00-373) at www.its.bldrdoc.gov/publications/2404.aspx (last accessed Jan. 28, 2014).

[157] *Id*.

[158] Fixed Service Satellite (FSS) is the official classification for geostationary communications satellites that provide broadcast feeds to television stations, radio stations, and broadcast networks. FSSs also transmit information for telephony, telecommunications, and data communications. For more information, see www.hq.nasa.gov/webaccess/CommSpaceTrans/SpaceCommTransSec3/CommSpacTransSec3.html#3_1_3 (last accessed Feb. 25, 2014).

[159] The risk with these devices, however, is that they may be easily modified in ways that could result in them interfering with DSRC operation. Because they are unlicensed, moreover, it would be difficult to enforce against modified devices causing such interference. This continues to be an area of concern to NHTSA.

GHz band. The Act requires the report on the portion of the study on the 5.850-5.925 GHz band no later than 18 months after enactment (August 22, 2013). NTIA published in January 2013 the results of their initial study evaluating known and proposed spectrum-sharing technologies and the risk to Federal users if the FCC allows U-NII devices to operate in the 5.850-5.925 GHz band.[160] The NTIA report identified a number of risks to FCC-authorized stations operating DSRC systems for ITS in the 5.850-5.925 GHz band and suggested mitigation strategies to explore.

On April 10, 2013, the FCC published in the *Federal Register* its NPRM to revise Part 15 of its Rules to permit U-NII devices in additional portions of the 5 GHz spectrum, including the 5.850-5.9250 GHz, so as to "increase wireless broadband access and investment."[161] While the FCC NPRM proposes permitting U-NII devices in the 5.850-5.9250 GHz band, DSRC, as the incumbent, would retain its primary allocation of the band – U-NII devices would have to operate on a non-interfering basis under the FCC Part 15 Rules.[162] In June 2013, at the request of DOT, NTIA forwarded to the FCC the comments and concerns that DOT expressed relating to the deployment and protection of DSRC in the 5.850-5.925 GHz band.

The Institute for Electrical and Electronics Engineers 802 standards committee has established a working group, known as the IEEE 802.11 DSRC Coexistence Tiger Team, that provides an international multi-stakeholder technical forum that includes industry experts previously involved in developing standards for both wireless local area networks and vehicular wireless communications.[163] While NTIA's January 2013 5 GHz Report indicated that NTIA would follow up with quantitative studies in connection with domestic and international regulatory proceedings involving the 5350-5470 MHz, 5850-5925 MHz, and other bands, NTIA believes that industry participants should first be afforded adequate time to identify acceptable

[160] The NTIA 5 GHz Report is available at www.ntia.doc.gov/report/2013/evaluation-5350-5470-mhz-and-5850-5925-mhz-bands.

[161] 78 Fed. Reg. 21320, at 21321 (Apr. 10, 2013).

[162] One of the primary operating conditions under Part 15 is that the operator must accept whatever interference is received and must correct whatever interference is caused. Should harmful interference occur the operator is required to immediately correct the interference problem, even if correction of the problem requires ceasing operation of the Part 15 system causing the interference. See 47 C.F.R. Section 15.5.

[163] In August of 2013, the Regulatory Standing Committee of IEEE 802.11 created a "Tiger Team" to bring together interested participants to exchange technical ideas and explore possible solutions to the band sharing issue as proposed in this NPRM. This group, referred to as the DSRC Coexistence Tiger Team, operates under the auspices of the IEEE 802.11 working group. Conference calls are conducted weekly, and submissions and emails are openly available to the public on IEEE document servers.

technology approaches for coexistence in the 5850-5925 MHz band. [164] The Tiger Team's meetings have been productive, providing a venue for presenting and discussing concepts regarding potential coexistence approaches. On January 24, 2014, the Tiger Team sent a letter to the FCC to summarize activities coordinated by IEEE 802.11.[165] As discussed in the letter the current work items for the group include:

- Review of ITS/DSRC field trials conducted to date
- Review of work to date on coexistence
- Presentations on use cases
- Presentation of possible coexistence approaches
- Modeling/simulation of possible coexistence approaches
- Prototype testing of candidate approaches

Thus far, the group has engaged in extensive discussions about the status and performance of DSRC systems, explored requirements for band sharing, and had presentations on some preliminary candidate approaches for sharing techniques. If viable candidates for sharing are identified as part of this effort, NTIA anticipates extensive field testing will be conducted by WLAN and DSRC stakeholders outside of IEEE 802.11.

While DOT is encouraged by the work of the Tiger Team, the candidate approaches presented thus far do not yet contain adequate content to evaluate whether spectrum can safely be shared without creating harmful interference. As the work of the Tiger Team progresses and mature technical proposals are submitted for review, DOT will continue to work with the NTIA to review and analyze these sharing approaches.[166] Once this analysis is complete, DOT, along with the NTIA and the FCC, will be better positioned to assess how the proposed changes to existing rules and regulations for harmonization across such a large swath of spectrum will impact DSRC. NTIA and DOT will continue to work with the FCC to explore different avenues to facilitate and encourage inter-industry and inter-agency collaborative efforts to assess the possibility of sharing in the 5.850-5.925 GHz band.

[164] Letter from Lawrence E. Strickling, Assistant Secretary for Communications and Information to the Honorable Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology Committee on Energy and Commerce (Jan. 27, 2014).

[165] The letter is available at https://mentor.ieee.org/802.18/dcn/14/18-14-0007-02-0000-dsrc-coexistence-tt-status-letter-to-oet.docx.

[166] DOT submitted comments to the NPRM through NTIA in June 2013. See http://apps.fcc.gov/ecfs/document/view?id=7022424618 (last accessed Jan. 28, 2014).

Research Need V-1 Spectrum Sharing Interference[167]

Research Activity: Effect of spectrum sharing on V2V Crash Avoidance Performance

Description: Evaluate the impact of unlicensed U-NII devices on the transmission and reception of safety critical warnings in a shared spectrum environment.

Target Completion: US DOT is working with NTIA and other stakeholders to evaluate sharing proposals made by the communications industry in order to help ensure that there will be no interference to DSRC-enabled V2V safety applications caused by any sharing of the spectrum with unlicensed devices.

Current or planned NHTSA research addressing this need:

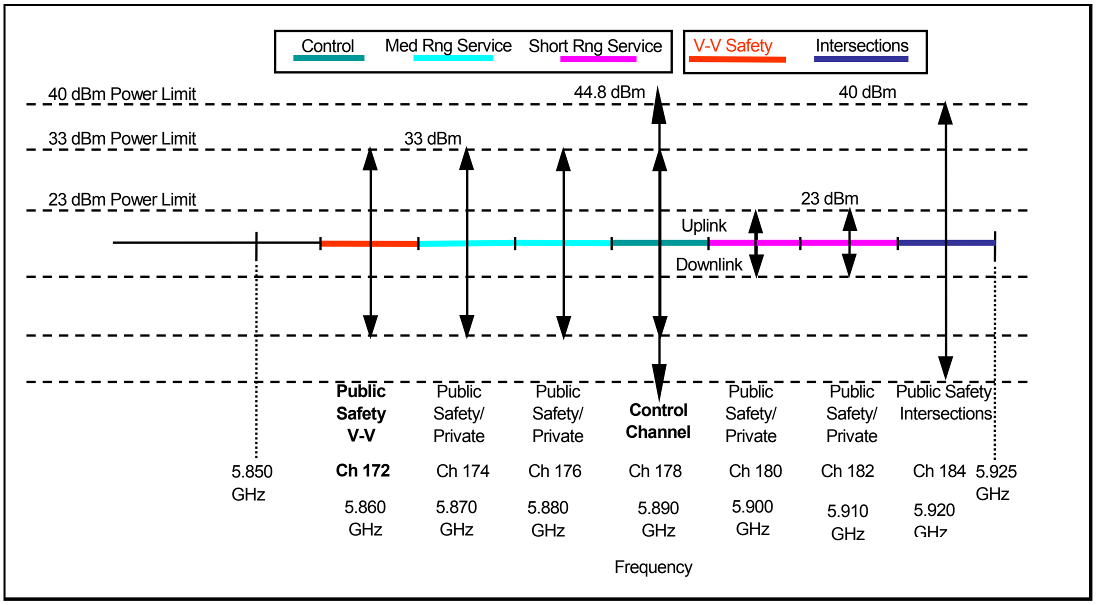
US DOT will continue to coordinate with NTIA and other stakeholders on the issue of shared spectrum testing.

d) V2V wireless communication channels

Currently, 75 MHz of wireless spectrum is allocated for DSRC by FCC. This spectrum is divided into seven non-overlapping 10 MHz channels, plus a 5 MHz guard band at the beginning of the frequency range. The FCC band plan for this spectrum specifies particular usage, power limits, etc. for these channels as shown in Figure V-2 below.

[167] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

Figure V-2 Band Plan for DSRC Channel Spectrum



As a radio, the DSRC unit operates on one frequency (or "channel") at a time – consider, for example, the AM/FM radio in vehicles today, which can receive one station or another depending on how it is tuned (tuning being the act of shifting signal reception from one radio frequency to another), but does not receive clearly when it is between stations, and cannot be tuned to more than one frequency at once.

The current V2V operation uses two radios, one tuned to channel 172 and dedicated for safety communications and another tuned to channel 174 for security-related communications. In addition, a third channel, 178, is used as a control channel to manage channel switching[168] to support messages on other channels related to other services/applications, such as mobility or environment.

Early on in the VSC-A project, researchers initially attempted to use channel 178 as both a "control" channel[169] and for transmission of the BSM, but using a single channel for both unduly restricted BSM transmission, potentially hindering safety. It was thought that a channel switching mode could be used on a single radio to support the BSM as well as use the other channels for other messages, because the channel switching mode would cause the BSM transmissions to switch from channel 178 to some other channel. However, because a radio can

[168] Channel switching is the use of a dedicated channel to route incoming messages to multiple "service" channels that use the incoming information. This method allow for a single radio to be used to support multiple functions.

[169] The control channel "tells" the radio which channel to "listen" to for specific information as well as transmitting that same information when the device is ready to transmit information.

only transmit or receive on a single channel at a time, channel switching only solves part of the problem – the radio still has to take turns between the BSM and the other necessary messages.

The sections that follow explain the modes of operation and how the research indicated the need to implement a dedicated channel for the BSM.

(1) Channel Switching Mode

In order to transmit and receive messages on different channels, DSRC will have to switch from one channel to another, which it may need to do in order to perform different functions necessary for V2V communications.

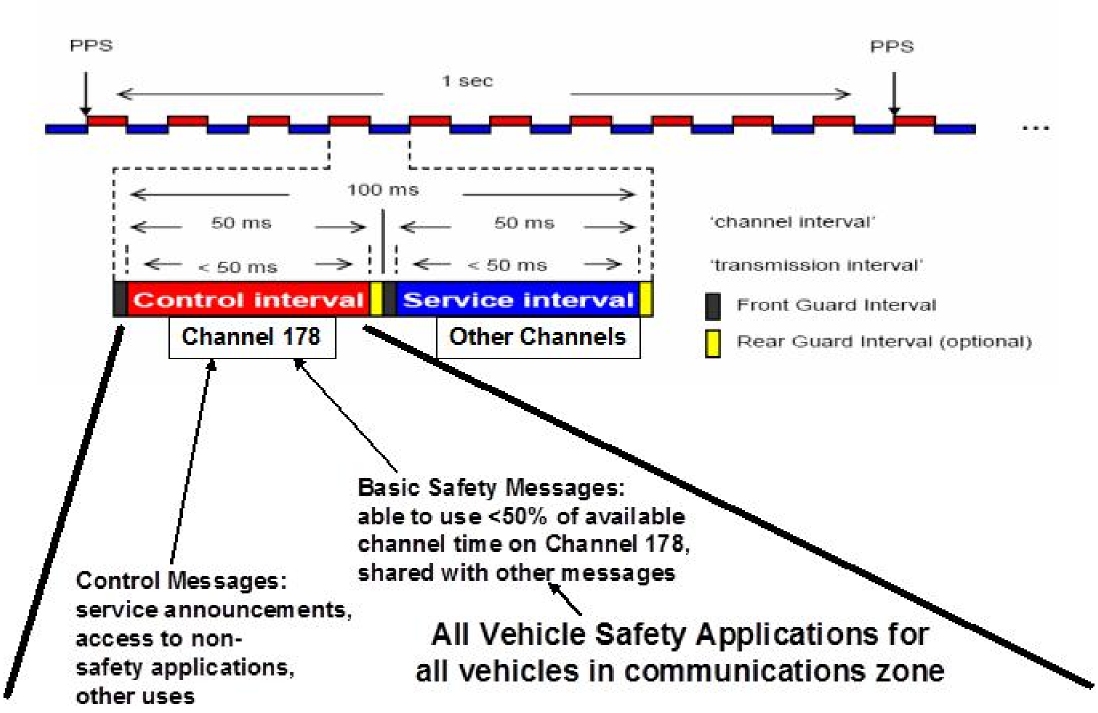
Time is an important facet of V2V communications, because BSM transmissions need to be received in a timely manner in order to warn drivers of potential dangers in time for them to react, among other things. If DSRC is switching from one channel to another, it may experience a time lag as the next channel is being picked up, which may potentially affect receipt of important transmissions. The IEEE 1609.4 standard[170] divides time for purposes of DSRC transmission into 100 millisecond sync intervals (the equivalent of 10Hz). The sync intervals are then sub-divided into a Control Channel (CCH) interval and a Service Channel (SCH) interval, and a time division mechanism is defined for a device to switch between the CCH and a SCH every 50 ms to transmit and/or receive DSRC messages.

As shown in Figure V-3 below, Channel 178 is designated as the “Control Channel.” It was originally envisioned that all vehicle and roadside units accessing this spectrum would use the control channel to determine what information is available on other channels, and then switch to the other channels to access the information.[171]

[170] For more information, see VSC-A Final Report: Appendix Volume 2.

[171] Id.

Figure V-3 Time Division Channel Usage


PPS
PPS
1 sec
...
100 ms
50 ms
50 ms
< 50 ms
< 50 ms
'channel interval'
'transmission interval'
Control interval
Service interval
Front Guard Interval
Rear Guard Interval (optional)
Channel 178
Other Channels
Basic Safety Messages: able to use <50% of available channel time on Channel 178, shared with other messages
Control Messages: service announcements, access to non-safety applications, other uses
All Vehicle Safety Applications for all vehicles in communications zone

During the VSC-A research initiative, vehicles participating in V2V safety communications using this channel switching operation sent and received BSMs on the CCH during the CCH interval. This would allow vehicles to participate in non-V2V safety communications on a SCH during the SCH interval for other DSRC services. While this safety communication model is not required by IEEE 1609.4, or any other standard, it was considered as the baseline approach for the initial research.

One of the main advantages of the above approach is that it allows a single-radio vehicle to participate in V2V safety by exchanging BSMs with its neighbors and also to avail itself of DSRC services that are offered during SCH intervals (e.g., by RSE). This capability is especially attractive as part of an initial DSRC deployment strategy to boost market penetration. One of the main disadvantages of this approach, however, is that safety messages are effectively limited to the CCH interval, and thus channel congestion is a significant concern. At high channel loads, the probability that two or more packets “collide” due to overlapping transmissions can become significant. As explained below, the research has indicated ways of mitigating the disadvantages, and NHTSA plans to do additional testing on congestion mitigation.

Due to a required 4 ms front guard interval V2V communications can only use a maximum of 46 ms out of the 100 ms sync interval. In other words, effectively only 46 percent "potentially" available bandwidth is available to be used because the remainder must be used for non-BSM transmissions, such as security, mobility, environment, and possibly commercial (auto diagnostics, requested assistance information) transmissions on other channels providing this information. Determining channel capacity via analysis is quite complex due to the MAC protocol used in DSRC. However, a simple calculation shows why 1609.4 time division causes a concern for V2V safety. As explained below, research indicates methods of addressing this concern are available. If a DSRC channel supports 6 Mbps, this is equivalent to 2,000 messages/second for 3,000-bit messages (the approximate size of an average BSM). At 10 messages/second/vehicle, this is equivalent to 200 vehicles in a given transmission region. With BSMs confined to the CCH interval, the capacity is cut to about 45 percent due to the guard interval and the need to complete packet transmissions before the start of the SCH interval. In this simple example, that is equivalent to 90 vehicles in a region. It is not difficult to construct realistic traffic scenarios in which a capacity of 90 vehicles in a transmission region represents a significant constraint.

(2) Multi-Channel Operation versus a Dedicated Safety Channel

Having two radios, one of which is always tuned to the dedicated safety channel, may help to avoid the need for channel switching and enable the vehicle to broadcast and receive BSMs the entire time it is in operation.

Having also determined that communication channel congestion could limit V2V safety system performance,[172] the CAMP VSC-A project team analyzed 11 scenarios of one- and two-channel operational approaches, within the constraints of IEEE 1609.4. This is discussed further in the Congestion Mitigation section of this paper – Section V.E.2.b).

3. Interoperability performance requirements

This section of the paper discusses the performance requirements for DSRC, GPS, and other system components that are understood to achieve interoperability.[173] This section covers four major topics: (1) overview of system performance requirements; (2) overview of requirements for exchanging messages (3) research history and technical maturity; (4) recommendations.

[172] CAMP, VSC-A Final Report (Sept. 2011, Report No. DOT HS 811 492A). See www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2011/811492A.pdf (last accessed Jan 28, 2014). [Hereafter, "VSC-A Final Report"].

[173] This section provides a general discussion of performance requirements for DSRC and GPS. Requirements needed to support specific safety applications are discussed in Section VI.

a) Overview of V2V program system performance requirements

This section describes how the specifications were developed. It provides a top-level view of the major factors that influenced the development of performance requirements for the V2V system.

The following factors were taken into account in developing the V2V system performance requirements.

1. Connected Vehicle Model Deployment safety application characteristics
2. Transmitting power a DSRC radio could provide
3. Receiving ability at a given area with a given transmitting power
4. Language vehicles speak when they communicate with one another
5. Language used for communication between vehicles and RSEs
6. Information necessary to be included in the BSM
7. Information necessary to be included in the communication between vehicles and the infrastructure~~.~~
8. Media devices could use to carry messages when they communicate with one another
9. Media devices could use to carry messages when they communicate with RSEs
10. Basic Safety Message data accuracy needs to be specified
11. Error tolerance and error correction capability (considering potential distortion) of over the-air signals being received by OBE
12. Capability of the system to accommodate all communication within a given area of coverage and for a given number of vehicles (DSRC channel congestion mitigation)
13. Method of synchronizing communication system network
14. The method of verifying and validating messages from other vehicles
15. The method of verifying and validating messages from other ECUs in a vehicle itself
16. Security scheme to protect data communication
17. Security scheme to initiate and ensure trusted key establishment
18. Security scheme to support key management
19. Physical security to protect security components and elements that will be essential pieces of establishing and sustaining the network trust at the Infrastructure side
20. Physical security to protect security components and elements that will be essential pieces of establishing and sustaining the network trust on the on-board DSRC devices
21. Security scheme to protect Personally Identifiable Information (PII)

b) Research history and technical maturity/readiness

Following is a summary of related research findings on performance requirements for DSRC and interoperability, a list of references, and a table for cross referencing to research activities, reports, standards, and the current status.

Initial system performance requirements were defined during the VSC project that started in 2002 and ran until 2005. During the VSC project, the VSC Consortium developed an initial set of safety applications that could be improved by communications with sources outside the vehicle. The VSCC then estimated benefits in lives saved and injuries avoided of these applications. VSCC and DOT then selected a subset of those applications for further development based on their potential safety benefits. VSCC developed communications performance requirements for the following eight applications.

- Traffic Signal Violation Warning
- Curve Speed Warning
- Rollover Warning
- Emergency Electronic Brake Lights
- Cooperative Forward Collision Warning
- Left Turn Assistant
- Lane Change Warning
- Stop Sign Movement Assistance

These requirements included the following.

- Message packet size of 200 to 500 bytes (all 8 scenarios)
- Maximum required range of communications of 50 to 300 meters (all 8 scenarios)
- One-way, point-to-multipoint broadcast messages (7 of 8 scenarios)
- Two-way, point-to-point messages (1 of 8 scenarios)
- Periodic transmission mode (6 or 7 of 8 scenarios)
- Event-driven transmission mode (1 or 2 of 8 scenarios)
- Allowable latency of 100 milliseconds (6 of 8 scenarios)
- Allowable latency of 20 milliseconds (1 of 8 scenarios)
- Allowable latency of 1 second (1 of 8 scenarios)[174]

The outcome of this project was, however, that the communications requirements would need further refinement as prototype vehicle safety applications are developed from a safety-systems design perspective.[175]

The extension of the VSC project, the VSC-A project, further refined and added to the minimum performance requirements. The VSC-A project developed performance requirements

[174] For more information, see Vehicle Safety Communications Project - Final Report (Report No. DOT HS 810 591) at www-nrd.nhtsa.dot.gov/pdf/surplus/nrd-12/060419-0843/PDFs/MainReport.pdf (last accessed Jan. 28, 2014).

[175] Id.

for GPS performance,[176] warning repeatability, maximum warning latency, true and false positive warning rates, EEBL, FCW, BSW+LCW, DNPW, IMA, and CLW.[177]

The requirements were refined yet again in the V2V Interoperability project, known as V2V-I.[178] These requirements were broken up into both functional (high-level) requirements and performance (detailed) requirements.[179] The V2V-Interoperability Report contains design requirements for the on-board equipment (DSRC radio, GPS receivers, and processors). Some of the requirements that were developed during these projects have been worked into a number of IEEE and SAE standards. For further reference on the development of the standards, please see Section V.E.

The performance requirements that were used and implemented in the specification documents for the VADs and ASDs during the Safety Pilot Model Deployment were developed directly from the V2V-I Project. During the Model Deployment over 3,000 vehicles have been equipped with V2V and V2I technologies and are driving around the public roadways of Ann Arbor, Michigan. Sixty-four of these vehicles are equipped with integrated OEM solutions (CAMP-developed device) that have been fully integrated into the vehicles, 300 vehicles have aftermarket technology installed, and 2,850 vehicles are outfitted with vehicle awareness devices that can transmit the BSM to other vehicles but cannot receive information with which to alert the driver. Many of these systems have internal components designed and built by a number of different manufacturers and suppliers. These vehicles have been operating together, as a system, providing alerts and advisories to drivers as a representation of how a fully functional V2V system might work. While this is a research project, and is built using prototype hardware, the performance requirements are adequate to ensure system functionality – i.e., the vehicles are capable of communicating with each other. The identified requirements are based on working systems that were collaboratively developed between NHTSA and CAMP, but since they are

[176] The VSC-A project performance requirement for GPS were further refined during the GPS available study. For a discussion of the performance requirements for GPS, s*ee:* Section V.D.1.d) "Relative Positioning."

[177] For more information, see VSC 2 Consortium, "Vehicle Safety Communications – Applications (VSC-A) Final Report: Appendix Volume 1 System Design and Objective Test," (Sept. 2011, Report No. DOT HS 811 492B) at www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 28, 2014) [Hereafter, "VSC-A Project Appendix Volume 1"]; see also VSC-A Project Appendix Volume 2 for full system requirements and further information.

[178] The critical system requirements were published prior to the Safety Pilot Model Deployment as the VAD and ASD system specifications. See System Requirements Description, 5.9 GHz DSRC Vehicle Awareness Device Specification, Version 3.6 (Jan. 25, 2012) at www.its.dot.gov/newsletter/VAD%20Specs.pdf (last accessed Jan. 28, 2014) and System Requirements Description, 5.9 GHz DSRC Vehicle Awareness Device Specification, Version 3.6 (Dec. 26, 2011) at www.its.dot.gov/meetings/pdf/T2-05_ASD_Device_Design_Specification_20120109.pdf (last accessed Feb. 20, 2014).

[179] The critical requirements can be found in sections 4 and 5 of System Requirements Description, 5.9 GHz DSRC Vehicle Awareness Device Specification, Version 3.6 (Jan. 25, 2012) at www.its.dot.gov/newsletter/VAD%20Specs.pdf (last accessed Jan. 28, 2014)

based on non-production systems, the agency does not consider them finalized, recognizing that at more work is necessary as discussed earlier in this section before production-level deployment can be realized. The following table shows a summary of the high-level requirements, including the maturity of the performance requirements that have been employed in the V2V program research. The table also shows the range of different research projects from which the Safety Pilot performance requirements were leveraged.

Table V-6 Performance requirements used in V2V research

Requirement	Research Activities	Requirements Exist for Safety Pilot	Finalized	Under Development	Comments
Safety application requirements	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	Application compliance test procedures, BSM Min Performance Req./SAE J2945
DSRC transmission range	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	e.g., 300 meters, 360 degrees, BSM Min Performance Req./SAE J2945
DSRC receiving range	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	e.g., 300 meters, 360 degrees, BSM Min Performance Req./SAE J2945
Language vehicles speak when they communicate with one another	VSC, VSC-A, V2V-I, Safety Pilot	✓	✓		communication protocol SAE J2735, IEEE 1609.2 and IEEE 1609.3 and IEEE 1609.4
Language used for communication between vehicles and RSEs	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	communication protocol IEEE 1609.2 and IEEE 1609.3 and IEEE 1609.4
Information necessary to be included in the V2V communication	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	BSM protocols; SAE J2735, BSM Min Performance Req./ SAE J2945
Information necessary to be included in the communication between vehicles and RSEs	VSC-A, V2V-I, Safety Pilot	✓		✓	WSM Protocols; IEEE 1609.3 & 1609.4
DSRC radio channel operational mode and usage for communication with other vehicles	VSC, VSC-A, V2V-I, Safety Pilot	✓	✓		IEEE 1609.4, BSM Min Performance Req./ SAE J2945
DSRC radio channel operational mode and usage for communication with RSEs	VSC, VSC-A, V2V-I, Safety Pilot	✓	✓		IEEE 1609.4, BSM Min Performance Req./ SAE J2945
Basic Safety Message data accuracy needs to be specified	V2V-I, Safety Pilot	✓		✓	BSM Minimum Performance Requirements/SAE J2945
Error tolerance and error correction capability (considering potential distortion) of over the air signals being received by OBE	VSC-A, V2V-I, Safety Pilot	✓		✓	IEEE 802.11p
Ability of the system to accommodate all communication within a given area of coverage and for a given number of vehicles (DSRC channel congestion mitigation)	VSC-A, V2V-I			✓	DSRC channel congestion mitigation research will continue beyond 2013 decision
Method of synchronizing communication system network	VSC-A, V2V-I, Safety Pilot	✓	✓		GPS (UTC) time; BSM Min Performance Req./ SAE J2945

Ability to verifying and validating messages from other vehicles	VSC-A, V2V-I, Safety Pilot	✓	✓		
Method of verifying and validating messages from other on-board ECUs (within a given vehicle. E.g., vehicle data bus)					Need for plausibility checks, data bus security is under consideration
Security scheme to protect V2V communication	VSC, VSC-A, V2V-I, V2V-CS, V2V-VSCS, Safety Pilot	✓		✓	Prototype SCMS design
Security scheme to initiate and ensure trusted key establishment	VSC, VSC-A, V2V-I, V2V-CS, V2V-VSCS, Safety Pilot	✓		✓	
Security scheme to support key management	VSC, VSC-A, V2V-I, V2V-CS, V2V-VSCS, Safety Pilot	✓		✓	
Physical security to protect security components and elements that will be essential pieces of establishing and sustaining the network trust at the Infrastructure side	V2V-CS, V2V-VSCS				
Physical security to protect security components and elements that will be essential pieces of establishing and sustaining the network trust on the on-board DSRC devices	VSC, VSC-A, V2V-CS, V2V-VSCS			in planning	
Security scheme to protect Personally Identifiable Information (PII)	V2V-I, V2V-CS, V2V-VSCS, Safety Pilot	✓		✓	

c) Software performance requirements

Research is needed to determine if the software components that NHTSA may require as part of an FMVSS can be regulated using objective tests, without requiring the use of specified algorithms. NHTSA has not previously regulated system aspects as detailed as software components. This may be necessary because a performance test may allow multiple pathways to compliance but may not result in full interoperability among devices. Because software can allow for multiple methods of producing the same result, there is a gap in our understanding of how potential multiple software solutions by different device manufacturers (or vehicle manufacturers) would affect the V2V system's ability to be interoperable.

As an example, congestion mitigation has currently been tested during the V2V-I project using two different mitigation algorithms. These algorithms were specified under the system requirements and units were fielded with these predetermined algorithms. They worked well and predictably under all test scenarios because all software components were the same. Had they instead been performance metrics such as “the channel busy ratio must stay below 70 percent at all times,” we do not know if different suppliers would have developed individual mitigation solutions and whether they would be interoperable. There is a risk that if different suppliers were to use different mitigation strategies, vehicles may not receive BSMs with the frequency needed for the safety applications to function.

Research Need V-2 Impact of Software Implementation on DSRC Device Performance

Research Activity: DSRC Device Performance Requirements

Description: Finalize requirements for V2V device software standards, performance, and requirements needed to ensure interoperability with other vehicles and roadside equipment, support safety applications, and adhere to security and privacy communications requirements.

Target Completion: Mid-2015 (draft report to NHTSA)

Current or planned NHTSA research addressing this need:

Working with both industry (CAMP) as well as independent (third-party) automotive and communications research companies, NHTSA is developing a complete description of functional, performance, and operational requirements for the on-board vehicle systems needed to support V2V communications.

d) Additional performance requirements research

Current performance requirements exist in a pre-competitive, prototype research state. We have been able to achieve a large scale (2,800 vehicles) test in which vehicles could reliably talk to each other, yet these requirements are not FMVSS-ready given that test procedures to gauge compliance with the requirements do not exist for all components of the system. Additionally, test procedures that do exist have not been evaluated to ensure that they produce objective, repeatable results, and minimum requirements necessary for some components of system such as the minimum broadcast frequency of the BSM necessary to support safety applications have yet to be determined.

NHTSA is currently engaged in research with Booz Allen Hamilton[180] to examine the minimum performance measures for DSRC communication and system security. This research will include functional and performance requirements for the DSRC device and present NHTSA with a list of recommended changes to these requirements as currently laid out for the Safety Pilot Model Deployment. An example of these recommendations would be how to deal with end-of-life issues on the DSRC components and security system.

In order to participate in the V2V system, the current design assumes that V2V devices will carry up to three years of security certificates. It is possible that V2V devices may retain these certificates upon their retirement. If the certificates were somehow obtained by a malicious

[180] NHTSA Task Order DTFH61-11-D-00019-T-13016 DSRC Communications Performance Measures.

party, they could be used to participate in the system without permission. To maintain the security of the system, some requirements for device end-of-life (e.g., forced memory purging of certificates, destruction of a malfunctioning or non-functional device, or some other end-of-life measure) will likely be necessary in exchange for participation in the SCMS, although it remains to be determined whether such requirements would be from NHTSA or from the entity managing the SCMS.

Research Need V-3 DSRC Data Communication System Performance Measures

Research Activity: DSRC Device Performance Requirements

Description: 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.

Target Completion: Mid-2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

The research to be completed under Need IV-2 will also address this research need.

Once performance requirements have been identified, objective performance metrics to measure those requirements will need to be developed to support FMVSS-level testing. NHTSA should be able to leverage the certification testing work used to support the Safety Pilot, although performance testing conducted for the Safety Pilot will need to reflect any changes the performance requirement research may suggest.

Research Need V-4 Development of Safety Application Test Metrics and Procedures

Research Activity: Safety Application Objective Test Procedures & Performance Requirements

Description: 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.

Target Completion: 2016 (draft test procedures)

Current or Planned NHTSA research addressing this need:

CAMP, NHTSA, and the Volpe Center are completing projects to address the development of objective test procedures for IMA and LTA safety applications. This research activity will include investigation of the rationale for and validation of various performance measures; test the practicability and need for non-ideal conditions testing; and evaluate the applicability of the tests to V2V based or V2V/Vehicle-based sensor combined systems.

E. System Limitations

1. What are the known system limitations for V2V communication?

V2V safety systems use messages broadcast by vehicles to enable cooperative crash warning applications. Traditional crash warning applications, on the other hand, use vehicle-based radar, lidar,[181] mono camera, stereo camera or combinations of these sensors to perform similar threat detection in order to enable crash warning applications. Each sensor has unique characteristics that translate into system advantages and disadvantages. This section discusses system limitations of V2V safety systems by comparing their characteristics to those of traditional crash warning systems. The discussion is based on the information summarized in the following table.

Table V-7 Collision Avoidance Sensor Summary

○	◔	◑	◕	●
Bad	Poor	Fair	Good	Excellent

Sensor Type	**Radar 24 GHz**	**Radar 77GHz**	**Lidar**	**Mono Camera**	**Stereo Camera**	**Radar + Camera**	**V2V**
Field of view	56^0	18^0	27^0	36^0	48^0	$18^0/36^0$	360^0
Typical range	60 m	200 m	10 m	(50 m)	(150 m)	200 m / 50 m	300 m
Accuracy	0.2 m	0.2 m	0.2 m	?	?	0.2 m / ?	< 1.5 m
Relative reliability in snow, fog, heavy rain	◕	◕	◕	◑	◑	◕	●
Reliability in direct sun and shadows	●	●	●	◑	◕	●	●
Reliability in "urban canyons"	●	●	●	●	●	●	◑
Reliability in tunnels and under heavy foliage	●	●	●	◕	◕	●	◕
Vulnerability to damage or misalignment	Yes	Yes	Yes	No	No	yes	No
Generally considered sufficient to react to	no	No	No	no	yes	yes	Yes

[181] Lidar 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.)

fixed objects (by OEMs)							
Number of objects (vehicles) that can be tracked/processed at any given time	17	17	17	?	?	17/?	TBD >200
Capable of close range, low speed range-rate estimates (city safe capability	No	No	Yes	No	No	No	for warning applications only
Requires multiple vehicles to be equipped	No	No	No	No	No	No	Yes
Supports pedestrian detection	need multi-sensor system	need multi-sensor system	need multi-sensor system	need multi-sensor system	yes	yes	TBD
Sufficient to support activation of active safety systems	No	No	No	No	yes	yes	TBD

a) Field of view and range limitations

The figures below illustrate a generic traffic scenario for both a conventional crash avoidance system and a V2V-based safety system. Assuming all vehicles are equipped with V2V, the orange vehicle in Figure V-4 receives messages from the other vehicles in a 360^{o} area bound by a 300 meter radius, enabling safety applications that monitor the entire surroundings for crash imminent threats. The conventional system shown in Figure V-4 includes forward-looking long range radar and mono camera, as well as short range radar on each rear corner for blind zone detection. The forward sensor fields of view are illustrated by the blue shading, which depicts the long-range radar, and the white shading, which depicts the mono camera. The white shading at each rear corner depicts the short-range blind spot radars. As illustrated, the forward-looking radar can be obstructed by the first vehicle directly ahead in its lane, and thus is often unable to track other vehicles in the same lane. Similarly, the camera can be obstructed by objects such as the commercial truck in the illustration. With the four sensors shown, the conventional system is limited to reliably detecting and monitoring only two of the vehicles shown, the vehicle directly in front and the vehicle in the blind zone at the rear left of the equipped (orange) vehicle. By contrast, the V2V system can warn of threats from any direction using a single GPS sensor and DSRC communications.

Figure V-4 V2V System

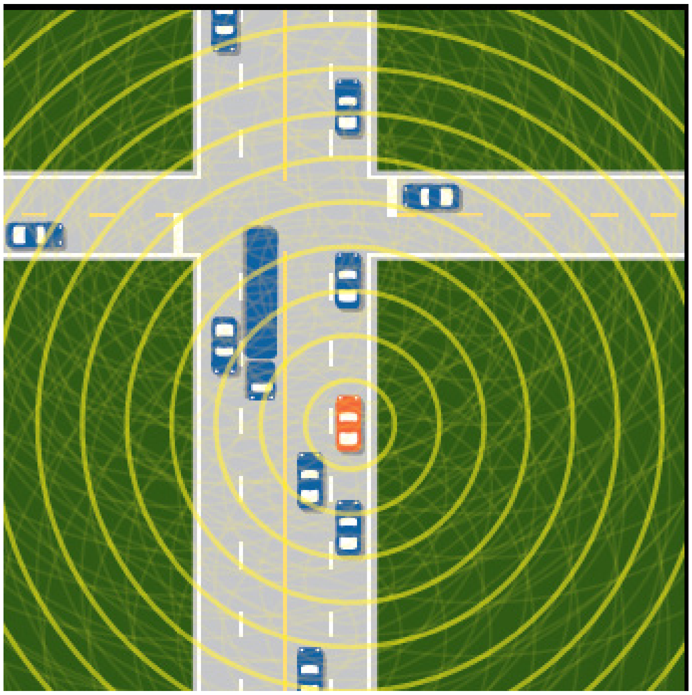
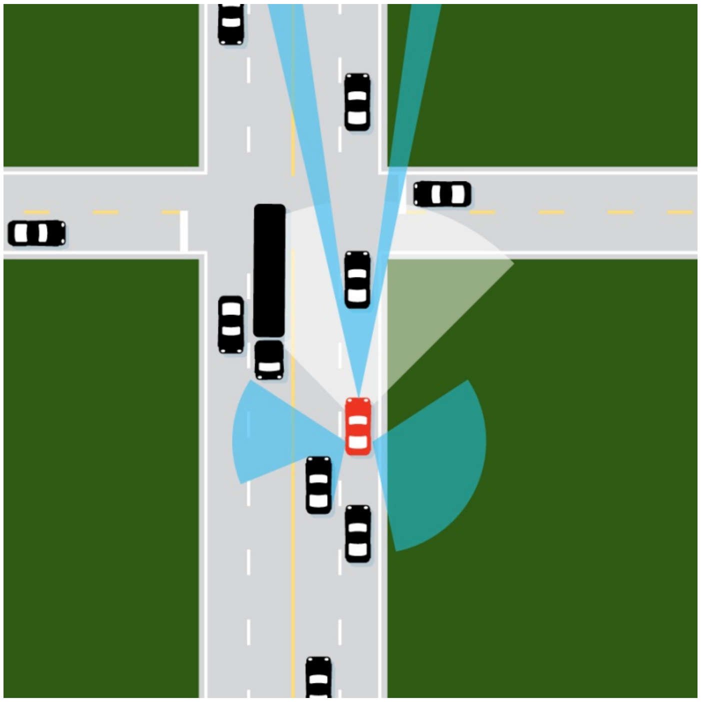


Figure V-5 Conventional System



b) *System availability limitations*

V2V system availability degrades gracefully[182] when subjected to reduced GPS availability (e.g., urban canyons or under extremely heavy foliage) or prolonged GPS outages (tunnels). In its current state, the V2V safety system is relatively immune to intermittent GPS outage (less than 1 second), which accounted for the majority (93%) observed during the 20,000 miles of data collected in the DOT-CAMP system performance testing.[183] Prolonged outages of 2 to 5 seconds result in graceful degradation of the system (safety applications), potentially limiting the applications to only those that require road-level positioning accuracy (e.g., intersection movement assist) and not allowing those that require lane-level accuracy (e.g., forward collision warning).

c) *Basic safety message congestion limitations*

Large scale deployment of V2V safety communications will require a communication system that will function and be able to support interoperability even when penetration of V2V into the vehicle fleet becomes widespread. There will be situations during normal driving conditions where a large volume of vehicles are driving in close proximity to each other, such as heavy freeway traffic. It will be important to ensure that the volume of messages in such "congested" situations does not somehow compromise the effectiveness of the system (and thus the effectiveness of the safety applications that might be enabled by the system) by saturating devices with messages, making it difficult to quickly sort out which are safety-critical and which are not, or even to transmit in general.

Testing of the scalability of the communications network has been conducted under two main projects, the Vehicle Safety Communications – Applications project[184] and the V2V-

[182] Fault tolerance, or graceful degradation, is the property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components. If its' operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a naïvely designed system in which even a small failure can cause total breakdown.

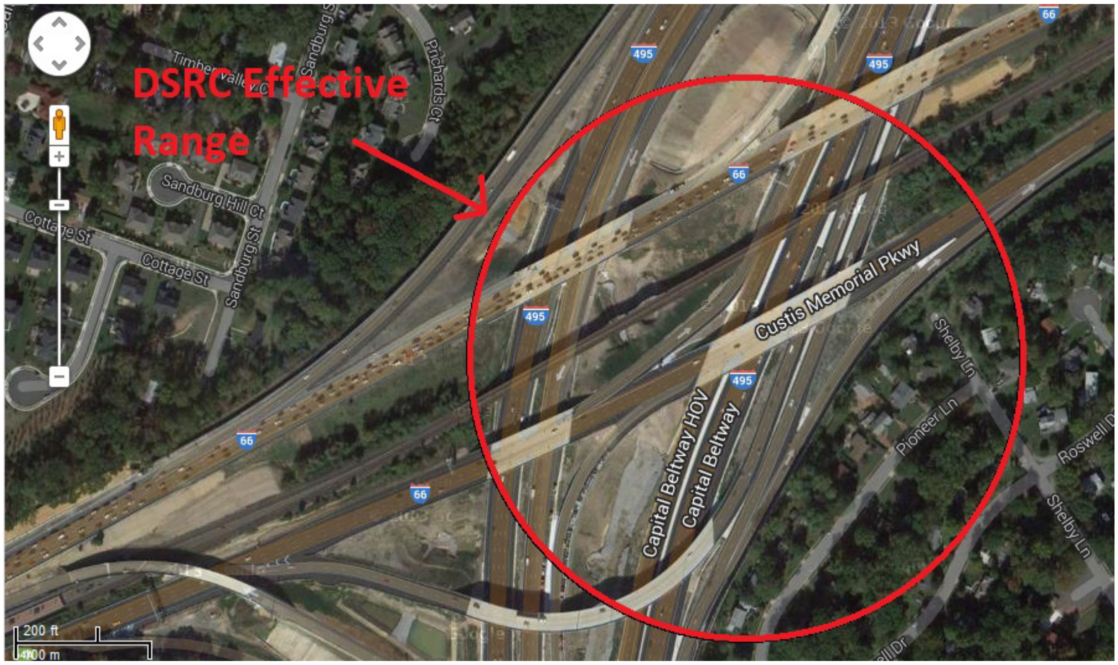
[183] Vehicle-to-Vehicle Safety System and Vehicle Build for Safety Pilot (V2V-SP) Final Report, Vol. 2: Performance Testing (Crash Avoidance Metrics Partnership on behalf of the Vehicle Safety Communications 3 Consortium, April 10, 2014). *See*: Docket No. NHTSA-2014-0022

[184] VSC-A was a 3-year collaborative effort between DOT and CAMP to develop and test communications-based vehicle safety systems to determine if DSRC at 5.9 GHz, in combination with vehicle positioning, can improve upon autonomous vehicle-based safety systems and/or enable new communications-based safety applications. The VSC-A project also developed performance requirements for GPS performance, warning repeatability, maximum warning latency, true and false positive warning rates, Emergency Electronic Brake Lights, Forward Collision Warning (FCW), Blind Spot Warning and Lane Change Warning (BSW+LCW), Do Not Pass Warning (DNPW), Intersection Movement Assist (IMA), and Control Loss Warning (CLW). See VSC-A Project Appendix Volumes 1 and 2 for full system requirements and further information. *See also:* Vehicle Safety Communications – Applications (VSC-A), Second Annual Report, January 1, 2008 through December 31, 2008 (Report No. DOT HS 811 466) at www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 28, 2014).

Interoperability project.[185] During VSC-A, 60 vehicles were tested for scalability of the network to see the effects of different data rates, multiple radios, and broadcast frequencies. The V2V-I project tested a grouping of 50, 100, 150, and 200 vehicles under a number of different V2V safety applications in multiple testing locations across the country.

As a point of reference, Figure V-6 shows the interchange between I-495 and Rt. 66 outside of Washington, DC. This interchange contains 2 express lanes and 4 regular lanes for I-495 running north and south and passing underneath Rt-66, which has 3 lanes running east and west. When off ramps are added, this leads to a total of 22 lanes of traffic in a 300 m radius. In grid-lock conditions, assuming an average car takes 24 ft. of lane space, this interchange can have over 800 vehicles in range of a single radio. The agency is conducting additional congestion research to better understand congestion limits and mitigation needs.

Figure V-6 I-495 & Rt 66 Interchange



Also tested during the V2V-I project were two algorithms for congestion mitigation.[186] These algorithms are designed to limit the frequency of BSMs broadcast during periods of high

[185] More information can be found in Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project - V2V-Interoperability, Draft Final Report, Section 4.2 (April 17, 2014). (Hereafter, "V2V-I Final Report"). See Docket No. NHTSA-2014-0022.

[186] Algorithm X is a transmission control protocol for scalable V2V safety communications that supports adaptive control of the message transmission rate and transmission power. Algorithm Y controls message transmission rate based on reported CBP from the neighboring vehicles and that measured by the host vehicle. The algorithm adapts

channel usage and at the same time ensure that vehicles were able to receive sufficient data to support the safety applications.[187]

Also developed under the V2V-I project was a proof of concept simulator designed to numerically simulate large vehicle networks. The V2V-I project found that even during the 200 vehicle test, at the maximum normal transmit rate of 10 Hz, the channel was not saturated, and all safety applications tested functioned normally. Although channel saturation was not reached, both congestion mitigation algorithms were able to demonstrate decreasing channel congestion while showing good safety application performance.[188]

Current research has shown that the V2V safety applications perform reliably in test scenarios with up to 200 vehicles in communication range. However, research conducted by CAMP and NHTSA has yet to estimate the number of other DSRC-equipped vehicles that a single DSRC radio would need to be exposed to in an environment (such as heavy freeway traffic) where channel congestion would be significant. Because the number of vehicles using the network within a particular broadcast area is not known, it is therefore not possible to compare the results of this testing to levels of channel congestion that might be experienced after full penetration of the technology.

Channel congestion may impact DSRC's effectiveness, which may in turn impact the effectiveness of DSRC-supported safety applications. Congestion mitigation may, therefore, be an issue that the agency needs to consider in developing potential future regulatory requirements for DSRC. NHTSA has planned additional research on this subject to address that need.

d) Relative positioning limitations

Based on testing during the initial phase of the Safety Pilot Model Deployment of several different GPS receivers of varying performance, quality and price, NHTSA believes that off the shelf, automotive GPS receivers on the market today are able to perform very well in V2V applications, although that statement should be qualified. GPS availability and solution accuracy deteriorate, for example, in deep urban environments and other areas of limited sky coverage. This will cause lane-level accuracy to degrade towards road-level accuracy in driving environments with limited sky visibility. While most of the safety applications require lane-level accuracy, and would thus be unavailable in those situations, road-level accuracy still allows the use of EEBL and IMA applications in these GPS-challenging locations. Any final determinations regarding the necessary performance for GPS units will be informed by the final results of the

the message rate up and down in order to maintain a desired level of channel utilization. For more information, see: V2V-I Final Report Section 4.2 and Appendix A, V2V Safety Communications Scalability Algorithms Details.

[187] V2V-I Final Report, at 79.

[188] V2V-I Final Report, at 79.

Safety Pilot, Driver Clinic system performance, and other ongoing research. Additionally, the deployment of new satellites, navigation industry improvements, and collaboration between the navigation industry and the automotive industry will improve GPS receiver accuracy and identify ways to address current challenging GPS environments.[189]

It should be noted that GPS receiver performance in the market is quoted in terms of the absolute positioning accuracy. The BSM minimum performance requirements for the vehicle positioning are currently phrased in terms of accuracy to an absolute position for purposes of the Safety Pilot, requiring the vehicle's reported latitude and longitude to within 1.5 meters of the actual position.[190] A relation must be made between the relative positioning performance required by the V2V safety applications and the receivers' advertised absolute positioning performance.

e) Comparison to sensor-based system

The V2V safety system communications is not impacted by weather (rain, fog, snow, sunlight or shadows). Radar and lidar perform reliably under all lighting conditions, while camera systems have some issues with shadows and lighting transitions, which are typical conditions for tunnels and under foliage during daylight. Additionally, V2V safety system communications are impaired by limited sky visibility, as in highly dense urban areas. In contrast, various conventional crash avoidance sensors perform reliably in urban canyons. In summary, both V2V safety systems and conventional crash warning systems have system availability limitations.

(1) Other Limitations for Conventional Sensor-based Systems

- Vulnerability to misalignment from impact (lidar and radar)
- Insufficient to react to stopped objects with a single sensor (lidar and radar)
- Limited number of vehicles can be processed (tracked) for threat determination
- Incapable of close range, low speed range-rate estimates (radar, camera)

(2) Other Limitations for V2V Safety Systems

- Requires a significant number of vehicles to be equipped for system effectiveness
- Accuracy is currently only sufficient for collision warning applications (see relative positioning section for future positioning improvements in Section V.E.1.d)

[189] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

[190] System Requirements Description: 5.9 GHz DSRC Vehicle Awareness Device Specification (Version 3.6, Jan, 25, 2012). See www.its.dot.gov/newsletter/VAD%20Specs.pdf (last accessed Jan. 28, 2014), requirement number SRD-USDOTOBE-003-ReqPOS003v001: Vehicle Position.

- Additional testing and field experience needed to establish level of trust of V2V messages sufficient to activate vehicle control applications

2. Potential mitigation strategies for known system limitations

a) System availability

For short duration GPS outages lasting a few seconds, devices can make use of inertial navigation units to predict the location of the vehicle. These units contain a number of accelerometers, gyros, and angular rate sensors that can be combined with mathematical models of vehicle dynamics to take the vehicle's position at loss of GPS and estimate the position further for a few seconds. Because of noise and error build-up in the sensors, the accuracy of the estimated position degrades the longer the estimation runs. Currently there are no long-term solutions for extended-duration GPS outages.

b) Basic Safety message congestion

Future research is currently planned under an extension of the V2V-I project, currently known as V2V-IE (phase 2). During this phase, physical testing will be conducted using up to 400 DSRC devices, both in vehicles and in specially-designed static test carts. This second phase will also work to refine the simulation, calibrating it against the data recorded during the first phase of the V2V-I project and data recorded during the field testing in phase 2. The goal of the simulation work is to simulate vehicle interactions far more numerous than what the agency believes can be practically field-tested. Following both the field testing and simulation work, the algorithms initially tested in phase 1 of the V2V-I project will be refined using the data collected during each. Finally, as the project closes, findings will be incorporated into SAE J2945 and other applicable SAE standards, which will facilitate development of devices that contain standardized congestion mitigation capability.

Research Need V-5 BSM Congestion Sensitivity

Research Activity: Basic Safety Message Congestion Mitigation

Description: 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.

Target Completion: Early 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

Analysis, research and testing of potential congestion challenges and mitigation strategies will be completed by CAMP under the existing Interoperability task.

Additionally, NHTSA believes that a DSRC channel congestion mitigation algorithm is important to ensure that the system identifies the most critical threats in densely populated traffic scenarios (assuming all equipped with V2V), to avoid missed threats and consequent risk to drivers.

c) Relative positioning improvements

Improvements to GPS signals and industry plans to produce automotive-grade receivers capable of using these signals will allow for increased positional accuracy in the future. The relationship between the specified absolute positioning performance of a receiver and its required relative positioning when measured against a different receiver needs to be better understood, and the study relating these two will lead to a more informed positioning performance requirement for V2V systems.

Given the observed differences in relative positioning performance in mixed pairs of receivers, such a relationship will need to be generalized for different receivers. CAMP has proposed, as part of Task 5 of the Vehicle-to-Vehicle Safety System Light Vehicle Builds and Model Deployment Support, a course of research to derive this relation. The path outlined in the proposal included a literature search for any previously-found relationships between relative and absolute positioning; an analysis of CAMP's previously-collected test data that includes both relative and absolute positioning, such as the Safety Pilot Performance Testing, and additional data collection activities. This additional data collection will expand the diversity of receivers from what is found in the literature search and from previous CAMP testing. The goal of this data collection and analysis will be to produce a generalized relationship between relative and absolute positioning for the receiver pairs tested.

Research Need V-6 Relative Positioning Performance Test

Research Activity:	Definition of Certification Requirements and DSRC Device Test Procedures
Description:	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.
Target Completion:	Onboard requirements (mid 2015), and draft test procedures (late 2015).

Current or Planned NHTSA research addressing this need:
NHTSA is investing in developing the equipment and procedures to test adherence to communication standards and performance requirements (including relative positioning) as outlined in J2945 and other standards.

The additional data collection CAMP is proposing as part of the relative positioning requirement definition offers an opportunity to evaluate the peculiarities of positioning performance observed during the Safety Pilot performance testing. These short periods (several minutes) of erroneous position were observed at particular geographic locations and were attributed by CAMP to particular combinations of vehicle and GPS receiver having differing positional biases. The testing of a wider range of different receivers will allow for the opportunity to observe these types of peculiarities, and a more informed assessment of their effect on positioning performance.

CAMP has additionally proposed collaborative work between them and the GPS suppliers to improve receiver performance for V2V safety. Using the GPS industry's expertise with CAMP's experience with V2V safety, this collaboration plans to identify improvements that could be made to the supplier's existing GPS hardware and software, further studying the effect of mixed receivers on relative positioning performance, and gaining a better understanding of tuning receivers explicitly for V2V applications leading towards the goal of a upgrading automotive grade GPS receiver.[191]

Research Need V-7 Vehicle and Receiver Positioning Biases

Research Activity: Interoperability Research

Description: Research to understand potential erroneous position reporting due to positional biases across multiple GPS receiver combinations.

Target Completion: 2014 (Published final reports)

Current or Planned NHTSA research addressing this need:

Recent work has been completed as part of Phase I of the NHTSA-CAMP V2V Interoperability project and FHWA-CAMP Light Vehicle Driver Acceptance Clinics Project System Performance Test task. The final reports are under publication review and should be published in CY14. Additional research is being performed in Task 5 of the FHWA-CAMP Light Vehicle Build and Model Deployment Support Project. The final report is expected to be published in early CY2015. The research findings will be reflected in CAMP's draft submission to the SAE J2945 subcommittee. No additional research is planned.

3. Device installation constraints and requirements

a) OEM Devices

OEM devices are likely to be installed during the construction of the vehicle. This results in fewer constraints on installation than other V2V devices require. Basic constraints should include GPS antenna location and offset (the antenna should be located in an area of the vehicle that is free of electro-magnetic interference and allows for an unobstructed view of the sky), and location of the transceivers (they should be located in an area of the car free of EMI that does not interfere with the transmission or reception of the BSM or security information). Since the

[191] Vehicle-to-Vehicle Safety System Light Vehicle Builds and Model Deployment Support (V2V-MD), Technical Proposal, Vol. 1 Statement of Work (Crash Avoidance Metrics Partnership on behalf of the Vehicle Safety Communications 3 Consortium, Feb, 15, 2012). See Docket No. NHTSA-2014-0022.

devices will be integrated into the vehicle, care needs to be taken not to overly restrict the manufacturer's ability to select internal locations for supporting hardware.

b) Aftermarket Devices

The agency believes a certified installer would likely be needed to complete the installation for aftermarket safety devices. It is imperative that all V2V components be properly installed to ensure that an aftermarket device functions as intended. Whereas some vehicle owners may choose to replace their own brakes or install other components on their vehicles themselves, installation requirements for ASDs will likely not be conducive to a do-it-yourself approach. Improper installation of a GPS antenna has the potential to affect V2V communications for that vehicle via false warnings, improperly timed warnings, etc. An improperly installed aftermarket device may put all other V2V-equipped vehicles it encounters at risk until the given vehicle stops communicating, or until its messages are rejected for misbehavior. After completing the installation into the vehicle, correct configuration settings for x, y, z offsets are critical for system operation.

4. Managing device updates and improvements

a) OEM Devices

OEM devices allow for a variety of different methods for upgrades and improvements due to their integrated nature. These devices will be integrated into the vehicle data bus, which will allow them to make use of the same methods that OEMs currently use to manage vehicle firmware updates. OEMs also have a large distribution network, allowing for a pre-existing pathway for vehicle owners to have a reputable entity upgrade vehicle-specific DSRC software updates. A similar method can be leveraged to renew security credentials and service misbehaving units.

OEM devices can also leverage the current methods of upgrade that existing consumer electronics use today. A smartphone connected to the car via Bluetooth, or acting as a mobile hotspot, can be used to wirelessly update security certificates. Also, built-in DVD and Blu-ray players in existing infotainment systems might serve as a physical method of installing upgrades and new security credentials. Lastly, any method used to upgrade software components in aftermarket devices can be leveraged to upgrade OEM devices as well.

b) Aftermarket Devices

There are a range of methods from the consumer electronics industry that can be used to provide updated applications, certificates, etc., for aftermarket safety devices. These include:

- Wi-Fi Access, Satellite
- Cellular Access
- Flash or SD Memory Card

An ASD could receive updates in virtually the same way that cell phones, tablets, and laptops acquire updates – by connecting the device to a Wi-Fi network and downloading any updates or improvements over the Internet or satellite. Alternatively, an ASD could use a cellular connection to a back office server. The main challenge with this approach is determining how to cover the cost of the data transferred over the cellular provider network. One solution would be to link the device to the owner's personal cell connection. A third way for an ASD to receive updates is to use a flash or SD memory card. This approach was used in the Safety Pilot Model Deployment when software updates were required for VADs and self-contained devices. This approach is somewhat analogous to using a DVD to update the GPS maps in OEM or aftermarket navigation systems. Security certificates could also be downloaded from a computer to the memory card and then loaded to the device.

F. Global activities and differences in V2V systems

1. Research and/or implementation of V2V communications in other regions

Significant V2V research and development activities are underway in both Europe and Asia. For Asia, Japan and Korea appear as the regional leaders for development leading to eventual production implementation. Europe has made clear statements toward implementing V2I mobility-focused applications by the 2015 timeframe.

2. Differences between the current U.S. regional vision and other regions

a) Comparison of U.S. to EU

The U.S. approach focuses on a core set of crash-critical V2V safety applications. In previous research conducted by the U.S. DOT under the Vehicle Infrastructure Integration (VII) Program, the major focus was V2I applications and establishing an infrastructure. The shift in primary focus to vehicle-based V2V applications facilitates implementation of ITS safety technologies without the costly infrastructure implemented through State and local government investment while achieving safety benefits at overall lower costs. While the EU has defined crash-critical safety applications as well, the priority in the EU is driver safety advisories (not safety-critical warnings), driver support messages (such as eco-driving), and commercial applications such as insurance.[192] The breadth and content of EU applications, including mobility applications, reflects their market-driven approach, whereas the V2V safety focus in the U.S. reflects the potential for reducing crashes.[193] In the EU standards development activities encompass a broader set of applications while DOT is primarily focused on developing standards

[192] Global V2X Deployment: Contrasts with U.S. Approach, at 35 (Bishop, Jan. 21, 2013) at Docket No. NHTSA-2014-0022

[193] Id.

to support V2V crash avoidance applications.[194] Release 2 of the ETSI standards, planned for 2017, will focus on crash avoidance.

European carmakers have committed to begin introducing DSRC systems in 2015 and it is likely that initial European introductions would be on high-end vehicles and/or newly re-designed vehicle models; a different approach than requiring DSRC on all vehicles. While initial introduction in Europe could come much sooner than the U.S., the number of equipped vehicles could grow faster after the initial start in the U.S., if the U.S. pursues a DSRC mandate for all new vehicles. However, vehicles deployed initially in Europe would address mobility, sustainability, and "soft" safety on "day one" for equipped vehicles, while the U.S. approach to address crash-critical safety in the initial deployment and to provide a framework for other areas, such as mobility and others would be more challenged to give benefits on "day one." Therefore the benefits obtained in the first years of deployment will be quite different between the U.S. and other regions of the world. Additionally, because the focus in the EU for DSRC systems is mobility and environment rather than safety, which primarily entails communications between vehicles and infrastructure rather than between vehicles, security is much less of a concern, and it is likely that DSRC mobility and environment applications can be rolled out without the need for a SCMS. This would eliminate the SCMS cost from DSRC implementation in the EU, although that would change if the EU was to move towards requiring DSRC-based safety applications. However, the current European model would entail infrastructure costs that are not envisioned in the initial stages of V2V implementation in the U.S.

In terms of spectrum allocation, the U.S. allocation calls for seven channels of 10 MHz each (a total of 75 MHz of spectrum located in the 5.85 to 5.925 GHz frequency band), with one channel designated as a control channel and one channel exclusively for safety. The EU allocation calls for the 5.875-5.905 MHz band to be designated for safety-related ITS functions with three 10 MHz channels, including the possibility of two additional channels being granted in the future. No control channel exists in the EU approach.

Activities on the infrastructure side in Europe are promising for a deployment corresponding to OEM introductions, but this is not a certainty. Advances in ITS have typically been fragmented and slow due to the EU Member States being sovereign nations. EasyWay, a major ITS deployment initiative sponsored by the European Commission, which supplements deployment funding at the national level, has published a Cooperative-ITS Roadmap aiming at 2017 deployment of V2X. In addition, the Amsterdam Group aims at 2015 deployment. Given these concerns, European Commission officials at the 2012 ITS World Congress noted they are

[194] Id.

discussing various instruments that could apply to deployment, such as incentives to road operators or cities.[195]

b) Comparison of United States to Asia

In Asia, Japan and Korea are most active in DSRC development, with Japan leading. In both countries, the initial focus is on adapting the Electronic Toll Collection system operating at 5.8 GHz. The Japanese government has deployed 5.8 GHz "ITS Spots," which communicate with electronic toll tags to offer limited V2X safety capabilities, as well as mobility and convenience services. Additionally, some Japanese automotive OEMs (mainly Toyota) are actively supporting the deployment of V2X using 760 MHz communications. Japan appears likely to proceed with a two-band solution, and suppliers have prototyped transceivers covering both bands. Deployment of 760 MHz systems could come as soon as 2014.

In China, this band is reserved for potential ITS use as well. There have been indications that Korea seeks to shift to 5.9 GHz to be more compatible internationally, but no announcements have been made. No information was discovered indicating any interest from China for ITS applications in the 5.9 GHz band.

Development of message sets in Japan is not yet complete but appears to be toward the BSM/CAM[196]/DENM[197] message sets. Harmonization of probe data message sets is currently underway between Japan and the U.S. Similar to the approach in Europe, deployment in Japan is mostly market-driven, with the government leading to provide initial roadside capability in the case of the 5.8 GHz system, and some OEMs pushing for the 760 MHz system for V2V crash avoidance.

The Japanese 5.8 GHz system is not compatible with the IEEE 802.11p protocol used in the U.S. and Europe, due to a Japanese law requiring legacy protocols. At the security level, there are advocates of using IEEE 1609.2 as the security framework, which would be compatible with the U.S. and Europe, but this has not yet been decided.

[195] *Id.*, at 39.

[196] Cooperative Awareness Message.

[197] Decentralized Environmental Notification Message.

VI. V2V Safety Applications

NHTSA reviewed the existing information on various safety applications that leverage V2V communications and on various driver-vehicle interface options. NHTSA's goal in this effort was to determine:

- The extent to which the available performance and test metrics cover the variety of circumstances under which crashes occur that V2V-based safety applications could address; and
- Whether the metrics are practicable, repeatable, objective, and can clearly distinguish systems that pass from those that fail.

A. Performance metrics currently available for V2V safety applications

There are a number of performance and test metrics currently available that can be used to evaluate the performance of the research-stage prototype V2V safety applications and systems. This information can provide a useful foundation for the agency to consider and build upon to potentially establish Federal Motor Vehicle Safety Standards.

While the existing performance and test metrics cover the main conditions under which each of these crash types occur, a common theme among the performance metrics for all of the applications is the lack of testing under all conditions within the context of the safety problem, including, for example, poor weather or road conditions. To move forward with regulatory action to mandate safety applications, the agency would need to understand whether performance and test metrics can take into account these less-than-ideal conditions. As an example, the safety problem contains crashes that occur on wet pavement, which increases vehicle stopping distances, requiring adjustments to when advisories or warnings would be provided to a driver: advisories or warnings should be provided sooner if more time is needed for the driver to respond or for the vehicle to perform. However, this would need to be balanced with the potential for advisories or warnings to become nuisances to the driver, which could reduce system benefit.

With this in mind, the agency will need to evaluate crash statistics further to better understand what percentage of crashes happen under less-than-ideal conditions and how potential adjustment to warning activation may help drivers. Current crash data indicates that *most* crashes happen under ideal conditions, but further analysis may yield opportunities that could be addressed by V2V technology. This research would also focus on providing clear rationales for the inclusion or exclusion of any performance and test metrics.

In addition to considering how the existing performance and test metrics could be refined, further development will help ensure the metrics are practicable, repeatable, and can clearly distinguish systems that conform to the performance metrics from those that do not.

B. The safety applications

This section focuses on the following V2V safety applications that address common rear-end, opposite direction, junction crossing, and lane change crash scenarios, as shown in Table VI-1 and described below:

Table VI-1 V2V Safety Applications

Crash Type	Safety Application
Rear-End	Forward Collision Warning (FCW)
	Electronic Emergency Brake Light
Opposite direction	Do Not Pass Warning
	Left Turn Assist (LTA)
Junction crossing	Intersection Movement Assist (IMA)
Lane change	Blind Spot Warning + Lane Change Warning (BSW+LCW)

- FCW: Warns the driver of an impending rear-end collision with another vehicle ahead in traffic in the same lane and direction of travel.
- EEBL: Warns the driver of another vehicle that is braking hard farther up ahead in the flow of traffic. The braking vehicle does not necessarily have to be in the direct line of sight of the following vehicle, and can be separated by other vehicles.
- DNPW: Warns the driver of one 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 in the opposite direction of travel. The application may also provide the driver an advisory warning that the passing zone is occupied when a passing maneuver is not being attempted.
- LTA: Warns the driver of a vehicle, which is beginning to turn left in front of a vehicle traveling in the opposite direction, that making a left turn, at this time, would result in a crash.
- IMA: Warns the driver when it is not safe to enter an intersection due to high collision probability with other vehicles at controlled (with stoplights) and uncontrolled (with stop, yield, or no signage) intersections.
- BSW + LCW: Warns the driver during a lane change attempt if the blind spot zone into which the driver intends to switch is, or will soon be, occupied by another vehicle traveling in the same direction. The application also provides the driver with advisory

information that another vehicle in an adjacent lane is positioned in the original vehicle's "blind spot" zone when a lane change is not being attempted.

C. Key Findings for each V2V Safety Application

1. Forward Collision Warning

Forward Collision Warning is an application that currently has well-developed research-level performance and test metrics. The agency's analysis identified where more information would be needed to fully explore the issues that could arise in a regulatory action regarding V2V safety applications, such as a supporting rationale that clearly explains the safety risk/crash scenario that each metric is designed to address and how the metric will address that risk/scenario. Test metrics have been developed by CAMP and have been further refined by Volpe in support of the Track 4A Forward Collision Avoidance project. Test metrics for non-V2V forward collision systems were also developed for NHTSA's New Car Assessment Program (NCAP) and the In-Vehicle Based Safety Systems (IVBSS) project. Many of these performance and test measures may be applicable to a V2V-based FCW application; however, additional metrics will need to be developed based on V2V's unique capabilities, such as the DSRC radio operating in inclement weather and being able to detect vehicles beyond the current capabilities of radar and visual sensors.

The test procedures for FCW developed by CAMP and Volpe address all three of the priority pre-crash scenarios included in the rear-end crash group: Lead Vehicle Stopped, Lead Vehicle Decelerating, and Lead Vehicle Moving. These three scenarios comprise 93 percent of the rear-end crashes. Additionally, several of the test scenarios developed address variations of the striking maneuver crash scenario, which, while comprising a small number of rear-end crashes, represents an incremental benefit that can be gained by a V2V-based FCW system. While not explicitly tested, the FCW application also has the potential to address the additional two Lead Vehicle Accelerating scenarios, which comprise the other 7 percent of the rear-end crash group

However, additional analysis is necessary to ensure that each performance and test metric is sufficiently supported by a clear rationale. The specifics of these test procedures, such as their required alert timing, speeds at which the test is run, and radius of curvature, vary in detail across the developing organizations, and the agency believes they may need to be further refined to better reflect the safety problem.

2. Emergency Electronic Brake Lights

Emergency Electronic Brake Light addresses the Lead Vehicle Decelerating scenario and shares some overlap in functionality with the Forward Collision Warning application. EEBL issues a warning to the driver when the lead vehicle is decelerating by a minimum of 0.4 g. Previous research indicated that relatively severe braking (0.55 g or higher) by the lead vehicle in LVD crashes accounts for approximately 15 percent of the total number of LVD crashes.[198]

3. Do Not Pass Warning

The agency found that the Do Not Pass Warning application currently has a less robust set of performance and test metrics compared to other V2V safety applications studied. Do Not Pass Warning addresses only a subset of opposite direction crashes because it addresses situations where the driver is intentionally conducting a passing maneuver using the lane of opposing traffic. The safety data indicate that the vast majority (approximately 90 percent) of opposite direction crashes occur when a driver unintentionally drifts into a lane with oncoming traffic (as opposed to drivers conducting a passing maneuver). The current design of the DNPW application, however, issues a warning to the driver only when the driver activates his turn signal when changing lanes.

The current test metrics that are available also do not test the DNPW application's ability to function under a wide variety of roadway conditions (e.g., under various road curvatures which may exceed the capabilities of the path prediction algorithm). For example, as 25 percent of the opposite direction crashes resulting from a passing maneuver do occur under varying roadway conditions, the currently-available test metrics may need to be altered or supplemented in order to test for those conditions.

4. Left Turn Assist (LTA)

Left Turn Assist is an application that addresses left turn across path/opposite direction crashes that constitutes approximately 7.4 percent of all light vehicle crashes. Recent research suggests that while executing a turn, drivers activate the turn signal about 75 percent of the time.[199] Current performance and test metrics for LTA require turn signal activation to activate the safety application. Although the research has suggested potential methods to predict left turns without an active turn signal, either (1) the application will need more development to predict

[197] Analyses of Rear-End Crashes and Near-Crashes in the 100-Car Naturalistic Driving Study to Support Rear-Signaling Countermeasure Development (Lee, Llaneras, Klauer, & Sudweeks, 2007, Report No. DOT HS 810 846). See www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2007/Analyses%20of%20Rear-End%20Crashes%20and%20Near-Crashes%20(DOT%20HS%20810%20846).pdf (last accessed Mar. 4, 2014).

[199] Turn Signal Usage Rate Results: A Comprehensive Field Study of 12,000 Observed Turning Vehicles (Ponziani, 2012, SAE Technical Paper 2012-01-0261). See http://papers.sae.org/2012-01-0261/ (last accessed Jan. 29, 2014).

left turns without a signal or (2) this information should be used to discount the estimated safety benefits of this application when turn signal activation is the only indication of driver intent.

However, there is some risk that relying on driver intent may produce false warnings resulting from the ambiguities of determining driver intent to execute a left turn. Finally, more testing would be required to ensure the values are tuned to the optimal values to determine when to provide imminent or advisory warnings compared to the current metrics. Further testing and tuning may potentially minimize false warnings. The OEMs understand that the current configuration of LTA that requires turn signal activation to indicate driver intent limits the application's effectiveness. As indicated above, the OEMs agree that more development is needed to ascertain driver intent not only for LTA but for other crash avoidance applications. However, various OEMs have indicated that this work is OEM-specific and each will investigate other methods to ascertain driver intent to support their individual safety applications.

5. Intersection Movement Assist (IMA)

Intersection Movement Assist has the potential for significant safety benefits and cost savings. As designed, IMA should address five types of junction-crossing crashes. These crashes, which collectively represent 26 percent of all crashes occurring in the crash population and 23 percent of comprehensive costs, can be categorized as follows: straight crossing paths at non-signal, left turn into path at non-signal (LTIP), right turn into path at signal (RTIP), running red light, and running stop sign.

Initial Safety Pilot Model Deployment results indicated there is opportunity for this application to issue false warnings in a real-world environment. Various roadway geometries (e.g., cloverleaf, on-ramp, exit ramp) that do not represent a crash-imminent situation can be incorrectly classified as conflict situations by the system. Improvements to the IMA algorithm for the second stage of driver evaluations indicate these false warnings can be improved as the algorithms mature through additional testing. It may be necessary to develop new performance and test metrics that are designed to mitigate false warnings on different roadways such as curved roads and at non-perpendicular intersections.

6. Blind Spot +Lane Change Warning

Blind Spot Warning/Lane Change Warning is an application that provides an advisory alert when another vehicle occupies the adjacent lane in the driver's blind spot. This advisory elevates to a warning when the driver signals his intent to change lanes through the activation of the turn signal. An advisory is not elevated to a warning if a driver unintentionally drifts into an adjacent lane, i.e., does not indicate intent by activating a turn signal. Additionally, drivers infrequently use turn signals in lane change near-crash events (<26 percent turn signal use, based upon an unpublished analysis of IVBSS data).[200] As a result, the application has the potential to address at least 19 percent of the crashes in the lane change crash group.[201]

D. Key conclusions for each application

1. Forward Collision Warning

Current FCW applications based on visual and radar detection systems can be stymied by certain lighting and weather conditions, and are limited with respect to distance. FCW applications using V2V technology can function in environments and under conditions beyond the current visual and radar detection systems (e.g., sunrise, sunset, rain, snow, >300m range), allowing for a more robust warning system. Some further refinement of performance and test metrics is advisable to align V2V-based FCW applications better to the safety problem, and to more clearly specify each of those metrics with a supporting rationale. With further development of the performance and test metrics, potentially greater safety benefits can be realized with a V2V FCW application, or a combined V2V and sensor-based system, as compared to visual or radar-based systems without V2V.

2. Blind Spot Warning + Lane Change Warning

BSW/LCW is an application that provides an advisory alert when another vehicle occupies the adjacent lane in the driver's blind spot. This advisory elevates to a warning (LCW) when the driver signals his intent to change lanes through the activation of the turn signal.

As discussed, lane change maneuvers can be either purposeful or accidental, and they may or may not involve use of the turn signal. In order to cover the variety of potential crash situations, it is recommended that other indicators of driver intent and vehicle movement be identified in addition to the turn signal, as well as ways of measuring them for use in a LCW application. Finally, the test metrics established to evaluate these systems need to test the LCW when vehicles are traveling at varying speeds between the host vehicle and remote vehicle to align more closely with the safety need.

3. Do Not Pass Warning

Do Not Pass Warning has the potential to reduce crashes that are not easily addressed by the limited detection range and line of sight capabilities of radar or camera systems. Incremental safety benefits can be realized from Do Not Pass Warning alone; however, as currently designed

[200] Data provided by Dr. W. Najm in 5/3/13 email, based upon analysis of IVBSS data. See Docket No. NHTSA-2014-0022

[201] Depiction of priority light-vehicle pre-crash scenarios for safety applications based on vehicle-to-vehicle communications (Najm, Toma, and Brewer, 2013, Report No. DOT HS 811 732). See: www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print (last accessed Jan. 29, 2014).

with reliance on turn signal activation and with functional limitations under certain road conditions (e.g., road curvatures), the application's benefits may not be as large as those from other applications. As an addition to a suite of other V2V safety applications, DNPW may be useful for realizing safety benefits at little marginal cost.

However, when only considering this smaller portion of opposite direction crashes the DNPW application has the potential to be well-suited for addressing this crash problem because V2V communications afford vehicles a rich set of information (e.g., position and trajectory) regarding the other vehicles on the road over a long distance.

DNPW could offer improved range over sensor-based systems and it may be advisable to investigate fused V2V and sensors systems and their ability to address DNPW-related crash situations.

4. Left Turn Assist

Left Turn Assist addresses the majority of crashes at intersections in which the turning vehicle is using the left turn signal. As stated above, research suggests that approximately 75 percent of drivers use turn signals when executing turns. Although previous research[202] efforts have suggested potential methods to predict left turns without an active left turn signal, either (1) the application will need more development to develop prediction techniques or (2) the benefits for this application must be discounted when turn signal activation is the only indication of driver intent.

It may be advisable for LTA to also consider yaw rate and steering wheel angle along with turn signal activation, heading, and vehicle speed to help determine driver intent and whether to issue a warning. However, these additions could affect the implementation of aftermarket safety devices.

Overall, a driver's failing to activate turn signals when making left turns is the largest limiting factor to the effectiveness of this application, reducing the number of crashes this application could potentially address by 1.9 percent. The proper formulation of performance metrics needs to consider all real-world driving situations that can be addressed by the LTA application. If performance metrics cannot address certain real-world conditions, we may not be

[202] The Time Course of a Lane Change: Driver Control and Eye Movement Behavior (Salvucci and Liu, 2002, Transportation Research, Part F, 5(2): 123-132). See http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.73.2172&rep=rep1&type=pdf (last accessed Jan. 29, 2014); also See Modeling Differences in Behavior Within and Between Drivers (Liu, 2011) in Human Modeling in Assisted Transportation: Models, Tools and Risk Methods, in 15-22 (Cacciabue, Hjälmdahl, Lüdtke, Riccioli, Eds., 2011) at http://mvl.mit.edu/MVLpubs/MVL_10.10_Liu_HMAT2010_Springer.pdf (last accessed Jan. 29, 2014).

able to claim that the systems meeting those tests can address the safety risks of those real-world conditions.

5. Emergency Electronic Brake Light

Emergency Electronic Brake Light addresses the Lead Vehicle Decelerating scenario and shares some overlap in functionality with the Forward Collision Warning application. EEBL warnings could improve through the use of additional information, such as lane-level information, street-level information, roadway geometry and elevation, etc. EEBL operation could be revised to include different scenarios not covered by FCW that could provide distinct benefits for EEBL compared to other applications.

6. Intersection Movement Assist

Intersection Movement Assist has the potential to address each of the crash types for real-world junction crossings. As currently implemented, the application does not issue a warning and the test metrics do not test for warnings under certain circumstances, such as when a vehicle entering an intersection is moving at low speeds. The analysis of the currently-available research has uncovered a number of limitations of the performance and test metrics.

The current test procedures should be modified to reflect a greater range of speeds and a greater variety of road geometry configurations, particularly non-perpendicular intersections, curved roads, and overpasses (a false positive test) to allow for extended safety benefits to be claimed for these crashes. A wider range of testing, especially at higher speeds (representing real-world crash speeds), will require the development of safer protocols that reduce or eliminate the consequences of a crash during testing, such as using remote guided targets as opposed to real vehicles.

7. False warning improvement research

The agency has determined that additional research to mitigate false positive warnings for the V2V safety applications identified above would be beneficial. If false positive warnings are perceived as annoying by the driver, user acceptance could decline, and driver response to true warnings might be negatively affected. This research need has been identified and work is underway to establish the research plan and conduct the necessary investigation to determine how to improve upon the performance of V2V safety application advisories and warnings through mitigating false positives.

The opposite of a false positive alert is a false negative alert. False negative alerts are also referred to as missed alerts. A missed alert occurs when two equipped vehicles are in an imminent crash situation and the associated safety application does not issue an alert. Missed alerts may result in a crash occurring that could have been avoided.

Missed alerts will be analyzed as part of the Safety Pilot Model Deployment. A preliminary FCW missed alert analysis was conducted using the first 6 months of data. The analysis identified seven possible no-alert situations that mimicked other FCW alerts situations. After further analysis of the time-to-collision, and when the subject applied the brakes; none of the situations represented a missed alert. Given the analysis was limited to a single safety application and only used the first 6 months of data, additional analysis using the full Safety Pilot Model Deployment data set will need to be completed before a determination can be made concerning the disposition of V2V missed alerts.

Research Need VI-1 False Positive Mitigation

Research Activity: Evaluation of False Positive Warning Reduction Remedies

Description: Assess the capability and capacity of possible refinements to reduce frequency of false positive warning while maintaining crash avoidance effectiveness.

Target Completion: 2016 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

NHTSA will leverage knowledge and experience gained during the Safety Pilot to develop various false-positive tests that exercise the ability of the DSRC-based safety systems to discern real threats from non-threat situations.

8. Performance measures improvement research

The agency also identified several areas where performance measures could benefit from additional research for each V2V safety application. This research need has been identified and work is underway to establish the research plan and conduct the necessary investigation to determine how to improve upon the performance of V2V safety applications.

The systems included in the Safety Pilot Model Deployment were designed to meet only limited CAMP test specifications and performance requirements. Accordingly, it is possible that fewer false positive warnings may have been observed during the Model Deployment if those same systems were designed to meet all of the test scenarios specified by CAMP and/or those covered by additional research testing (e.g., Track 4, IVBSS).

Research Need VI-2 Safety Application Performance Measure Rationale

Research Activity: Safety Application Objective Test Procedures & Performance Requirements

Description: Develop a rationale to support each performance and test metric recommended for incorporation into an FMVSS.

Target Completion: 2016

Current or Planned NHTSA research addressing this need:

A component of developing certification level Safety Application Objective Test Procedures (included in the Research Need V-4 activities previously described).

Research Need VI-3 Practicability of Non-Ideal Driving Condition Testing

Research Activity: Safety Application Objective Test Procedures & Performance Requirements

Description: 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.

Target Completion: 2016 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

A component of developing FMVSS level Safety Application Objective Test procedures (included in the Research V-4 activities previously described).

Research Need VI-4 Fused and Non-Fused V2V Safety Application Test Procedures

Research Activity: Safety Application Objective Test Procedures & Performance Requirements

Description: 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).

Target Completion: 2016

Current or Planned NHTSA research addressing this need:

A component of developing FMVSS level Safety Application Objective Test procedures (included in the Research V-4 activities previously described).

Research Need VI-5 Performance and Test Metric Validation

Research Activity: Safety Application Objective Test Procedures & Performance Requirements

Description: Conduct test validation to ensure that the performance and test metrics are objective, repeatable, and practicable.

Target Completion: 2016

Current or Planned NHTSA research addressing this need:

A component of developing FMVSS level Safety Application Objective Test procedures (included in the Research V-4 activities previously described).

As a part of the agency’s research, it is prudent to have real-world validation of the performance and test metrics. In other words, we would ideally have some data to indicate that systems meeting the agency’s final performance requirements and test procedures in a potential FMVSS will address the safety problem as anticipated in the real world. This research need includes many components that are described above and capture in one comprehensive research activity, "Safety Application Objective Test Procedures & Performance Requirements" that has been previously described via Research Need V-4.

E. Driver-vehicle interface

While the current research-based performance and test metrics developed to evaluate the V2V safety applications are relatively robust, they do not focus on the driver-vehicle interface (DVI); an area that provides challenges not only for V2V safety but for many facets of vehicle safety devices and applications. The collaborative V2V research efforts of both CAMP and Volpe did not include the DVI as a research topic. Further, the Safety Pilot Model Deployment research was not designed to analyze and compare the different aspects of the various DVIs and, overall, the effect that specific aspects of the DVI have on safety benefits has not been clearly defined and quantified.

Other available research, such as the NHTSA Crash Warning Interface Metrics and Human Factors Connected Vehicle research projects, should yield results to help inform how the agency could proceed with more explicit guidelines or, potentially, standards for V2V DVIs. However, current available research does not yet have a method to evaluate the effectiveness of these DVI characteristics or to delineate a minimum standard for these characteristics. As a result, the DVI currently does not have performance or test metrics. Some characteristics of the DVI have research data to suggest ranges of potential performance metrics. However, these metrics were not determined considering the safety problem or a representative sample of U.S. drivers. Questions such as what are the best DVIs for particular safety applications and whether DVIs should be standardized for all vehicle types and manufacturers have not been answered.

Research Need VI-6 DVI Minimum Performance Requirements[203]

Research Activity: V2V DVI Safety Application Study (Mini-Sim- multiple sites) and V2V DVI Characterization Study

Description: Determine DVI's impact on effectiveness of system and safety benefits applications to establish minimum performance for crash avoidance and objective test procedures.

Target Completion: 2015

Current or Planned NHTSA research addressing this need:

This research need is being addressed by several existing projects that will result in the Development of DVI minimum performance requirements for various DVI characteristics.

[203] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

A potential regulatory action on V2V safety applications would not necessarily need to prescribe all elements of the DVI. However, at least some requirements (e.g., timing of the warning) are necessary not only to ensure that the DVI can effectively assist the driver in reacting appropriately to a crash-imminent warning, but also to ensure that warning requirements can be objectively evaluated.

F. Summary of major recommendations concerning safety applications

1) Conduct additional analysis to ensure that each performance metric is supported by a clear rationale (i.e., explain the safety risk/crash scenario that each metric is designed to address and how the metric will address that risk/scenario). The agency may need to conduct additional research to refine and validate the existing performance and test metrics against a variety of conditions under which crashes can occur.
    a) Consider the inclusion of non-V2V sources of information (radar, camera, etc.) in the development and validation process for performance and test metrics, and how to handle their operation if they co-exist on a subject vehicle.
2) Conduct additional research and analysis on Driver Vehicle Interface warning characteristics that can effectively enable drivers to react appropriately and avoid the crash.
    a) This research should consider the safety problem and a representative sample of U.S. drivers. The goal of this research should be to identify minimum DVI characteristics that are necessary.
    b) This research should also consider whether multiple warnings/alerts can occur under real-world driving conditions, how frequently they might occur, and whether it is appropriate to consider methods for prioritizing those warnings to ensure that drivers are able to interpret the warning.
3) Consider whether regulatory action on various aspects of the V2V system can/should be conducted independently (e.g., separate FMVSSs covering communications protocol/basic safety message and the available applications).
4) Conduct additional research to determine the minimum basic safety message broadcasting range and frequency that are necessary to support each V2V safety application. The minimum BSM range and frequencies found in this research would need to be considered in the implementation of a message congestion mitigation strategy (Sections V.E.1.c) and V.E.2.b)).

G. System compliance and enforcement

The Safety Pilot played a critical role in helping the agency to begin to understand what V2V system compliance and enforcement strategies and procedures might be necessary if the agency decided to proceed with rulemaking to require V2V technology. "Standing up" the Safety

Pilot environment, for example, required conducting informal certification and compliance activities to ensure that participating devices were interoperable and that safety applications were functioning according to the specifications developed for the pilot activity.

However, the kinds of compliance obligations that vehicle (and V2V device) manufacturers could face if NHTSA did proceed with rulemaking for V2V would likely be much more rigorous than anything faced by participants in the Safety Pilot. V2V devices *must be* interoperable in order for a V2V system to work properly; safety applications will not be effective if messages are not transmitted and received correctly. Assuming that the agency did decide to proceed with rulemaking, a standard requiring DSRC devices in all new vehicles would likely specify in detail (perhaps with some incorporation by reference of relevant parts of IEEE and SAE standards, which we would assume would be improved by that time to address the issues discovered during the Safety Pilot, etc.) exactly what specifications all related devices would have to meet. The agency recognizes that additional research and development is required to develop those specifications and accompanying test procedures, although we expect that much of the work completed to stand up the Safety Pilot can be leveraged as a foundation.

Research Need VI-7 Compliance Specifications and Requirements

Research Activity: DSRC Device Performance Requirements, and Test Procedures

Description: Development of performance requirements, test procedures, and test scenarios to evaluate a device's compliance with interoperability standards, security communication needs; and to support safety applications.

Target Completion: Onboard requirements (mid 2015), and draft test procedures (late 2015). Candidate performance requirements, test procedures, and test scenarios identified (late summer of 2015).

Current or Planned NHTSA research addressing this need:

The research need is addressed through activities previously described under Research Needs V-2 and V-3. This research will identify the initial level of performance requirements, test procedures, and test scenarios that will facilitate evaluating the compliance of DSRC devices.

Once NHTSA establishes a FMVSS, vehicle and device manufacturers would be required to certify that they comply with it in order to sell vehicles and devices. Non-compliance with a FMVSS could result in enforcement action by NHTSA (e.g., a requirement to recall affected vehicles and devices, an injunction from selling affected vehicles and devices until remedied, civil penalties). Additionally, if V2V devices develop a safety defect, manufacturers (both of vehicles and V2V devices) may also be subject to a recall. It is possible that manufacturers may choose to rely on some kind of third-party certification for V2V devices to ensure uniform adherence to NHTSA's requirements, but NHTSA would not expect to participate in that certification.

NHTSA may need to conduct further research into how to ensure that all V2V devices subject to a recall can be located, given the possibility that some devices may be mobile and go from vehicle to vehicle or owner to owner. Section VIII.B.3 discusses the possibility that for vehicles manufactured with V2V devices installed, the SCMS may be able to create a link at the time of manufacture between specific installed V2V devices or production lots of devices and enrollment certificates that later may help vehicle manufacturers and NHTSA identify defective V2V equipment. NHTSA worked with CAMP to identify and document alternative approaches that could be implemented to link device batches to enrollment certificates. However, it is not yet clear how such a linkage would be created for V2V devices that are not installed by the manufacturer, an important enforcement matter for NHTSA should the standards include aftermarket equipment.

VII. Public Acceptance

A. The importance of public acceptance

The Safety Act requires that FMVSSs issued by the agency be practicable, and an important part of that consideration is whether the public is expected to accept and correctly use the technologies installed in compliance with the standard. According to the case law, a standard issued by the agency will not be considered practicable if the technologies installed pursuant to the standard are so unpopular that there is no assurance of sufficient public cooperation to meet the safety need that the standard seeks to address.[204] Crash avoidance technologies in general, and V2V in particular, are new to consumers, and new technologies that can dramatically change the driving experience always have the potential to raise public acceptance issues. For V2V technologies, the extent to which the public understands and embraces the enhanced level of safety (and other mobility and environmental benefits) made possible by a V2V environment will need to outweigh the risks to individual privacy, actual or perceived, introduced by these technologies. Additionally, as a practical matter if not a legal one, industry acceptance and cooperation may be equally important, should NHTSA take steps to regulate V2V technologies via FMVSS, particularly since NHTSA is hopeful that industry will play a central or supporting role in establishing key components of the SCMS, which is required to support deployment of V2V technologies.

1. Potential key aspects of consumer acceptance for V2V communication

a) Enhanced levels of safety

V2V technologies can potentially provide considerable safety benefits, but consumers are more likely to accept V2V technologies quickly if they understand *how* vehicles with this technology can be safer. Crash avoidance technologies play, at first glance, a more abstract role in keeping consumers safe than crashworthiness features. If a driver avoids a crash, it may be difficult for the driver to detect whether it was the driver's own skill or the on-board technology that actually "saved" them, as compared to a crashworthiness technology like air bags, which clearly deploy to protect the driver and occupants in a crash. Consumers who cannot clearly see benefits to V2V technologies could be more tentative in their acceptance of V2V for longer than they might be with other safety technologies. Performing outreach to educate consumers on the safety benefits of V2V technologies, as well as on the privacy-protection methodology built into the V2V communications system, will likely be helpful to improving consumer acceptance, should the agency move forward with regulation. Some possible methods of public outreach

[204] *Pac. Legal Found. v. Dept. of Transp.*, 593 F.2d 1338, 1345-46 (D.C. Cir.), *cert. denied*, 444 U.S. 830 (1979).

include working with industry to produce and air Public Service Announcements (PSAs) and conducting publicly-accessible – and media-covered -- technology demonstrations with V2V-enabled vehicles nation-wide.

Preliminary research from the auto industry, however, seems to indicate that at least some members of the public would be interested in V2V-type technologies on their vehicles. On June 5, 2013, at the Telematics Detroit Conference, the Alliance of Automobile Manufacturers released poll results finding that a majority (59 percent) of consumers "believe that technological innovations such as driver-assist technologies are making cars safer, and 6 in 10 consumers want to check out these systems next time they buy a car."[205]

b) *Security from new forms of cyber-attack*

With increasing frequency, legislators and the media have raised questions about whether the prevalence of electronic control in today's high-tech motor vehicles has created new vectors (or sources) for cyber-attack on the motoring public. For example, during a hearing in 2013, Senate Commerce Committee Chairman Jay Rockefeller asked, "As our cars become more connected -- to the Internet, to wireless networks, with each other, and with our infrastructure -- are they at risk of catastrophic cyber-attacks?"[206] To date, NHTSA's V2V research has not included research specific to this issue, as researchers assumed that the possibility of cyber-attacks on motor vehicles was an existing vector of risk – not a new one created by V2V technologies. However, should the agency move forward with regulation, it may be important for improving public acceptance of the technology for us to assess, specifically, whether and how V2V technologies augment existing – or create additional – paths of cyber-attack that may affect motor vehicle security. The agency may also wish to explore the availability and appropriateness of measures to mitigate cyber-attack risks specific to V2V technologies (if any exist). Additionally, efforts to achieve consumer acceptance through public outreach and education on the benefits of V2V technologies may help to assuage public concern that V2V technologies will increase the danger of cyber-attacks on motor vehicles.

In the June 5, 2013, poll released by the Alliance mentioned above, it was also found that consumers, when questioned about self-driving vehicles, expressed concerns about cyber-security (i.e., 81 percent about a computer hacker controlling the car), companies collecting data from the self-driving cars (i.e., 75 percent), and companies sharing this information with the government (i.e., 70 percent). It is important to note that consumers were responding about self-

[205] Consumers Still Want to Be in the Driver's Seat, Self-Driving Cars Raise Concerns (Poll on Alliance Web site, June 5, 2013) at www.autoalliance.org/INDEX.CFM?OBJECTID=156688B0-CD5D-11E2-8898000C296BA163 (last accessed Jan. 29, 2014).

[206] U.S. to monitor cybersecurity risks as car connectivity grows (Automotive News, May 15, 2013) at www.autonews.com/article/20130515/OEM11/305159928#axzz2Z1OdGToG (last accessed Jan. 29, 2014).

driving vehicles and not about V2V communication specifically,[207] but their concerns about cyber-security and collection of data about their driving behavior are concerns that consumers could have regarding any sort of vehicle for which they believed could present such risks.

While the agency recognizes the difference in potential risk between V2V technologies that simply warn drivers about impending danger and technologies that actually intervene in driving, this distinction may not yet be so clear to consumers, and work could be done to make that distinction clearer to improve public acceptability of V2V (ideally without also negatively impacting acceptability of more advanced technologies).

c) Reasonable cost increases

Another component of consumer acceptance is cost. The extent to which consumers are willing to embrace V2V technologies will depend, in part, on the resulting cost increase in new motor vehicles. Generally speaking, cost as an issue for consumers has been considered in terms of whether it is high enough to cause many consumers to delay purchasing a new vehicle. It is not an issue that has been raised very often – but, if consumers delay purchasing of new vehicles in any significant way, presumably there will be a delay in the stream of expected benefits. This is an issue that the agency considers for any safety regulatory action that it undertakes.

The preliminary costs for V2V (initial cost estimated at about $350 and then decreasing with the learning curve) are less than some of the more notable safety equipment. For example, frontal air bags for the driver and right front passenger are estimated to cost $496, and antilock brake systems are estimated to cost $424 (all in 2012 dollars).

d) Privacy protection and acceptable levels of risk to exposure

Perhaps the most significant component of consumer acceptance in the V2V context will be the extent to which V2V technologies create consumer anxiety about risks to individual privacy, whether the risks are actual or simply perceived. As discussed below, if consumers believe—contrary to the actual facts-- that the V2V system as contemplated will enable the government or others to track the speed or location of their motor vehicles, the public may be less likely to support a regulatory mandate requiring the technology, regardless of any resulting enhancements to levels of safety.

Should the agency move forward with a V2V regulation, it will need to perform and make public a privacy impact assessment (PIA) of its proposed V2V FMVSS. Discussed in detail in Section VII, a PIA must capture and quantify all privacy risks introduced by proposed regulatory requirements, and assess the extent to which technical, physical and organizational controls designed to minimize such risks do so adequately. Once complete, the PIA will enable

[207] See Section VII.A.3.b) for NHTSA’s current findings on driver responses to similar topics in the Safety Pilot.

NHTSA (and DOT as a whole) to determine whether the level of residual risk to individual privacy, with all controls in place, is acceptable.

A critical part of any efforts to achieve consumer acceptance through public outreach will be assuring consumers that V2V technologies do not pose a significant threat to privacy and have been designed to help protect against vehicle tracking by the government or others. Additional privacy research and analysis (some of which will be folded into the agency's planned security and privacy risk assessments) is expected to provide NHTSA and DOT with an even more substantial basis for making such public assurances than currently exists.

2. Potential issues With industry support for V2V communication systems

Support from the automotive industry is not legally required in order for NHTSA to move forward with regulating V2V technology, but it is certainly desirable from a policy perspective, and may be important if the agency anticipates that the security system would be developed and stood up by an industry consortium. Industry support may be hindered by concerns about costs associated with the security system required to support V2V communications – who will bear the burden of such costs and, to the extent that it is the consumer, whether V2V can offer any "day one" benefits to consumers that justify the increase in new vehicle costs resulting from regulation of V2V technologies. Industry support also may be impaired both by uncertainty about how a regulatory action might impact in-vehicle crash avoidance systems, and by the perception by industry that V2V technologies will result in increased legal liability.

Additionally, for what appear to be largely economic reasons, industry support also will turn, in part, on the extent to which V2V technologies create consumer anxiety about actual *or perceived* risks to individual privacy. Industry members, through the VIIC and individually in meetings with NHTSA, have expressed concern that consumers will opt not to buy new vehicles if the agency mandates V2V technologies without protecting consumer privacy to the extent industry believes is necessary, and without providing consumers with assurances of privacy protection in a very public way, as through PSAs and public outreach.

Industry also may be able to use suggestions from the agency on how to facilitate consumer acceptance of V2V technologies if the agency eventually decides to require them. In addition to privacy, another factor that can be relevant to public acceptance of technologies is how well they work over the vehicle's lifetime. As discussed elsewhere in this report, we anticipate that BSMs will need to be accompanied by security certificates to establish their trustworthiness; if vehicles need to be resupplied periodically with certificates, or if vehicles need software upgrades regularly (or even occasionally), there may be consumer acceptance issues if receiving these certificates and upgrades requires what they consider to be undue effort or expense on their part. At the same time, however, if consumers reject the effort or expense, the systems may not function properly, which can cause other consumer acceptance issues. Ensuring appropriate consumer participation in V2V system maintenance will be a topic that the agency continues to explore.

3. Preliminary information on consumer acceptance

As part of its research thus far, the agency has accumulated some preliminary information on consumer acceptance of advanced crash avoidance systems (sensor-based and V2V-based).[208] This information provides an early look into consumer concerns and their perceptions on the value of these types of systems.

Based on our preliminary research described above, drivers generally have some interest in the new crash avoidance technologies, even if they do not yet have extensive knowledge about them. Consumers who have driven vehicles with crash avoidance technology appear to be generally positive about this technology, regardless of whether the technology is sensor-based or V2V-based. Exposure to specific crash avoidance technologies seems to increase drivers' interest in purchasing those same technologies in future vehicles.

However, even though consumers express interest in purchasing vehicles with crash avoidance technologies, public opinion polls do not show that drivers are willing to spend a lot of additional money in order to purchase vehicles with these systems. In contrast, there is some indication that use of currently-available crash avoidance technologies has resulted in reduced claims/losses for the owners of vehicles with these features.[209] If this trend continues and drivers determine that the new technologies can reduce their insurance costs, they might be willing to increase the amount of money they are willing to pay for a vehicle with crash avoidance technology.

The agency intends to supplement its preliminary research in the areas of consumer acceptance of V2V technology to better understand consumer behavior in reaction to these technologies. This research would help inform approaches for system implementation if the agency decides to move forward with a regulatory action.

[208] Independent Evaluation of the Driver Acceptance of the Cooperative Intersection Collision Avoidance System for Violations (CICAS-V), Pilot Test July 2011, (Stearns and Garay-Vega, Report No. DOT HS 811 497) and Integrated Vehicle-Based Safety Systems (IVBSS) Field Operational Test Final Program Report (Sayer, et al., June 2011, Report No. DOT HS 811 482) both at www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 29, 2014).

[209] More good news about crash avoidance, at 1-4 (Insurance Institute for Highway Safety, 2013, Status Report 48 (3)) at www.iihs.org/externaldata/srdata/docs/sr4803.pdf (last accessed Jan. 29, 2014).

Research Need VII-1 Consumer Acceptance[210]

Research Activity: Consumer Acceptance Research on V2V

Description: 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

Target Completion: 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

NHTSA will initiate Consumer Acceptance research in 2014.

a) Driver clinics conducted for connected vehicles and applications

As part of the V2V Light Vehicle Driver Acceptance Clinics project (conducted from September 2010 to March 2013), some preliminary assessments were made about whether and how drivers accept and respond to V2V safety technology. Beginning August 8, 2011, and ending January 21, 2012, four-day driver acceptance clinics were held in six cities,[211] with driver recruitment being conducted by independent recruitment agencies that used existing databases of known interested parties, advertisements, and/or cold-calling. At each clinic, around 112 drivers participated in a structured exposure to the V2V technology.[212] This exposure included completing pre-and post-drive questionnaires, receiving an oral and a video briefing about V2V technology, and being oriented to the vehicles and the course that would be driven. Clinic vehicles were supplied by nine OEMs, one from each OEM. Not all of the applications being assessed were included in each of the vehicles. In order for all of the participants to experience the majority of the safety features, some of the participants were asked to drive two different vehicles.[213] In addition, 104 drivers at each clinic participated in a focus group discussion about the V2V technology and their experience in driving these vehicles.[214]

[210] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

[211] Brooklyn, Michigan; Brainerd, Minnesota; Orlando, Florida; Blacksburg, Virginia; Fort Worth, Texas; and Alameda, California.

[212] Specifically, the EEBL, FCW, BSW/LCW, DNPW, IMA, and LTA applications.

[213] Participants driving the Ford, GM (Cadillac), Honda (Acura), or Mercedes were not asked to switch vehicles. Those driving the Toyota switched halfway to the Hyundai, and vice-versa, with similar switches being made between the Nissan (Infiniti) and the VW/Audi vehicles.

[214] Vehicle-to-Vehicle Safety System and Vehicle Build for Safety Pilot [V2V-SP], Draft Final Report, Volume 1: Driver Acceptance Clinics (April 10, 2014). See Docket No. NHTSA-2014-0022.

Key findings from the pre- and post-questionnaires[215] completed by drivers at these clinics include:

- Overall Impressions: Overall impressions of the V2V vehicles were positive, with approximately 85 percent of all responses considered to be positive. The most frequent negative response, accounting for only 4 percent of all responses, was a general "disliked the warning."

- Effectiveness: the majority of comments were positive regarding how effective the issued alerts were at communicating the direction of the scenario-specific threat (i.e., approximately 60 percent positive, with 22.5 percent giving a neutral response).

- Desirability: the desirability of the safety features was extremely high with 90 percent of participants agreeing that they would like to have the V2V communication safety feature in their personal vehicle.

- Intuitiveness: the intuitiveness of the vehicle's alerts was rated very high (i.e., approximately 89 percent of respondents felt that the alert issued was extremely effective at gaining their attention and directing attention to the threat. Similarly, 90 percent agreed that the alert issued was easy to understand.).

- System Limitations: Most respondents (61.1 percent) were unsure whether or not drivers might confuse one warning with another from a different safety feature, while 30 percent did not think this would be an issue.

- The majority of respondents (90.5 percent) would want to be notified whenever the V2V communication became unavailable; however, 43 percent of respondents stated that they would accept an unavailability rate of 10 percent or lower.

- The majority of respondents do not believe that the V2V benefit would be noticeable until 70-80 percent of vehicles are similarly equipped.

Some overall reactions by focus group members about V2V include:

- "Standard on all vehicles" was far preferred to the term "mandatory," which some respondents perceived as too controlling. Participants felt that communication efforts

[215] Safety Pilot: Preliminary Analysis of the Driver Subjective Data for Integrated Light Vehicles (Scott Stevens, July 2013, HS63A3 – Project Memorandum). See Docket No. NHTSA-2014-0022

around the system should avoid the word "mandatory" or other terms implying government control, but could use terms such as "your own personal co-pilot."

- Participants tended to agree that the benefits of saving lives and preventing or mitigating crashes far outweigh potential drawbacks such as driver dependency, complacency, and over-reliance on the system.

- Participants considered the scenarios experienced during the driving portion of the clinic as being very relevant and applicable to their everyday driving experiences.

- The applications considered the most appealing and/or relevant overall were FCW, BSW, EEBL, and IMA, although there was slight variation of this depending upon the region of the country that the respondent lived.

- Participants felt there were near-term problems (e.g., texting, disregard for rules, poor driving) that need to be addressed before starting a new, complicated, interdependent technology, even though there did not appear to be any short-term solutions in identified for these near-term problems.

- Participants' reactions to the various warning implementations used by the OEMs (e.g., visual, audible, haptic where present and the locations thereof) were mixed, but there was a fair amount of consensus around having the warning appear the same across OEMs to avoid confusion when driving different vehicles.

b) Model Deployment driver acceptance surveys

As part of the Safety Pilot Model Deployment project, assessments were made to determine whether and how drivers accept and respond to V2V safety technology. The V2V technology with which these vehicles were equipped included six safety applications that were developed to assist the drivers in avoiding risky situations that might result in a crash if the driver did not take corrective action: EEBL, FCW, BSW/LCW, DNPW, IMA, and LTA,[216] although not all of the applications being assessed were included in each of the vehicles.

During the first 6-month period (i.e., August 2012 to February 2013), half (i.e., 64) of the participants drove the vehicles, and, at the end of that 6-month period of time, filled out the driver acceptance survey. The remaining 64 drivers began driving the same OEM-provided and equipped vehicles at the beginning of the next 6 months of the pilot (i.e., February 2013), and

[216] See id., at 5, Table 1 for additional information on the safety features that were available by OEM.

they filled out the same driver acceptance survey at the end of the next second 6-month period of time (i.e., August 2013).

A preliminary analysis was conducted on the subjective survey data obtained from the drivers who drove the V2V-equipped vehicles for the first 6 months, and was reported in a July 2013 draft report. Overall, driver's responses were very mixed toward the V2V safety features, with a large proportion of drivers giving neutral responses. Their responses to "What did you like most about the Connected Vehicle system?" included "Alerted me to traffic situations I otherwise wouldn't have been aware of," but the drivers focused on the rate of alerts that they regarded as incorrect, with 42 percent citing incorrect alerts (e.g., distracting, not always clear, too short in duration), when asked what they like least.[217] Especially in regard to FCW, the false alerts appeared to have some effect on desirability of the FCW safety feature. The more false FCW alerts a driver believed they had received, the less they agreed with the statement, "I would like to have FCW on my personal vehicle."[218]

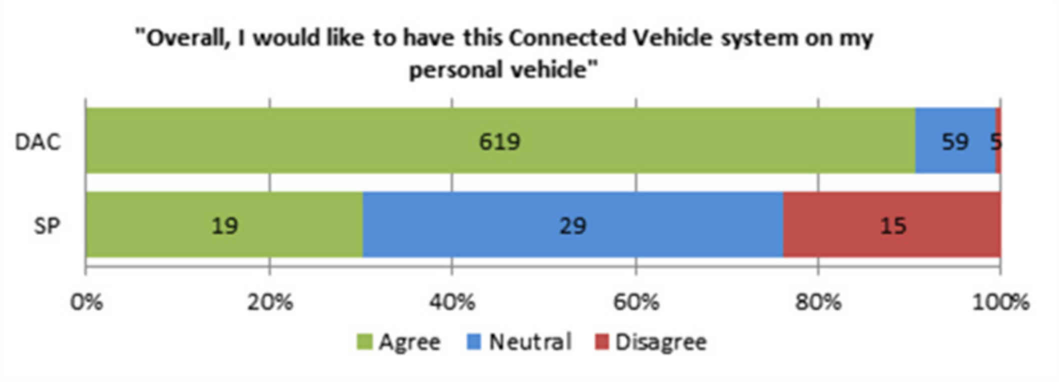
Since many of the driver survey questions that were used in the Driver Acceptance Clinics were used in the Safety Pilot Model Deployment, a comparison of results is possible. However, the light vehicle Driver Acceptance Clinics were staged demonstrations of the V2V technologies that were conducted using integrated vehicles by each of the eight OEMs between August 2011 and January 2012. The volunteers drove equipped vehicles on a closed course through a series of staged scenarios designed to illustrate how the different safety features could be of use, and only interacted with other vehicles driven by professional drivers. The main difference was the overall distributions of answers to the questions asked, with almost all drivers giving the highest rating for every system and question for the Driver Acceptance Clinics, whereas responses in the Safety Pilot Model Deployment were largely neutral. These results are not surprising given the differences in environment with the Driver Acceptance Clinics, a controlled demonstration, as compared to the Safety Pilot Model Deployment, a real-world driving situation. Table VII-1 and Figure VII-1 provide a sample of the distribution of driver responses.

[217] Id., at 9.
[218] Id., at 36.

Table VII-1 Comparison of Findings between Driver Acceptance Clinics and Safety Pilot Model Deployment during the First 6 Months

	Driver Acceptance Clinics	**Safety Pilot Model Deployment (Phase 1 Drivers)**
Would like to have V2V technology on their personal vehicle	91%	30%
Most highly rated safety feature	IMA	BSW/LCW
Said distraction was less than using car radio	75%	51%
Thought the system would not cause overreliance	42%	73%
Amount young drivers worried about overreliance compared to older drivers	more	Less
Main gender difference was	Higher ratings for the **EEBL** by women (more useful, desirable, effective, and understandable)	Lower ratings for the **IMA** by women (less desirable, effective, understandable, and with more incorrect alerts)
Generally more favorable ratings for the overall system from older drivers in both, especially for the **EEBL** (higher ratings of **FCW** among older drivers only seen in Safety Pilot Model Deployment)		

Figure VII-1 Full comparison of DAC and SP Driver responses



Upon completion of the Safety Pilot Model Deployment, the total data set, including the data from the second 6 months, will be analyzed to confirm the findings in this report. Since some changes were made to the safety applications that affected the false warning rates (i.e., decreased the number of false warnings), this analysis could prove to be very useful, in examining the rate and amount of change of a driver's opinion about a V2V safety application as the false warning rate decreases. Information gained from this analysis can be used to judge future driver opinions of V2V safety applications, as the applications are improved, based upon the information obtained in the Safety Pilot Model Deployment.

Preliminary indications are that driver acceptance of the IMA application improved in the last 6 months of the project. This improvement in driver acceptance correlates with the enhanced performance of the IMA application as a result of changes by the OEMs to address the sources of concern, especially what were perceived as false warnings. Generally, the applications used in the Model Deployment were not fine-tuned to suppress false warnings in situations where production systems would. Continued refinements, to the extent possible for IMA and other V2V applications, may help address some of the concern without affecting the effectiveness of the systems.

The survey also attempted to gauge participants' concern with regard to privacy issues through four questions: "How willing would you be to have Connected Vehicle technology on your vehicle that, when combined with other information may allow:

A) A business entity to learn about your vehicle's location and travel patterns?

B) The government to learn about your driving behavior and patterns?

C) A third party organization to learn about your driving behavior and patterns?

D) Appropriate personnel to determine criminal behavior such as hacking?

Note that these questions were intended to address possible perceptions, not the reality of the contemplated system, which is not designed to permit the collection of the types of data referred to in questions A through C.

In response, drivers did express concern about privacy with V2V technologies, with over half declaring that they were "not willing" to have businesses, government, or a third party organization learning about their driving behavior and patterns. When the idea of criminal behavior such as hacking was introduced, this number fell to 28 percent, indicating more people would be willing to accept some level of tracking. This is the clearest expression that the agency currently has of driver opinions of V2V privacy issues when drivers have actually experienced V2V technology over an extended period of time. While a larger sample set would be more informative, these results indicate that this is an issue that the agency needs to consider carefully as implementation proceeds.

VIII. Privacy Considerations

A. Privacy considerations – what they are and why they are important

Risks to consumer privacy, whether actual or perceived, are intertwined with consumer and industry acceptance of V2V technologies. For this reason, privacy considerations are critical to the analysis underlying NHTSA's decision about whether and, if so, how to proceed with V2V research or regulation.

At the outset, readers should understand some very important points about the V2V system as contemplated by NHTSA. The system will not collect or store any data on individuals or individual vehicles, nor will it enable the government to do so. There is no data in the safety messages exchanged by vehicles or collected by the V2V security system that could be used by law enforcement or private entities to personally identify a speeding or erratic driver. The system—operated by private entities—will not permit tracking through space or time of vehicles linked to specific owners or drivers or persons. Third parties attempting to use the system to track a vehicle would find it extremely difficult to do so, particularly in light of far simpler and cheaper means available for that purpose. The system will not collect financial information, personal communications, or other information linked to individuals. It will enroll V2V enabled vehicles automatically, without collecting any information identifying specific vehicles or owners. The system will not provide a "pipe" into the vehicle for extracting data. The system will 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.

Generally, privacy considerations inherent in mandated V2V technologies include such issues as:

- Should the V2V system provide "anonymity"[219] for drivers, as suggested by industry, in order to prevent location tracking and otherwise protect individual privacy?
- Should the V2V system provide "anonymity" for drivers *even if* doing so:
    - Prevents identification and prosecution of hackers accessing computers or data on the V2V system without authorization?

[219] The VIIC has defined "real anonymity" as "end-to-end anonymity" (i.e., no collection of any personally-identifying information at any time in connection with bootstrapping or provision of security services or mandatory applications). By contrast, NHTSA avoids use of the term "anonymity" in the V2V context, in recognition of the fact that some limited risks to individual privacy exist in the current V2V design even through it does not provide for collection of any individually identifying information.

    - Impedes NHTSA’s ability to investigate and recall defective V2V motor vehicle equipment (i.e., for highway safety purposes)?
- Or, for system security and/or highway safety purposes, should the V2V system collect data that may link location or other information that drivers may potentially perceive as sensitive (e.g., speed) to an individual driver or vehicle, either directly or indirectly?
- Are there ways to satisfy NHTSA’s need to identify potentially defective V2V devices without collecting data that may link location or other potentially sensitive information (e.g., speed) to an individual driver or vehicle, either directly or indirectly?
- Can a V2V system with no mechanism for identifying or tracking down hackers or other “bad actors” be sufficiently secure for NHTSA or consumers to rely on?
- What specific risks to privacy stem from the V2V system? How likely is the potential occurrence of such risks? What would be the extent of harm if the events occurred? For example, to what extent do either the SCMS design or the unencrypted BSM introduce privacy risks, including but not limited to the risk of location tracking?
- What physical or technical controls should the V2V system contain to mitigate location tracking and other privacy risks “by design”?
- What policy or organizational controls should the V2V system contain in order to minimize the likelihood of unauthorized access to insider information that could facilitate tracking or create other risks to privacy?
- What role, if any, *should* or *can* the Federal Government play in assuring individual privacy in connection with mandated V2V technologies – especially if it plays no role in owning or governing the SCMS?
- Is Federal legislation necessary to protect consumer privacy adequately in the context of a mandated V2V FMVSS, as suggested by CAMP and the VIIC?

1. Transmission, collection, storage, and sharing of V2V data

There are two primary categories of V2V system functions that involve the transmission, collection, storage, and sharing of V2V data by, and between, the V2V system components and other entities: system safety and system security.

The V2V system’s safety functionality (i.e., the safety applications that produce crash warnings) requires that V2V devices in motor vehicles send and receive a basic safety message containing information about vehicle position, heading, speed, and other information relating to vehicle state and predicted path. The BSM, however, contains no personally identifying information (PII) and is broadcast in a very limited geographical range, typically less than 1 km. Nearby motor vehicles will use that information to warn drivers of crash-imminent situations. Except in the case of malfunction, the system will not collect and motor vehicles will not store the messages sent or received data sent/received by V2V devices.

The security needs of the V2V system require the exchange of certificates and other communications between V2V devices and the entity or entities providing security for the V2V system (i.e., the Security Certificate Management System). These two-way communications are encrypted and subject to additional security measures designed to prevent SCMS insiders and others from unauthorized access to information that might enable linkage of BSM data or security credentials to specific motor vehicles.

NHTSA also needs to ensure that the V2V system is protected from defective devices. This agency safety function is likely to require that the V2V security system collect and share, on a very limited basis, some V2V data linking V2V device production lots to security credentials. Neither the V2V system nor NHTSA will collect, store or have access to information that links production lots of defective V2V devices with specific VINs or owners.

2. Privacy policies framework

Industry members, via CAMP, the VIIC, and in individual OEM meetings with NHTSA, have suggested that the Federal Government should play a central role in protecting individual privacy in the V2V context, through regulation or governance over the SCMS. Both CAMP and the VIIC have taken the position that the security system for V2V technologies should conform to the central tenets of the VIIC Privacy Policies Framework (version 1.0.2), dated February 16, 2007. That document would require that the security system:

- Collect and transmit only "anonymous" data from mobile users for mandatory applications
- Keep such data "anonymous" until securely destroyed
- Collect PII only with consent of the consumer
- Use/transmit that PII only in ways to prevent misuse/leakage and unauthorized attacks on the system

On the basis of these general tenets, the VIIC has identified as specific security system requirements:

- End-to-end anonymity for privately owned/leased vehicles and occupants for all mandatory V2V technologies, including security system processes (bootstrapping and certificate distribution) and mandatory applications and services
- For mandatory services, no ability to track specific identified vehicles across space and time, concurrent or after-the-fact
- Protection from attacks on system integrity, including from hackers and system administrators (i.e., "insiders"), by:
    - Providing secure, end-to-end encryption of vulnerable communications;
    - Changing short-term security certificates and vehicle identification every few minutes to prevent location tracking;
    - Assigning certificate signing requests (CSRs) - now called Enrollment Certificates or Long-term Certificates -- in an anonymous fashion;

  - Providing for multiple, legally/administratively separate SCMS entities with distinct governances, none of which have sufficient knowledge, information, or means necessary to link short-term certificates to CSRs/Enrollment Certificates and ultimately to vehicles/OBE, all of which should be prohibited "by law" from allowing or colluding to achieve re-identification;
  - Providing sufficient security to prevent hackers, users, and system administrators from accessing or deriving any information that can be linked, directly or indirectly, to individuals, motor vehicles, or OBE (e.g., via VIN or vehicle-specific part numbers).

CAMP and the VIIC also have taken the position that Federal legislation implementing the Privacy Policies Framework (as well as other policy and technical aspects of DSRC deployment) is necessary to provide adequate privacy protections for consumers in the context of mandated V2V technologies.

NHTSA takes privacy very seriously. If NHTSA moves forward with regulating V2V technologies, we are committed to doing so in a manner that both protects individual privacy and promotes this important safety technology. In NHTSA's view, the VIIC's 2007 Privacy Policies Framework provided an initial framework and useful starting point for development of privacy-protective V2V technologies. However, both V2V technologies and policies impacting privacy have continued to evolve over the last six years. Additionally, since 2007, DOT and V2V stakeholders have identified mission-critical and system-specific safety information needs that affect system privacy and have necessitated development of various additional controls to mitigate adverse privacy impacts. For these reasons, some aspects of the tenets and specific requirements set forth in that document no longer may be viable.

For example, in order to preserve anonymity and prevent tracking, the 2007 Privacy Policies Framework envisioned the creation/collection of no data whatsoever that could link a security certificate that authenticates a V2V message to the on-board device or motor vehicle that generated that message. However, as discussed below, in order for NHTSA to investigate and ensure the recall of defective V2V equipment, the security system must collect/store data that facilitates linkage between some categories of misbehavior reports (to be identified as the misbehavior functions mature) and the production lots of V2V equipment that generated those messages. Without collection by the SCMS of such information, NHTSA will not have an adequate basis on which to ensure the system's protection from defective devices.

As detailed below and elsewhere in this report, by design, V2V devices will transmit safety information in a very limited geographical range. Nearby V2V devices will use that information to warn drivers of crash-imminent situations. As currently designed, the system and V2V devices do not intend to collect or store the contents of messages sent or received. However, in the case of malfunctions, a limited number of BSM elements relevant to assessing performance will be stored, but in a manner designed to preserve personal privacy to the maximum extent possible, consistent with the need to address the root cause of the malfunction if it is, or appears to be, widespread.

We have worked closely with CAMP and the VIIC to develop a technical and policy approach that helps guard against risks to individual privacy. As conceived, the system will contain multiple technical, physical, and organizational controls to minimize privacy risks – including the likelihood of vehicle tracking by individuals and government or commercial entities. Additionally, even though V2V is still in a research phase, DOT's Chief Privacy Officer and Office of the General Counsel and NHTSA's Offices of the Chief Counsel and Chief Information Officer have worked closely with the DOT research team throughout the life of the project to identify and assess the privacy implications of the V2V system and DOT's related mission needs. For example, DOT's Privacy Officer worked with the Office of the Chief Counsel of OST-R and the Office of the General Counsel to publish a Systems of Records Notice covering collection of personally identifying information during the Safety Pilot and, in so doing, identified appropriate controls to mitigate risks to individual privacy associated with that effort.[220] These offices also supported the NHTSA's V2V team in its initial assessment of the possible privacy risks associated with the V2V system (detailed below).

As aspects of the V2V system (such as the misbehavior functions, communications media, and ownership/governance models) become more defined, NHTSA will continue to work with the Department's Privacy Officer and Office of the General Counsel to assess and reassess any threats to privacy that may be introduced by V2V technology and help identify mitigation measures to minimize any such risks. Additional discussion of NHTSA's interim privacy risk assessment and next steps can be found in Section VIII.B.

3. The fair information practice principles

DOT and NHTSA privacy assessments are based on the framework of the fair information practice principles (FIPPs). Rooted in the tenets of the Privacy Act, the FIPPs provide a foundation for the privacy laws of multiple States, Federal and international governments, and organizations. A FIPPs-based analysis is predicated on privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council, and the Privacy Controls, articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.

[220] 77 Fed. Reg. 12641 (Mar. 1, 2012) at www.gpo.gov/fdsys/pkg/FR-2012-03-01/pdf/2012-4964.pdf (last accessed Jan. 30, 2014).

The control families consist of:

- **Transparency**: What mechanisms will provide the consumers with information about the data being collected and transmitted by the V2V system and how that data will be used?
- **Individual Participation and Redress**: Will consumers have a reasonable opportunity to make informed decisions about the collection, use, and disclosure of their PII, if collected, or other data that may be used to identify them, directly or indirectly? Will they be active participants in decisions regarding the collection and use of their data?
- **Purpose Specification**: For what purposes is the system collecting, using, maintaining, or disseminating the specific data elements or categories of data being collected? (for example, here is where NHTSA might indicate that V2V data collected by roadside infrastructure will be aggregated, de-identified, and transmitted for use in mobility, environmental, and/or commercial applications)
- **Data Minimization**: Explain why the data collection isn't excessive and how long the data will be retained
- **Use Limitation**: Assure the subjects of the data collection that the data will not be used for purposes incompatible with the purpose for which it was collected (as detailed in the purpose specification section)
- **Data Quality and Integrity**: How will the system assure data quality and integrity throughout the data lifecycle and in all business processes associated with data use?
- **Security**: What physical, technical and procedural measures will system administrators take to protect the data? The PIA's analysis of security controls in the security system that mitigate privacy risks should be specific enough to provide consumers with a comprehensive understanding and adequate assurance that information is protected – but not provide a roadmap for would-be hackers to attack the system.
- **Accountability and Auditing**: How does system ensure that the privacy controls outlined above are executed?

The answers to these questions and the specific controls that NHTSA will need to identify and require, if consistent with our legal authority, within each of the control families, will flow from a technical privacy risk analysis of the V2V system. This analysis will be conducted once now-fluid aspects of the security system design (e.g., misbehavior management) are closer to finalization, once the agency knows how the SCMS will be managed (e.g., owned, organized, and operated), and once the agency knows what communications media will be selected by the SCMS owners for messaging between the SCMS and V2V devices.

A draft Privacy Impact Assessment (PIA), based on the agency's technical risk analysis, would need to be completed and ready for publication concurrent with any NPRM that NHTSA may issue, should it move forward with regulatory action. A PIA is an analysis required by the E-Government Act of how the V2V system handles information in identifiable form[221] to:

- Ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and,
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[222]

The draft and final PIA will document how DOT has considered and analyzed privacy from the beginning stages of the V2V system's development throughout the system's life cycle (i.e., collection, use, retention, processing, disclosure, and destruction). The PIA also gives the public notice of this analysis and helps promote trust between the public and the Department by increasing transparency of the Department's systems and missions.

In order to conduct this comprehensive privacy risk assessment of the V2V system as part of a V2V regulatory action, NHTSA will need to identify and quantify the level of any privacy risks stemming from each of the three discrete areas of the V2V system -- the OBE/DSRC messages, the communications media for messaging between the SCMS and V2V devices, and the SCMS. Although a PIA cannot be finalized until a draft NPRM exists, most of the technical analysis can be completed well in advance of that time. The next section describes NHTSA's work on a PIA to date.

B. NHTSA's interim privacy risk assessment

NHTSA, with the support of the DOT Privacy Officer and NHTSA's Office of the Chief Information Officer, conducted an interim privacy risk assessment of the V2V system. As multiple aspects of the system design remain in flux, the initial privacy risk assessment was

[221] The E-Government Act of 2002 applies to "information in identifiable form." The National Institute of Standards and Technology (NIST) has stated that the term "information in identifiable form" is "[o]ften considered to have been replaced by the term PII [personally identifiable information]." See Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Appendix C (April 2010, NIST Special Publication 800-122) at www.nist.gov/manuscript-publication-search.cfm?pub_id=904990 (last accessed Jan. 29, 2014). However, NIST also notes that terms such as "information in identifiable form" are similar to NIST's definition of PII and "organizations should not use the term PII (as defined in this report) interchangeably with these terms and definitions because they are specific to the ir particular context." Id.

[222] OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003, OMB Memorandum, M-03-22, Attachment A, Section II.A.6) at www.whitehouse.gov/omb/memoranda_m03-22 (last accessed Jan. 29, 2014).

based on a "snapshot" of the V2V system envisioned by the CAMP/DOT research team. In addition, this assessment assumed that SCMS would have one important additional capability (not a part of the prototype security system design) required to address NHTSA's need for information to support its defect investigation and recall duties.

The initial privacy risk assessment contains an important caveat, namely, that *further development of the technology or organization of the V2V system is likely to result in changes – possibly significant changes -- to the interim privacy analysis and findings.* For this reason, the interim assessment was intended to provide the structure and serve only as a robust starting point for NHTSA's definitive assessment of risks to privacy that could stem from a V2V regulatory action. As the V2V system and NHTSA's procedural posture evolve, so too will the scope of and detail in this privacy assessment.

The primary system components analyzed were:

1. The **OBE and BSM** – On-Board Equipment (OBE) as well as BSMs containing unencrypted GPS/location data required for V2V safety applications;
2. The **Communications Network** – use of DSRC, cellular, or other communications media to transmit encrypted security-related messages between OBEs (and possibly RSEs) and the SCMS; and
3. The **SCMS** – the organizations/functions/infrastructure providing PKI security to the V2V system.

Our interim analysis assumed that any V2V system deployed through a NHTSA regulatory action will have a capability not inherent in the latest SCMS design: the ability for DOT and/or the V2V equipment manufacturers to access information that links problematic certificates/messages collected by the SCMS with production runs or lots of potentially defective V2V equipment. This capability would have ensured that information NHTSA needs for defect and compliance purposes is collected by OEMs and/or relevant SCMS entities and made available to the agency in a timely manner.

As is the case with all such analyses, NHTSA's interim risk assessment included the following procedural steps:

- **Establish Business Needs:** What are the critical business needs that a V2V system must satisfy?
- **Identify System Functions:** What system functions serve those business needs?
- **Identify Data Needs/Transactions:** What data needs/transactions stem from the identified system functions?
- **Describe Nature of Resulting Risks:** What risks result from the collection, storage, or dissemination of data on the system? Do the data transactions increase privacy risks to existing related systems (both safety and security systems within a motor

vehicle, and opt-in systems like OnStar that collect motor vehicle data from on-board systems and transmit it elsewhere)?

- **Identify and Explore Technical/Policy Controls:** As currently envisioned, what technical and policy controls mitigate the identified privacy risks? Should there be others?
- **Determine Likelihood:** What is the likelihood of the risks? Likelihood is calculated for threat, vulnerability, and impact as part of the risk impetus (i.e., an individual or organization's motive for engaging in the activities creating the risk), not the risk itself. This can be expressed as, $L = [(T * V)/I]$. This inquiry necessarily must take into account the relative cost and ease of access to the same data via existing technologies and data sources.
- **Quantify Resulting Risks:** On the basis of consequence/harm and likelihood, what is the impact of the resulting risks, can those risks be mitigated by any controls, and are there risks that remain unmitigated (i.e., residual risk)? Residual risk comes from the application of controls to the risk set $RR = R – I$.
- **Assess Consequences/Harm:** What are the consequences of the potential risks identified?

It is important to emphasize that residual risk stemming from the V2V system will never be zero due the inherent complexity of the V2V system design and the diversity/large number of interacting components/entities, both technological and human. Additionally, technology changes at a rapid pace and may adversely impact system controls designed to help protect privacy in unforeseen ways. For these reasons, as is standard practice in both the public and private sectors, the primary function of a privacy risk assessment is to identify residual risk and its potential consequence/harm. On the basis of that critical information, agency decision-makers then will be in an informed position to determine whether that residual risk is acceptable – and, in the alternative, whether functionality should be sacrificed in order to achieve an acceptable level of residual risk, and if so, what functionality.

On the basis of then available information and stated assumptions, NHTSA's interim risk assessment identified the system's business needs, relevant system functions, nature of the resulting risks, and existing/other technical and policy controls. It also captured the team's attempt to provide an initial rough estimate of the extent, likelihood, and consequences/harm of risk stemming from the system. There was consensus among the team members that, should NHTSA proceed with regulatory action, DOT will need to obtain technical input from external security and privacy experts by proceeding with planned privacy research. Such research will help us to make a more fine-grained estimation of the extent, likelihood, and consequences/harm of risk stemming from the V2V system. It also will assist the Department and NHTSA in garnering public support for V2V by providing technical data to support NHTSA's position that the V2V system protects the privacy of participants and makes geo-locational tracking highly unlikely.

It is important also to note that NHTSA's interim privacy assessment did not take into account the business or informational needs of other DOT modal administrations, other Federal agencies (such as DOJ, DHS, FCC, and FTC), and State and local stakeholders. NHTSA will need to consider whether to expand our assessment to identify and analyze the different or additional privacy risks that may stem from the V2V-related activities and needs of other entities. For example, the safety, mobility, and environmental V2I and V2X applications being developed primarily by FHWA, FMCSA, and their respective stakeholders might generate different or additional information needs. The FTC, as the entity that regulates the privacy relationships between private entities and consumers, may have some interests in the privacy practices and controls (including information collection) designed into V2V security system if the system ends up being owned and managed privately. Finally, the FCC, as regulators of the spectrum, might have informational needs related to their enforcement functions, the collection of which could impact our privacy risk assessment.

1. V2V system needs/functions that necessitate data transactions posing potential risks to privacy

NHTSA's interim privacy analysis identified three categories of V2V system needs/functions that pose potential risks to privacy during data transactions:

- System safety (BSM data sent/received by V2V devices to enable safety applications)
- System security (certificates and other communications between V2V devices and SCMS)
- Agency safety and enforcement functions (data linking V2V device production lots to long-term enrollment certificates)

The critical foundation for NHTSA's privacy risk assessment is the data collected, transmitted, stored and disclosed within, by, and between the V2V system components and other entities. The team identified several data needs/transactions that could introduce privacy risks into the V2V system, including:

- The collection, transmittal, storage, and potential uses of unencrypted GPS and related path history information used in safety applications;
- The collection of data linking long-term security credentials with production runs/lots of V2V equipment used by NHTSA in investigation and recall purposes;
- The certificate and related linkage/bundling data collected and transmitted within the various functions of the SCMS used for distributing certificates; and
- The transmission and storage of location information broadcast when cellular (a potential communication option) is used as a method of communication between V2V devices and the SCMS for security-related purposes used for distributing certificates and other security-related communications.

2. Potential risks to privacy introduced by V2V communications or other data transactions necessary to satisfy system need

The team identified the following potential risks to privacy in the V2V system on the basis of the V2V data transactions that are necessary to satisfy system needs: (a) location tracking via BSM; and (2) identification of individuals and individual behaviors.

a) Location tracking via BSM

NHTSA is aware of concerns that the V2V system could broadcast or store BSM data (such as GPS or path history) that, if captured by a third party, might facilitate very-localized vehicle tracking. In fact, the broadcast of unencrypted GPS, path history, and other data characteristics in or derived from the BSM appears to introduce only very limited potential risks to individual privacy. Preliminary research performed for NHTSA suggests that tracking a specific car or driver based on BSM would be both difficult and costly. Nevertheless, the likelihood of tracking – or availability of information and technologies that facilitate linking location or other BSM data to a specific motor vehicle, address, or person – will be a key inquiry for DOT/NHTSA and their privacy and security consultants going forward.

Research Need VIII-1 V2V Location Tracking via BSM

Research Activity:	Privacy Risk Assessment of V2V System
Description:	Assess the availability of information and technologies that facilitate linking data in the BSM to determine a motor vehicle's path
Target Completion:	2015 (draft report to NHTSA)
Current or Planned NHTSA research addressing this need:	
NHTSA will conduct a privacy risk assessment of the V2V system that includes an analysis of the ability of vehicles to be tracked via BSM transmissions and the resultant impact of possible tracking to an individual's privacy	

It is theoretically possible that a third party could try to capture the transitory locational data in order to track a specific vehicle. However, we do not see a scenario in which one wishing to track a vehicle would choose the V2V system as the means. Nevertheless, NHTSA is conducting further research to accurately assess the level of privacy risk inherent in the broadcast of unencrypted BSM data.

Other methods exist for tracking a vehicle's location path, such as through electronic emanations from the car itself or from on-board electronics such as cell phones (although DOT consultants advise that both methods are expensive and difficult) and use of a single identifier broadcast from the vehicle (e.g., E-ZPass, OnStar™). NHTSA's planned comprehensive privacy risk assessment will need to consider the ease and cost of other methods of location tracking in connection with assessing the likelihood of location tracking via data in the unencrypted BSM.

b) Identification of individuals and individual behaviors:

Because a BSM does not identify a specific vehicle or individual, the V2V system as currently designed would not provide such a clear link to a driver or owner. However, the ease with which BSM data characteristics may be used to identify, either directly or indirectly, a specific vehicle, driver, or owner will be a subject of ongoing research and will be central to NHTSA's assessment of the likelihood of various risks to privacy.

Research Need VIII-2 V2V Identification Capabilities

Research Activity: Technical Analysis of the Potential Privacy Risk of V2V Systems

Description: 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)

Target Completion: 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

NHTSA will conduct a privacy risk analysis of the V2V system that includes an investigation of the use of BSM records to identify a vehicle, address, or individual.

At the component level, the specific potential tracking risks include:

- **OBE/BSM**: Location tracking via radio identification
- **Network Communications**: Location tracking via cellular IP address or computer-specific Wi-Fi address
- **SCMS**: Location tracking via after-the-fact reconstruction of GPS info in linked security certificates

3. Technical, physical and/or policy controls evaluated to minimize potential privacy risks

Generally, privacy risk controls fall into 3 categories:

- **Physical Controls**: Physical protections that reduce privacy risks (for example, a tamper-proof casing around the computer module storing a motor vehicle's certificates or high-security access procedures to gain physical access to an SCMS server facility)
- **Technical Controls**: Data-protective technologies designed into a system
- **Policy Controls**: Laws or organizational policies that make unauthorized data collection, storage, or disclosure less likely by creating organizational and/or functional separation and imposing organizational or legal consequences against hackers or malfeasant insiders

The current V2V security design contemplates a PKI security system that makes use of both asymmetric and symmetric keys and other technical, organizational, and policy controls (including, as applicable, compliance with the Privacy Act, FISMA[223] and other Federal statutes, regulations and policy relevant to privacy in Federal information technology systems) intended to prevent or make far more difficult tracking of devices, either contemporaneously or after the fact. Examples of technical controls in the current security design intended to minimize the risk of tracking via linking of security credential information in the unencrypted BSM include 5 minute certificates and shuffling of certificates prior to reuse.

The SCMS design also anticipates policy controls like organizational and/or functional separation, and organizational consequences to deter collusion that might enable tracking, such as separation of the enrollment function from the certificate issuance/distribution functions; separation of the certificate issuance and distribution functions; and having several certificate shuffling and location-obscuring functions.

As discussed above in connection with governance, ultimately, the SCMS Manager will be the entity that establishes and enforces physical, policy, and technical controls that are applicable to: (1) all of the CME entities that make up the SCMS, and (2) the communications media used by CME organizations to communicate with both V2V devices and RSE. Once greater clarity of the SCMS structure and governance emerges, we will need to inventory and assess the privacy controls applicable to the SCMS in connection with our comprehensive privacy risk assessment.

Research Need VIII-3 V2V Inventory of Privacy Controls

Research Activity: Technical Analysis of the Potential Privacy Risks of V2V Systems

Description: Inventory and assess the privacy controls applicable to the SCMS in connection with our comprehensive privacy assessment

Target Completion: 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

NHTSA will conduct a privacy risk analysis of the V2V system (Research Need VIII-4) that includes the development of an inventory and assessment of privacy controls.

4. Significance of the identified potential privacy risks

Assessing the significance of the potential risks to privacy that stem from the V2V system, in light of identified controls to mitigate those risks, is the final step in a comprehensive privacy analysis. With the help of subject-matter experts, NHTSA will need to quantify the level

[223] Federal Information Security Management Act of 2002.

of each potential privacy risk. The level of privacy risk (typically categorized as high, medium, and low) is a function of:

a) Adverse impacts to privacy that would arise if the circumstance or event occurs; and

b) Likelihood of Occurrence (which necessarily must take into account the relative cost and ease of access to the same data via existing technologies and data sources).

Thus, Privacy Risk = Impact x Likelihood.

Overall, based on present information and our interim privacy assessment, we have reason to believe that a properly-designed V2V system would curtail any serious risks to privacy. The agency acknowledges there may be no way to *entirely* eliminate privacy risks from the V2V system, but believes the efforts expended to develop robust security system designs to protect individual privacy collaboratively through our cooperative research efforts appear to meet that need. However, NHTSA intends to perform an even more comprehensive and definitive assessment of any proposed regulatory action to identify potential risks to privacy and ensure that appropriate controls are in place to help mitigate such risks.

Research Need VIII-4 V2V Privacy Risk Assessment[224]

Research Activity: Technical Analysis of the Potential Privacy Risk of V2V Systems

Description: 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. This assessment will include previously identified Research Needs in this section: V2V Location Tracking via BSM; VIII-2, V2V Identification Capabilities; and VIII-3, V2V Inventory of Privacy Controls

Target Completion: 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

This privacy risk analysis will provide the information about the latest security design and related privacy risk to enable the Department to perform a comprehensive Privacy Impact Assessment as required by law to determine how to balance individual privacy, data security, and safety.

[224] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

IX. V2V Communications Security

A. Overview and importance of security

Public acceptance and the adoption of cooperative V2V safety applications will depend on appropriate levels of security as an integral part of the system. In contrast to other types of safety technologies, the V2V safety applications are cooperative—meaning that both vehicles must send, receive, and analyze data in real-time. This cooperative exchange of data about potential threats and hazards forms the basis of alerts and warnings to drivers to support their decisions and actions to avert impending incidents. This is a new paradigm that is in contrast to the stand-alone sensor-based vehicle system. However, a cooperative system can only work when participants in the system are able to trust the alerts and warnings issued by V2V devices working with messages from other V2V devices.

Thus, the basis of a relevant V2V security system is "trust"—a requirement that thousands of data messages will be authenticated, in real-time, as coming from a trusted (if unknown) source. It is also a critical element in achieving interoperability—o that vehicles of different make/model/year will be able to exchange trusted data without pre-existing agreements or altering the actual vehicle designs.

Further, the system must be secure against internal and external threats or attacks. Three primary elements of the V2V system require security:

1. Communications (the medium, the messages/data, the certificates, and any other element that supports message exchange);
2. Devices; and
3. Structure (organizational, operational, and physical).

Last, in addition to these requirements, the system needs to be: scalable to meet the needs of over 350 million users across the Nation; extendable to accommodate other types of applications such as V2I mobility, management, and environmental applications; and financially sustainable.

Eleven years of research (i.e., examination of different security approaches, technical architecture and configuration decisions, testing of prototypes, and development of an operational and organizational structure) have resulted in the current security design concept for a V2V system, as discussed below.

Cryptography is the approach that has been used historically to secure communications. Intended recipients have a "key" that allows them to decrypt and read the original message. It can be implemented in varying ways to achieve different levels of security. These include: (a) data confidentiality; (b) data integrity; (c) authentication; (d) non-repudiation (which means a sender cannot deny a message that they have sent); or (e) authorization (grants access rights to others to perform actions).[225]

Encryption techniques rely upon algorithms that have evolved significantly over time and were recently accelerated by the advent of powerful computers. Algorithms are calculations with well-defined steps that can be followed as a procedure—in this case, a procedure to encrypt and decrypt information.

The operations are dependent upon a separate piece of information known as a "key" which can be varied and which then varies the output of the algorithm. In a "symmetric" encryption system, there is one key—the secret key used to encrypt the message is the same one used to decrypt a message. In an asymmetric encryption system, keys come in pairs—each message sent contains one half of this key pair, and the receiving device has the other key.

Advancements in computing power provide industry with the ability to employ advanced algorithms and larger keys, thus making decryption thousands of times more difficult without the key.

1. Security options considered

In considering which option would most effectively provide trusted message exchange and secure communications for safety-critical applications, the DOT and V2V research development team (including CAMP security experts) compared three options—symmetric encryption systems, group signature systems, and asymmetric public key infrastructure systems. When assessing these alternatives, the V2V research team (both DOT and CAMP members) was looking for an option that:

- Did not require the identity of the participating parties and, accordingly, supported the goal of appropriately preserving privacy;
- Was fast enough to fit within the bandwidth constraints of DSRC and the processing constraints of the V2V on-board equipment;
- Entailed a number of over-the-air bytes needed for security that fit within the constraints of DSRC bandwidth and size of the BSM in the message payload; and
- Supported non-repudiation.

[225] Handbook of Applied Cryptography (Menezes, van Oorschot, and Vanstone, ISBN 0-8493-8523-7) at http://cacr.uwaterloo.ca/hac/about/chap1.pdf (last accessed June 28, 2013).

Table IX-1 provides a comparison of the “options” as alternatives and notes that characteristics of each approach are beneficial to the V2V needs or contain “fatal flaws.” The (*) denotes characteristics that do not meet key criteria for the V2V system (safety, security, privacy, latency, cost, non-repudiation are the key criteria) while the (^^) denotes beneficial characteristics.

Table IX-1 Security Approach Alternatives[226,227]

<table>
<tr><td colspan="3">1. <b>Symmetric Key Systems</b>
This approach requires that both parties have the same secret key. Securely distributing keys in such a system becomes infeasible when securing multiple types of devices with a large and expanding base of users. The approach is suitable for systems where the endpoints can be tightly controlled – for example, tolling, or ATMs, or military radio. Asymmetric cryptography is suitable for systems where membership is highly dynamic or where endpoints cannot be so tightly controlled – for example, web browsers or postage stamps.</td></tr>
<tr><th>Cryptography method</th><th>Beneficial Characteristics</th><th>Limitations</th></tr>
<tr><td>Symmetric-key ciphers
(stream ciphers, block ciphers)*</td><td>▪ Extremely fast</td><td>Key distribution or pre-storage is:
▪ A security vulnerability and
▪ Too cumbersome at large scale*
▪ There is no non-repudiation.
o Global symmetric-key is more vulnerable to compromise.
o V2V needs authentication for trust, not encryption (BSM not encrypted).</td></tr>
<tr><td>Arbitrary length hash</td><td>▪ Fast, could be used if anchored by periodic certificates</td><td>▪ Need for key distribution in later packets <b>adds over-the -air overhead and slows</b></td></tr>
</table>

[226] Cryptographic primitives are well-established, low-level cryptographic algorithms that are frequently used to build computer security systems. These routines include, but are not limited to, one-way hash functions and encryption functions. When creating cryptographic systems, designers use cryptographic primitives as the ir most basic building blocks. Because of this, cryptographic primitives are designed to do one very specific task in a highly reliable fashion. They include encryption schemes, hash functions and digital signatures schemes. Since cryptographic primitives are used as building blocks, they must be very reliable, i.e., perform according to the ir specification. Id.

[227] E.g., Understanding PKI: concepts, standards, and deployment considerations, at 11-15 *(*Adams & Lloyd, 2003) at Docket No. NHTSA-2014-0022; Managing information systems security and privacy, at 69 (Trček, 2006) at Docket No. NHTSA-2014-0022; Public key infrastructure: building trusted applications and Web services, at 8 (Vacca, 2004) at Docket No. NHTSA-2014-0022; and Network Security with OpenSSL, at 61-62 (Viega, et al., 2002) at Docket No. NHTSA-2014-0022.

functions (MACs)[228], (“keyed hash”)		**latency** ▪ May require **precise timing regime** (e.g., TESLA)
Pseudorandom sequences	• Building block for authentication/encryption	• Cannot be used on their own for authentication or encryption
Identification primitives*	▪ Extremely fast	▪ Same key distribution issues as symmetric-key ciphers* ▪ Risk to privacy*

2. Public Key Infrastructure Systems (Asymmetric Key Systems)

Organizations today predominantly use PKI as a primary means of securing communications. This approach allows users to “…securely communicate on an insecure public network, and reliably verify the identity of a user via digital signatures.” The system also allows for the “…creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity. A PKI system creates and manages digital certificates, which maps public keys to entities or permissions, securely stores these certificates in a central repository; distributes them to users as needed (or upon request); and revokes them in the case of misuse, system or devices failures, or malicious behavior.” The public key(s) in an entity’s certificate can be used to authenticate the entity, directly encrypt data for the entity, or establish a shared symmetric key that can be used to protect bulk data.

Cryptography method	Beneficial Characteristics	Limitations
Public-key ciphers	▪ Easy distribution of public key ▪ Can distribute pairwise or group symmetric keys for bulk encryption	V2V needs authentication for trust, not encryption (BSM not encrypted).
Signatures	▪ Easy distribution of public key^^ ▪ May gain sufficient speed coupled with appropriate certificate exchange mechanism (e.g., Verify on Demand or Periodic broadcast)	▪ Slower than symmetric systems ▪ Adds more packet overhead than symmetric systems
Identification primitives	▪ Building block for signatures	▪ In general interactive – cannot be used to authenticate broadcast messages.

3. Group Signatures (Subset of PKI Systems)

This approach allows a single public key to verify signatures created by the many unique private keys of all the group members. The keys are issued by a central authority that can identify misbehavers and revoke credentials. Only group members have a valid signature and a member of a group can anonymously sign a message on behalf of the group. The signer is anonymous, except the signer can be identified with the group manager’s secret key; thus, the anonymity can be broken by the group manager.

[228] The acronym MAC has two accepted industry definitions depending on the industry and context. For this context it is defined as Message Authentication Code.

Cryptography method	Beneficial Characteristics	Limitations
Group Signatures	▪ Easier key distribution - Single public key verifies many unique private key ▪ Anonymous except to the central authority	▪ Signature too big for over-the -air requirements* ▪ Revocation checking is computationally expensive ▪ Lose backwards privacy protection at revocation* ▪ Master key holder can forge messages and compromise privacy

4. **Non-Keyed Systems**

These are simply algorithms that are useful building blocks in other cryptographic systems. Note that with the evolution of cryptographic technologies over the years, non-keyed options are no longer considered separate alternatives, but building blocks used to implement either the Symmetric-key or Public-key options. Thus, the first two options are the only actual alternatives to choose from (group signatures were dismissed because of the privacy requirements).

Cryptography method	Beneficial Characteristics	Limitations
Arbitrary length hash functions	Used as building block in keyed methods (e.g., signatures)	Not keyed, so can't be used on their own to establish identity or to encrypt data*
One way permutations	Used as building block for signatures	Not keyed, so can't be used on their own to establish identity or to encrypt data*
Random sequences	Used as building block in keyed methods (e.g., group linkage values). Allow efficient construction of sequences for which an adversary cannot guess the next or previous entry	Not keyed, so can't be used on their own to establish identity or to encrypt data*
Arbitrary length hash functions	Used as building block in keyed methods (e.g., signatures)	Not keyed, so can't be used on their own to establish identity or to encrypt data*

In viewing the tables above, the public key infrastructure option (asymmetric key) using the signature method was deemed to offer the most effective approach to implementing communications security and trusted messaging for a very large set of users. Thus, it was chosen for the BSM. Importantly, the effectiveness of this approach is highly dependent upon the technical design decisions regarding *how* to implement this approach in its given environment.

2. Overview of PKI and how it works

How a PKI architecture is implemented can vary from one system to another. The choices made in configuring a PKI architecture speak to the type of goals and objectives for a system and focus on choices that:

- Support a particular level of strength of security or privacy that is desired or needed by the system, and assure longevity to the security that is longer than the lifespan of the equipped vehicles.
- Support scalability; extensibility to other uses (if desired); system operations, maintenance, upgrades, and evolution needs; and ease of access and use requirements
- Address issues such as technology limitations or constraints, or cost limitations
- Mitigate risks and types of attacks envisioned on the system.

Noting the system objectives articulated by the research team (trusted messaging, feasible operations, and appropriate privacy protection), the following discusses the basic elements of any PKI, and notes the challenge in designing a security approach specific to the V2V system.

All basic PKI systems are comprised of the following elements and functions, at a minimum[229]

- **A Certificate Authority (CA)**—an entity that acts as the "trusted third party" to provide the action to "authenticate" the entities within a network. It typically does so by signing and distributing digital certificates. The CA also typically revokes certificates and publishes a certificate revocation list so that valid users know to ignore certificates of users who have been revoked. A CA is considered the root of trust in a PKI.
- **A Registration Authority (RA)** — the entity that is certified to register users and issue certificates. This function is performed by the CA in the simplest PKI systems.
  - **A Root Certificate Authority** (sometimes the CA and sometimes a separate entity)—the highest trusted entity within a PKI security system, the Root CA typically has a self-signed and issued certificate. A certificate that is issued by a CA to itself is referred to as a trusted root certificate, because it is intended to establish a point of ultimate trust for a CA hierarchy. Once the trusted root has

[229] E.g., http://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx (last accessed Jan. 30, 2014); https://www.juniper.net/techpubs/en_US/junos10.4/information-products/topic-collections/nce/pki-conf-trouble/index.html?topic-49285.html (last accessed Jan. 30, 2014) and www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=8&cad=rja&ved=0CFAQFjAH&url=http%3A%2F%2Facs.lbl.gov%2F~mrt%2Ftalks%2FsecPrimer.ppt&ei=ua7IUdyTBvKv4APlqYCABg&usg=AFQjCNHO-XXndSLpKwls7VHbNsk_Ckmamw&sig2=d5L8IFMnEegw39L1dE-hJA (last accessed Jan. 30, 2014).

    been established, it can be used to authorize subordinate CAs to issue certificates on its behalf.[230]

    - **Digital Certificates** (also known as public key certificates)—electronic "documents" that use a digital signature to bind a public key with an identity.[231] Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root CA. Many software applications assume these root certificates are trustworthy on the user's behalf. For example, a web browser uses them to verify identities within SSL and TLS secure connections. However, this implies that the user trusts their browser's publisher, the certificate authorities it trusts, and any intermediates the certificate authority may have issued a certificate-issuing-certificate, to faithfully verify the identity and intentions of all parties that own the certificates. This (transitive) trust in a root certificate is the usual case. The most common commercial variety is based on the International Telecommunication Union Telecommunication Standardization Sector standard X.509.[232]
- **Secure hardware and software** (servers, stores, repositories; also known as a central directory)—hardware and software to support the processing of certificate requests, save issued certificates before they are distributed, or save revoked certificates. May generate certificates and validate received certificates. Also used in back-up systems.
- **Communications**—wire line, wireless, or Internet services that provide the communications capacity over which management capabilities are enacted to receive requests, distribute certificates, collect misbehavior reports, revoke certificates, and distribute the CRL. Average sizes of PKI objects are:
    - Private/public key pair = typically 1 KB
    - Local certificate = 2 KB
    - CA certificate = 2 KB
    - CA authority configuration = 500 bytes
    - CRL (average size is variable, depending on how many certificates have been revoked by a particular CA) = typically between 300 bytes to 2MB+

Basic technologies used in achieving security levels with these PKI elements include the following.[233]

- Encryption provides confidentiality; can provide authentication and integrity protection
- Hash algorithms/checksums provide integrity protection; can provide authentication
- Digital signatures provide authentication, integrity protection, and non-repudiation.

[230] See http://technet.microsoft.com/en-us/library/cc778623(v=ws.10).aspx (last accessed Feb. 25, 2014).

[231] See www.verisign.com.au/repository/tutorial/digital/intro1.shtml (last accessed Jan. 30, 2014).

[232] See www.itu.int/rec/T-REC-X.509 (last accessed Jan. 30, 2014).

[233] An Introduction to Distributed Security Concepts and Public Key Infrastructure (PKI) (Mary Thompson) See www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=8&cad=rja&ved=0CFAQFjAH&url=http%3A%2F%2Facs.lbl.gov%2F~mrt%2Ftalks%2FsecPrimer.ppt&ei=ua7IUdyTBvKv4APlqYCABg&usg=AFQjCNHO-XXndSLpKwls7VHbNsk_Ckmamw&sig2=d5L8IFMnEegw39L1dE-hJA (last accessed Jan. 30, 2014).

All of these approaches are employed in the V2V security design concept, as well as some unique technologies such as butterfly keys and linkage values that will be defined in the next section.

3. Limitations of existing PKI systems

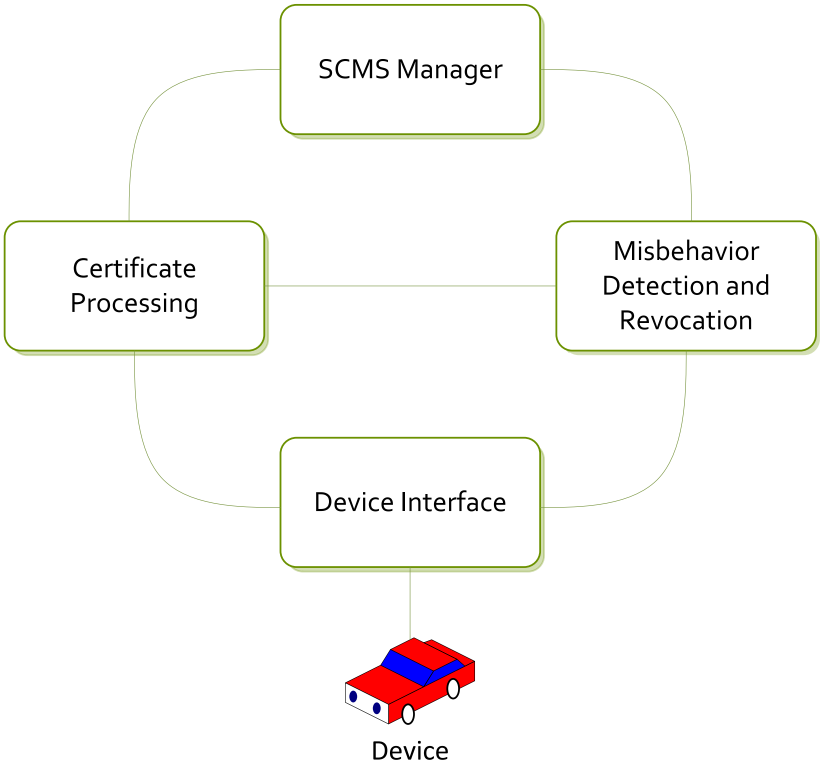
No other PKI system exists today that is broad enough to serve as a key safety-critical model. Most other systems involve data exchange among parties that are either known to each other as trusted sources (e.g., the military knows each of its communication points) or are identifiable (e.g., the FAA air traffic controllers around the Nation can identify each of the planes involved in safety-critical data exchange). Also, most other safety-critical systems employ highly secure networks (e.g., the military) or private networks (e.g., the military) and cannot leverage either existing communications systems or the Internet (to keep capital investment costs to a minimum and to achieve widespread access) in a manner that does not introduce additional vulnerabilities and risks.

Most of the existing commercial systems, by comparison, do leverage the Internet and wireless systems. These systems enable on-line purchasing or on-line financial transactions in a way that allows for easy accessibility to millions of users. They do not, however, meet the level of privacy protection, as these organizations have pre-existing agreements with the CA and thus user identity resides within databases and is typically used as part of the authentication process.

B. Current V2V security design concept

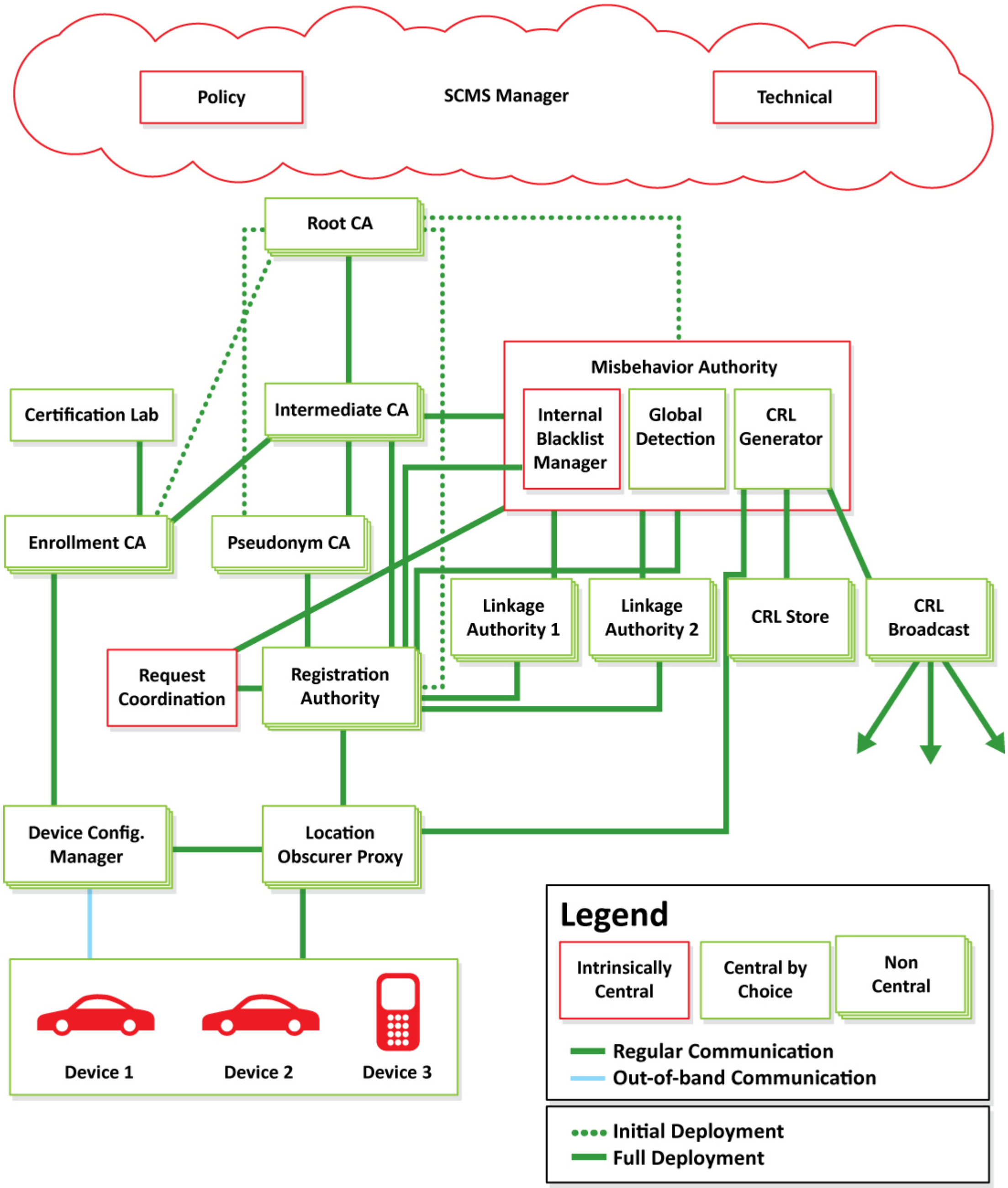
Figure IX-1 presents, at a high level, the basic use-cases of the V2V security system. They are similar to the basic functions of any PKI.

Figure IX-1 Simplified V2V Security System



The remainder of this section expands upon this basic design to present the current V2V security design. Figure IX-2 illustrates the complexity of the V2V security design associated with meeting V2V environment needs. After the illustration, each component is defined.

Figure IX-2 Current V2V Security System Design for Deployment and Operations



This image presents both an initial deployment model as well as a full deployment model. Note that this diagram shows the initial deployment model where there is no Intermediate CA and the Root CA talks to the MA, PCA, and ECA (dotted lines). In the full deployment model, these entities communicate with the Intermediate CA instead of the Root CA to protect the Root CA from unnecessary exposure (solid line).

Additionally, it should be noted that in initial deployment, some entities are considered centralized-by-choice for simplicity and because multiple entities are not required while the number of equipped vehicles is small. As penetration increases, these entities can proliferate and become decentralized. The entities that are expected to only have one in initial deployment include the Root CA, the Enrollment CA, the LOP, CRL Store, and CRL Broadcast.

This more complicated technical design is current as of January 2014. The technical design was provided by:

- The Crash Avoidance Metrics Partnership, a team of eight OEMs and their security experts and other partners.[234] This team developed the illustration.
- The VIIC—a consortium of OEM policy staff supporting the technical design team.

The technical design has been reviewed for its technical functionality by staff of the DOT from NHTSA, the ITS JPO, FHWA, and the Volpe Center.

1. SCMS component functions

The following discussion of SCMS functions focuses on communications and activities within the SCMS. The technical design for the SCMS includes several different operating functions that together make up the overall SCMS structure.

We note that the interactions between the components shown in Figure IX-2 are all based on machine-to-machine performance. No human judgment is involved in creation, granting, or revocation of the digital certificates. The functions are performed automatically by processors in the various V2V components, including the OBE in the vehicle. The role of personnel within the SCMS is to manage the overall system; protect and maintain the computer hardware and facilities; update software and hardware; and address unanticipated issues.

Generally, these SCMS operating functions fall into two categories: pseudonym functions and bootstrap functions. In order for the SCMS to support the security needs of the V2V system, the various SCMS functions must work together to exchange information securely and efficiently.

2. Pseudonym functions/certificates

The security design makes use of short-term digital certificates used by a vehicle's on-board equipment to authenticate and validate sent and received basic safety messages that form the foundation for V2V safety technologies. These short-term certificates contain no information about users to protect privacy, but serve as credentials that permit users to participate in the V2V

[234] Including security experts from ESCRYPT, Inc., CAMP, and Booz Allen Hamilton.

system. Pseudonym functions create, manage, distribute, monitor and revoke short-term certificates for vehicles. They include:

- Intermediate Certificate Authority (Intermediate CA) is an extension of the Root CA shielding it from direct access to the Internet. It can authorize other Certificate Management Entities (CMEs) (or possibly an Enrollment Certificate Authority [ECA]) using authority from the Root CA, but does not hold the same authority as the Root CA in that it cannot self-sign a certificate. The Intermediate CA provides flexibility in the system because it obviates the need for the highly protected Root CA to establish contact with every SCMS entity as they are added to the system over time. Additionally, the use of Intermediate CAs lessens the impact of an attack by maintaining protection of the Root CA.

- Linkage Authority (LA) is the entity that generates linkage values. The LA has been designed to come in pairs of two, which we refer to as LA1 and LA2. The LAs for most operations communicate only with the RA and provide values, known as linkage values, in response to a request by the RA (see below) and PCA (see below). The linkage values provide the PCA with a means to calculate a certificate ID and a mechanism to connect all short-term certificates from a specific device for ease of revocation in the event of misbehavior.

- Location Obscurer Proxy (LOP) obscures the location of OBE seeking to communicate with the SCMS functions, so that the functions are not aware of the geographic location of a specific vehicle. All communications from the OBE to the SCMS components must pass through the LOP. Additionally, the LOP may shuffle misbehavior reports that are sent by OBEs to the MA (see below) during full deployment. This function increases participant privacy but does not increase or reduce security.

- Misbehavior Authority (MA) acts as the central function to process misbehavior reports and produce and publish the certificate revocation list. It works with the PCA, RA, and LAs to acquire necessary information about a certificate to create entries to the CRL through the CRL Generator. The MA eventually may perform global misbehavior detection, involving investigations or other processes to identify levels of misbehavior in the system. The MA is not an external law enforcement function, but rather an internal SCMS function intended to detect when messages are not plausible or when there is potential malfunction or malfeasance within the system. The extent to which the CMEs share externally information generated by the MA about devices sending inaccurate or false messages – either with individuals whose credentials the system has revoked or with law enforcement – will depend on law, organizational policy, and/or contractual obligations applicable to the CMEs and their component functions.

- Pseudonym Certificate Authority (PCA) issues the short-term certificates used to ensure trust in the system. In earlier designs their lifetime was fixed at five minutes. The validity period of certificates is still on the order of "minutes" but is now a variable length of time, making them less predictable and thus harder to track. Certificates are the security credentials that authenticate messages from a device. In addition to certificate issuance, the PCA collaborates with the MA, RA, and LAs to identify linkage values to place on the CRL if misbehavior has been detected.

- Registration Authority (RA) performs the necessary key expansions before the PCA performs the final key expansion functions. It receives certificate requests from the OBE (by way of the LOP), requests and receives linkage values from the LAs, and sends certificate requests to the PCA. It shuffles requests from multiple OBEs to prevent the PCA from correlating certificate IDs with users. It also acts as the final conduit to batching short-term certificates for distribution to the OBE. Lastly, it creates and maintains a blacklist of enrollment certificates so it will know to reject certificate renewal requests from revoked OBEs.

- Request Coordination is critical in preventing an OBE from receiving multiple batches of certificates from different RAs. The Request Coordination function coordinates activities with the RAs to ensure that certificate requests during a given time period are responded to appropriately and without duplication. Note that this function is only necessary if there is more than one RA in the SCMS. The technical process behind this function is still under development.
- Root Certificate Authority (Root CA)) is the master root for all other CAs; it is the "center of trust" of the system. It issues certificates to subordinate CAs in a hierarchical fashion, providing their authentication within the system so all other users and functions know they can be trusted. The Root CA produces a self-signed certificate (verifying its own trustworthiness) using out-of-band communications. This enables trust that can be verified between ad hoc or disparate devices because they share a common trust point. It is likely that the Root CA will operate in a separate, offline environment because compromise of this function is a catastrophic event for the security system.

- SCMS Manager is the function that will provide the policy and technical standards for the entire connected vehicle industry. Just as any large-scale industry ensures consistency and standardization of technical specifications, standard operating procedures, and other industry-wide practices such as auditing, the SCMS Manager would perform and monitor these types of activities. This can happen in a number of ways. Often in commercial industries, volunteer industry consortiums take on this role. In other industries, or in public or quasi-public industries, this role may be assumed by a regulatory or other legal or policy body. Despite the choice of how to implement a central administrative body, it is expected practice that one would be established for the SCMS. As no decisions about ownership or operation have been made, we do not advocate for public or private ownership, but include the basic functions we expect the SCMS Manager would perform in our discussions and analyses. The expectation is that the SOPs, audit standards, and other practices set by this body would then be executed and complied with by each CME individually. It is also assumed that any guidance, practices, SOPs, auditing standards, or additional industry-wide procedures would be set based on any Federal guidance or regulation. The SCMS will also remove or revoke entities that do not comply with standards or misbehave.

3. Initialization functions/enrollment certificate

The security design also includes functions that carry out the bootstrapping process, which establishes the initial connection between a motor vehicle's OBE and the SCMS. The chief functional component of this process is the Enrollment Certificate Authority that assigns a long-term enrollment certificate to each OBE. To the extent required by NHTSA or other stakeholders, it is during the bootstrap process that the SCMS can create a link between specific OBEs or production lots of OBEs and enrollment certificates that later may be used by OEMs and NHTSA to identify defective V2V equipment. The design does not indicate when bootstrapping should take place, but NHTSA has suggested that it might need to take place at the time of OBE manufacture to facilitate the level of linkage between long-term enrollment certificates and equipment production lots that NHTSA needs for enforcement purposes (e.g., to identify defective equipment).

Note that, at this time, bootstrap functions have been fairly well defined for OBEs. The process for establishing the connection between aftermarket safety devices and the SCMS has not been defined; nor will it be defined by CAMP (it will need to be defined by ASD manufacturers who will need to work with the final structure of the SCMS to determine how to do this process).

Initialization functions include:

- Certification Lab does not take part in the particular use cases [of the SCMS]. It instructs the ECA on polices and rules for issuing enrollment certificates. This is usually done when a new device is released to the market or if the SCMS Manager releases new rules and guidelines. The Enrollment CA uses information from the Certification lab to confirm that devices of the given type are entitled to an enrollment certificate. As identified in Section VI.G, details regarding the Certification and Enforcement are not currently determined.[235]

- Device Configuration Manager (DCM) is responsible for giving devices access to new trust information, such as updates to the certificates of one or more authorities, and relaying policy decisions or technical guidelines issued by the SCMS Manager. It also sends software updates to the OBEs. The DCM coordinates initial trust distribution with OBE by passing on credentials for other SCMS entities, and provides the OBE with information it needs to request short term certificates from an RA. The DCM also plays a

[235] At this point, the extent and level of testing that the Certification Lab will actually perform is still to be determined. The role of the labs could range from simply managing a checklist of requirements to performing extensive technical certification tests, including: device performance, FCC compliance, cryptographic testing (at the level of FIPS-140), and/or interoperability testing. The intent is that the SCMS manager, after it is created, will determine the full roles and responsibilities of the Certification Lab. Vehicle and device manufacturers may decide to rely in part on a certification lab to support the ir own certification of compliance with any relevant standards NHTSA may issue.

role in the bootstrap process by ensuring that a device is cleared to receive its enrollment certificate from the ECA. It also provides a secure channel to the ECA. There are two types of connections used from devices to the DCM: in-band and out-of-band communications. In-band communication uses the LOP, while out-of-band communication is sent directly from the OBE to the ECA by way of the DCM.

- Enrollment Certificate Authority (ECA) verifies the validity of the device type with the Certification Lab. Once verified, the ECA then produces the enrollment certificate and sends it to the OBE. Once the OBE has a valid enrollment certificate, it is able to request and receive certificates from the SCMS.

a) Unique technologies employed in the current V2V PKI security system design

Following are some of the additional technologies that are unique to the V2V PKI Security System:

b) Butterfly Keys:[236]

Butterfly keys are a novel cryptographic construction that allows a device to request an arbitrary number of certificates, each with different signing keys and each encrypted with a different encryption key, using a request that contains only one verification public key seed and one encryption public key seed and two “expansion functions” (which allows the second party to calculate an arbitrarily long sequence of statistically uncorrelated (as far as an outside observer is concerned) public keys such that only the original device knows the corresponding private keys).

Without butterfly keys, the device would have to send a unique verification key and a unique encryption key for each certificate. Thus, butterfly keys reduce the upload size of certificate requests, and allow requests to be made when there is only spotty connectivity (although they also increase the size of the certificate upload). They also reduce the work to be done by the requester to calculate the keys, thus reducing computational burden.

(1) Linkage values

To support efficient revocation, end-entity certificates contain a linkage value that is derived from cryptographic seed material. Publication of the seed is sufficient to revoke all certificates belonging to the revoked device, but without the seed an eavesdropper cannot tell which certificates belong to a particular device. (Note: the revocation process is designed such that it does not give up backward privacy.) For protection against insider attacks, the seed is the combination of two seed values produced by two Linkage Authorities; this ensures that no single organizational entity knows enough information to identify a single device. An extension to the linkage values approach allows for group revocation, so that if all devices of a particular type

[236] A Security Credential Management System for V2V Communications (Whyte, Weimerskirch, Kumar, and Hehn). See Docket No. NHTSA-2014-0022=

have a flaw they can be revoked with a single entry on the revocation list, while keeping group membership secret until the relevant group seed is revealed. Group revocation is considered an option besides revocation of single devices.

Linkage values and linkage authorities (LAs) are used to enable the SCMS to support seven requirements.

- There should be an efficient way of revoking all the certificates within a device
- There should be an efficient way of revoking all the certificates within a group of devices
- Certificates should not be linkable by an eavesdropper unless the owner has been revoked
- Membership to a group should not be disclosed unless that group has been revoked
- If a vehicle's security credentials are revoked, the vehicle should be identifiable going forward but its movements before it was revoked should not be trackable.[237]
- Similarly, if a group of vehicles' security credentials are revoked, a device belonging to that group should be identifiable as a member. However, it should not be possible to determine the membership to a group before the group revocation took place.
- No single entity within the system should be able to determine that two certificates belong to the same device or to the same group. An exception to this rule is the Misbehavior Authority.

If there is a requirement that no single entity within the SCMS should be able to identify a vehicle, once an LA is introduced, this requirement is no longer fulfilled. For that reason, two LAs are introduced and the information that allows for identification is split between them.

(2) Misbehavior Authority/CRL

Most SCMS functions listed above are fairly well developed. One critical function, which has not yet been fleshed out adequately for DOT to assess, is the Misbehavior Authority (MA) -- the central function responsible for processing misbehavior reports generated by OBE and producing and publishing the CRL. This list, once distributed, identifies digital certificates that are no longer valid and the OBE should no longer rely on messages from the identified digital certificates. The size of the CRL depends on the frequency of list distribution and rate of misbehavior across the vehicle fleet. On-board storage for and the costs of distributing the CRL are two major cost generators in the technical design.

The MA also will be responsible for performing global misbehavior detection, involving the collection of a sampling of misbehavior reports from OBE for purposes of detecting system-wide misbehavior and revoking misbehaving entities. Global detection processes have not yet

[237] Because the current design now reuses certificates, vehicles will be backwards-trackable for the period of the batch life. This design anticipates certificate batches to be valid for a week.

been defined. Should NHTSA decide to move forward with regulatory action, it will be important for NHTSA to continue to work with CAMP and perhaps other consultants to mature the misbehavior detection processes,[238] as these are critical to system integrity and have a direct relationship to system costs.

Research Need IX-1 Misbehavior Authority[239]

Research Activity: Misbehavior Detection

Description: 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.

Target Completion: Initial requirements completed in 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

NHTSA is currently working with CAMP to develop Misbehavior Detection and Reporting strategies for both local and global misbehavior detection. Initial requirements that define the Misbehavior Authority functions will be complete in 2015. Validation and demonstration efforts will continue through 2016.

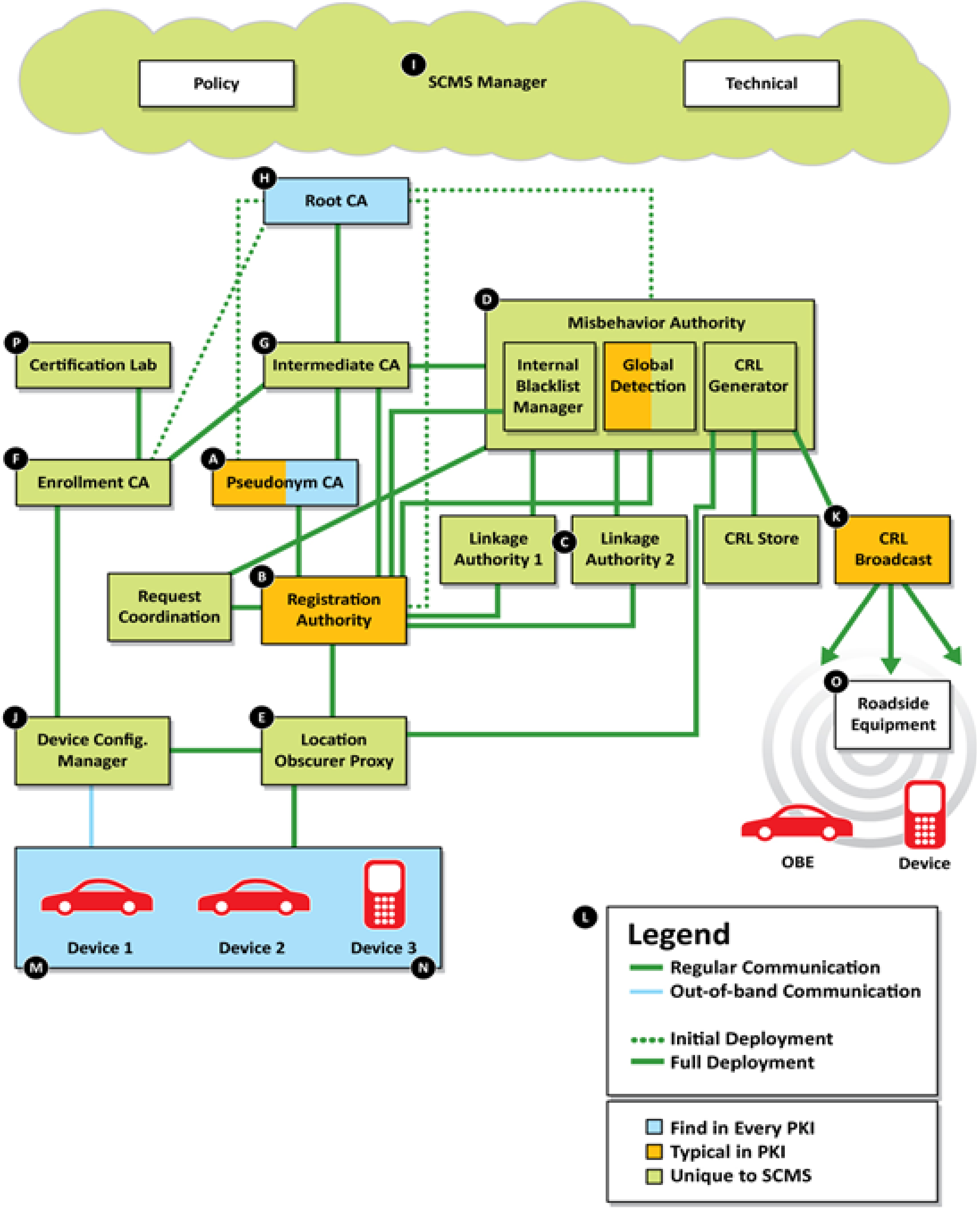
4. Comparing a basic PKI to the V2V security design

Based on the definition of these additional elements that is needed for a secure V2V environment, Figure IX-3 illustrates the differences between a “basic PKI system” that is similar to those in use today versus the V2V PKI that can deliver the highest levels of privacy protection, can be scaled to support 350M+ users, and can mitigate risks and attacks that are associated with systems in use today and in the near future.

[238] Some specific tasks could include evaluating: (1) how onboard diagnostics for V2V devices for local detection (malfunction) could reduce the size of the CRL; (2) how misbehavior search algorithms for global detection (malfunction and malicious) could be developed; (3) the approach and feasibility of using “epidemic distribution” to eliminate the need for a CRL; and (4) what new vulnerabilities to attack and what new enhanced data communication capability exist.

[239] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

Figure IX-3 V2V Security Design Comparison to a Basic PKI



The boxes in blue are the entities/functions found in every PKI. The boxes in gold are typically associated with today's PKI systems. The boxes in light green are unique to the V2V

PKI. Note that the complexity requires an overall “security credentials management system” manager. Note also that some entities/functions are split to support privacy preservation.

The additional elements added by the research team to the V2V security design are needed for the following reasons:

- The requirement to protect privacy appropriately requires a system that divides and separates some of the functionality to ensure that no one element (entity) has the ability to match records that would lead to identification of a specific driver or specific vehicle.
- There are two linkage authorities that create linkage values. Linkage values allow one entry on the CRL to revoke an entire batch of certificates, instead of having to list each certificate. This drastically reduces the size of the CRL and the communications requirement. An LA has enough information that an inside attacker can track a user. Therefore, the linkage value comes from the output of two separate linkage authorities, neither of which has enough information to track anyone. Splitting the linkage authority creates additional privacy protection but also increases organizational costs.
- The need for appropriate privacy protection has led to a greater amount of digital certificate usage; digital certificates use random identifiers that change frequently so as to lower the risk of identifying any one vehicle or driver with a particular digital certificate. The decision on how many certificates are used in a given time period or how to employ random identifiers is still to be determined (options are described but not yet decided upon). It may be a flexible choice based on type of application. Notably, allowing for different schemes might also make attacks on the system more difficult.
- Privacy considerations also have resulted in the addition of an element to obscure location coordinates when a vehicle or device communicates with the system (e.g., to request more digital certificates or to report misbehavior detected locally, around the vehicle).
- While misbehavior authorities exist in today’s PKI system (typically as a part of a CA) to detect and take actions to mitigate or remove malicious behavior, the V2V PKI’s MA is described as a separate and more complex entity than exists today. Not all of the described functionality of the V2V MA has been demonstrated (e.g., the use of local detection and reporting) in industry. It is, however, planned for demonstration and testing as an operational prototype that is being planned as part of the ongoing near-term CAMP research.
- The trust requirement has resulted in the design of a direct interface with a certification lab entity to verify that each type of device meet standards proving their capabilities to be trusted, secure, and interoperable.
- Request coordination is added as a function to ensure that an OBE cannot obtain multiple batches of certificates by sending requests to several RAs at the same time.

5. V2V security research conducted or underway

Table IX-2 provides a summary of the security research conducted over the past eleven years and currently underway. The research supported the development of a SCMS, explained previously, that was prototyped for the Safety Pilot Model Deployment. The different research projects built off of the previous research projects to investigate and then define the components and processes of a security system for V2V communications. The prototype SCMS that was implemented to provide Safety Pilot Model Deployment communications security will provide data that will be used to understand and evaluate the capabilities of the current prototype, and possibly indicate how it can be improved.

Table IX-2 V2V Communication Security Research

Research Project	Time Period	Research Focus
Vehicle Safety Communications (VSC)	2002-2005	Secure communications that included identifying options for: • Trust mechanisms • ID misbehaving devices • PKI architecture
Review by the National Institute of Standards and Technology (NIST)	2004	NIST reviewed the security options alternatives analysis, agreed with the security approach chosen (PKI), reviewed the emerging PKI configuration for V2V, and identified concerns that the research team would need to address as development moved forward.
Vehicle Safety Communications – Applications (VSC-A)	2006-2010	Development of high-level security design that covered: • Over-the-air performance of an authentication scheme • Identification of privacy mechanisms • Analysis of channel options for security • Refinement of the attacker model • Initial development of misbehavior detection schemes

Research Project	Time Period	Research Focus
Vehicle-to-Vehicle-Communications Security (V2V-CS)	2010-2012	Research Objectives included: • Determined security requirements and derived communication channel requirements. • Delivered a simplified initial and final deployment security model that identified the 3000/year certificate model with no infrastructure required for the first three years. • Performed a system-based risk assessment using the proposed initial and full deployment models. Assessment identified both privacy and security risks. • Began definition of the SCMS to understand the organizational and operational requirements; identified a need to research ownership/operations from a centralized versus non-centralized perspective. • This version of the SCMS formed the basis for the Safety Pilot Model Deployment prototype.
Vehicle-to-Vehicle-Interoperability, Phase 1 (V2V-I)	2010-2012	Research objectives for defining interoperability included further research into security from an operational perspective. The research covered: • Definition of a concept of operations for a V2V security; tested the operations with 200 vehicles to observe channel congestion using both cellular and DSRC. • Definition of a process of certificate management and an initial process for misbehavior detection. • Publication of design specifications on IP.com and licensing of the operational design for use in the Safety Pilot Model Deployment.
Oak Ridge National Laboratories (ONRL)	2012	Before the launch of the Safety Pilot Model Deployment, ORNL tested the prototype security system.

Research Project	Time Period	Research Focus
Safety Pilot Model Deployment (SPMD)	2012-2013	Implementation of a prototype that included: • Support for device initialization • Pre-load of certificates onto devices • Over-the-air certificate reload • Testing of the certificate revocation list • Testing of misbehavior reporting function
Vehicle-to-Vehicle-Vehicle Safety Communications Security Studies (V2V-VSCS)	2012-2014	Research is underway and includes: • Finalization of the SCMS design with a focus on simplifying and optimizing operations • Cost analysis of the SCMS with a sensitivity analysis on the assumptions associated with the current design concept. • Identification of optional methods to link batches of on-board equipment devices to enrollment certificates
V2V Interoperability Project/Phase 2 (V2V-I/Phase 2)	2012-2014	Research is underway and is focused on misbehavior detection and reporting – the algorithms and operational requirements needed to ensure that this function works under real-world conditions that will lead to development of a deployment use case.
Independent Evaluation of V2V Security System Design	2014-2015	To better understand the state of the current design, the DOT needs an independent entity's assessment to inform the DOT of the status of the design and provide a basis for future policy and technical decisions.

6. Overall application of cryptography in V2V communications

The security approach for V2V system is based predominantly on use of a public key infrastructure to support trusted messaging, feasible operations, and appropriate privacy protection. Other forms of security—symmetric encryption, physical security and system controls, organizational security, and legal deterrence policies are incorporated judiciously throughout the system. The decisions on where and how to apply security have been made with safety as the highest priority, and a balance between protecting privacy appropriately, latency and bandwidth concerns, preliminary costs, flexibility, and non-repudiation. Additionally, all of the cryptographic methods are expected to provide a security level of at least 128 bits and are NIST compliant.[240]

Below is a high level but technical summary of how these various mechanisms are built and applied at key risk points throughout the system:

- **Digital Certificates:** Are based on the Elliptic Curve Qu-Vanstone Implicit Certificate Scheme[241]; and IEEE Standard 1609.2-2013[242] is used for generating digital certificates. Keys with the certificates are generated using the "butterfly keys" scheme, which is not yet standardized.
- **Digital Signatures:** Are based on the Elliptic Curve Digital Signature Algorithm from the Digital Signature Standard that is used for digitally signing messages.[243] Note that NIST requires the use of a hash function (SHA-256[244]) during ECDSA signature generation, for security purposes. The CAMP design follows this principle.
- **Asymmetric Encryption:** Elliptic Curve Integrated Encryption Scheme as specified in IEEE Standard 1363a-2004[245] is used for asymmetric encryption. In the CAMP design, ECIES is used only to encrypt a symmetric key, which is then used for encrypting a message to the receiver using symmetric encryption (as described below). ECIES internally makes use of keyed-hash message authentication codes.[246]

[240] Approved Security Functions for FIPS 140-2 (May 30, 2012, Federal Information Processing Standard Publication, Annex A) at http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf (last accessed Jan. 30, 2014); and Recommendation for Pair-Wise Key Establishment Schemes using Discrete Logarithm Cryptography, Revised (Mar. 2007, NIST Special Publication 800-56A) at http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf (last accessed Jan. 30, 2014).

[241] As specified in the Certicom Research, see:

- Standard for Efficient Cryptography (SEC) 4: Elliptic Curve Cryptography, version 2.0., (Certicom Research, May 21, 2009) at www.secg.org/download/aid-780/sec1-v2.pdf (last accessed Jan. 30, 2014).
- SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), version 1.0. (Certicom Research, Jan. 24, 2013) at www.secg.org/download/aid-796/sec4-1.0.pdf (last accessed Jan. 30, 2014).

[242] Wireless Access in Vehicular Environments: Security Services for Applications and Management Messages (IEEE Std. 1609.2-2013) at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6509896&queryText%3D1609.2 (last accessed Jan. 30, 2014).

[243] Digital Signature Standards (DSS) (NIST, FIPS PUB 186-4, Jul. 2013) at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf (last accessed Jan. 30, 2014).

[244] Secure Hash Standard (SHS) (Mar. 2012, NIST, FIPS 180-4,) at http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf (last accessed Jan. 30, 2014). For a description of SHA-256, *see* http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf (last accessed Jan. 29, 2014).

[245] Standard Specification for Public-Key Cryptography-Amendment 1: Additional Techniques (IEEE Std. 1363a-2004,) at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1335427&queryText%3DIEEE+Std.+1363a-2004 (last accessed Jan. 30, 2014).

[246] The Keyed-Hash Message Authentication Code (HMAC) (2008, NIST, FIPS PUB 198-1) at http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf (last accessed Jan. 30, 2014).

- **Symmetric data encryption**: Symmetric data encryption is expected to be used for two separate purposes within the SCMS. The first purpose, to protect internal SCMS entity communications, has not yet been determined. Symmetric data encryption is likely to be used because it is more efficient than using asymmetric data encryption, for this purpose. But the public-private key pair (asymmetric) would be used to distribute the symmetric keys (periodically changed).

The second purpose is to provide a one-way compression of the linkage seeds to convert them into the pre-linkage values that are sent to the RA. It uses a keyed hash that offers proof of the legitimacy of the linkage authority that created them.

In both cases, the design calls for using the Advanced Encryption Standard (AES)-128.

- **Linkage Values:** Are generated using SHA-256 and using AES in raw[247] mode as input to the one-way compression that creates the keyed hash that conceals the linkage seeds (as described above).[248] Counter with CBC-MAC (CCM) mode"[249] is used to randomize the initial AES encryption and provide authentication.

  Uses of these different cryptographic applications include:

  - **Basic Safety Message**: Digital signatures only are used; the digital certificates that a vehicle receives from the SCMS are also attached to BSMs for verification purposes. The receiver trusts the message if it can validate the certificate.
  - **Communications between vehicles and the SCMS**: Asymmetric encryption is used for confidentiality when a devices needs to reach a component of the SCMS. Digital signatures are added to show that the request is coming from a valid device. Examples include:
    - To reach the RA or the MA with a certificate request or misbehavior report, a device uses asymmetric encryption to encrypt the content for the RA or the MA.
    - To show that the certificate request is valid, the device creates a signature using the private key corresponding to the public key in the enrollment certificate.
    - To show that a misbehavior report is valid, the device creates a signature using the private key corresponding to the public key in a currently valid pseudonym certificate before sending the signed content.

[247] Also known as Electronic Codebook or ECB mode.

[248] As specified in: Recommendation for Block Cipher Modes of Operation (2001, NIST Special Pub. 800-38C).

[249] Recommendation for Block Cipher Modes of Operation (2001, NIST Special Publication 800-38C) at http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf (last accessed Jan. 30, 2014). Also see the CCM Mode for Authentication and Confidentiality (2004, N.W. Group) and Counter with CBC-MAC (CCM) (Sept. 2003) both at http://tools.ietf.org/html/rfc3610 (last accessed Jan. 30, 2014).

- **Communications inside the SCMS (entity to entity)**: For performance reasons, communications between the entities use symmetric encryption together with the message authentication code (MAC). The symmetric encryption provides confidentiality, and the MAC provides integrity. Together, they provide authenticity but not non-repudiation (i.e., one entity cannot tell which of the two communicating parties generated the MAC). As the SCMS separates ownership (power) and data, non-repudiation becomes less of an issue. The only exception is the communication with the MA. Here, non-repudiation is required to make sure that a request really came from the MA and was not staged by the other SCMS entity. The MA is the only entity that needs to digitally sign its requests (as opposed to using the MAC); and only during misbehavior investigations. Note the keys for symmetric encryption will be distributed to entities within the SCMS using their public-private key pairs (that is, in asymmetrically encrypted messages).
- **Certificates for vehicles and SCMS entities**: Digital certificates are used and include the linkage values described above.

7. Additional information on the current V2V security system design and research

As evidenced by the research, the current V2V security system has been developed through a set of highly technical, incremental decisions. Along the way, outside review by NIST, Oak Ridge National Laboratories, and the DOT modal partners in FHWA, FTA, and the Volpe Center have questioned decisions, highlighted concerns, and discussed/analyzed new options.

When the research results are viewed holistically, the following statements can be made about the system and accomplishments to date:

- DOT and its partners have developed a leading-edge approach to communication security, one that will enable trusted messaging, feasible operations, and preserve user privacy appropriately.
- The approach to security is based predominantly on proven cryptographic methods. Standards are employed that are tailored specifically for these security purposes; they are industry-consensus standards that are being harmonized with Europeans at the ISO[250] level.
- A working prototype has been built that proves that the basic, fundamental operations are feasible in a real world environment.
- An operational and organizational structure (architecture) is being designed that is relatively stable. Most elements are well defined – even to the point of identifying number of personnel, number of servers, hardware, etc. But there are new entities that still need definition of functions and processes.

[250] ISO is the International Organization for Standardization.

Models show SCMS requirements for resources[251] and for bandwidth are relatively modest even when scaled up to full deployment.[252] While the SCMS will be unprecedented in scale for a PKI system, it is not remarkable compared to existing IT systems. First year estimates for a few million equipped vehicles (equivalent to only a few percent penetration) indicate the need for approximately 30 high-end computers (processors/servers) and roughly 4500 other pieces of equipment like disk drives, monitors, keyboards, personal computers, etc. distributed across perhaps 40 facilities. Year 25 estimates for ~300 million equipped vehicles, (penetration above 95 percent) indicate the need for roughly 550 high-end computers and 29,000 other pieces of equipment distributed across perhaps 95 facilities. This covers almost all traffic over the entire country. Note the specific estimates are rough and preliminary but provide a good ballpark understanding of the scale. Data throughputs between entities are estimated at a tiny fraction of current data flows for video entertainment, for example.[253]

- European regulators and industry are using a very similar approach despite focusing on a different set of system objectives—mobility and opt-in applications. They have noted that they will likely adopt practices from the U.S. design, once finalized, when they look to implement V2V safety applications. There is a movement to harmonize on security policies at an international level.

- Strength/Validity/Break-ability of the design:

  - The design incorporates digital signature algorithms and hash algorithms that are NIST compliant and predicted to be strong until sometime in the future. (ECDSA-256 is expected to be un-breakable for another 20 years.)

  - Some initial work has been conducted with the prototype system in Safety Pilot Model Deployment to test the system to see where vulnerabilities exist. Some were found as “back-door holes” associated with the system operator and with devices. These tests have formed lessons learned that are informing the development of certification processes for devices, and are anticipated to be incorporated into standard operating procedures, deployment guidance, and policies (including within the new RSE specification).

  - Planned penetration testing will provide insight into the reliability and resiliency of the design.

[251] Including such resources as hardware, software, energy/power, and personnel.

- Notably, costs for *breaking* the key element of this security approach --ECDSA encryption-- is estimated to be very high by security experts[254]

Research Need IX-2 Cryptographic flexibility

Research Activity: Independent Evaluation of Vehicle-to-Vehicle Security Design

Description: 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. Research is needed to determine if and how the existing SCMS and overall security solution design should change to build this flexibility or modularity into the system.

Target Completion: 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

NHTSA will initiate an Independent Evaluation of the Vehicle-to-Vehicle Security Design in FY14 (Research Need IX-3) that will include an assessment of the design to support a cryptographic algorithm change.

C. Overview of system integrity and management

Generally speaking, "system integrity" is defined as the state of operating within the limitations of mandated (not necessarily by government) or prescribed operational and technical parameters, performing its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.[255] "System management," in turn, is defined as execution of the set of functions required to support a communications network and the individuals, activities, or organizations that are the network's end users. For end users, such functions may include registering, verifying, enrolling, credentialing, billing, or revoking credentials. For the network, such functions may include controlling, planning, allocating, deploying, coordinating, and monitoring the resources of the network; initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management. Such tasks typically do not include provision of end user equipment.[256] In this case the functions support operations of the Security Certificate Management System for V2V communications.

[254] Vehicle Safety Communications-Applications: Final Report, Appendix Volume 3, at F-45. See www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 15, 2014).

[255] Federal Standard 1037C (General Services Administration document in support of MIL-STD-188). See www.its.bldrdoc.gov/fs-1037/fs-1037c.htm (last accessed Jan. 30, 2014).

[256] Id.

As used in this discussion, the terms “system integrity” and “system management” together are intended to encompass all of the functions, activities, and organizations that play a role in ensuring the security and trustworthiness of V2V communications and the privacy of system users based on the public key infrastructure (PKI) framework and technical design produced through joint research by DOT and CAMP. The term “user” refers to users of devices, whether original equipment or aftermarket.

The technical requirements for the current V2V communications security design require a SCMS made up of individual Certificate Management Entities (CMEs) to administer the security functions supporting the connected vehicle system. The term “CME owner/operator” refers to the entities that will have legal and operational control over individual organizations that run SCMS functions.

To be viable from NHTSA’s standpoint, the SCMS, as a whole, and the individual CMEs must satisfy certain key principles established by DOT in 2012:[257]

- Security and ability to detect and respond to attacks – the system must incorporate functions and processes to protect and monitor the systems. These functions must be able to identify anomalies and take action if anomalies present a threat to system operation.
- Privacy protection at the appropriate level – the system, through design and procedure, needs to appropriately protect the identity and daily activity of users of the system.
- Support of transportation safety – the system must contribute to supporting the safety need.
- Cost-effectiveness – the cost to operate the system must be balanced to the benefit attributed to the system.
- Extensibility across applications on a national scale – the system must be expandable to support nationwide development of V2V technology.

Both system integrity and system management are critical pre-conditions for safe, reliable V2V communications and appropriate privacy protection for users in a V2V-enabled environment. System integrity, by maintaining the state of the SCMS operation within established performance parameters and providing security for V2V messaging without deliberate or unintentional unauthorized interference, creates the environment of trust required for cooperative safety messaging. Users of the system must be able to trust the content of the messages received from other users. System integrity forms the critical basis for that essential

[257] Principles for a Connected Vehicle Environment Discussion Document (DOT, April 18, 2012). See www.its.dot.gov/connected_vehicle/principles_connectedvehicle_environment.htm (last accessed Jan. 30, 2014).

trust. At the same time, system management facilitates and enables system integrity by performing the set of technical and organizational functions that provide the foundation for system integrity.

Elements key to establishing system integrity and management include:

- The System's Technical Design,
- System Functions,
- System Organization,
- System Ownership and Operation,
- Enforcement of System Integrity and Management, and
- System Governance.

Some of these key elements were discussed in detail in Section IX.B – namely, system technical design and system functions – and therefore will not be covered again in this section. In the following sections, we address the remaining key system elements in turn.

Please note that a majority of the content of the System Integrity and Management and subsequent governance discussions are based on comprehensive SCMS research by Booz Allen Hamilton, detailed in the BAH report entitled *Security Credentials Management System (SCMS) Design and Analysis for the Connected Vehicle System*, dated December 27, 2013.[258]

1. Key elements of system integrity and management

Section IX.B describes a technical security system design for initial and full deployment in detail. For this reason, the discussion below provides only a brief, high-level summary of the aspects of the technical design necessary to support and put in context the subsequent policy discussion of System Organization, Ownership and Operation, and Governance. Preliminary system costs are addressed in detail in Section XI.

The SCMS technical design reflects the processes associated with certificate production, distribution, and revocation. Figure IX-4 above illustrates how the SCMS functions interact with each other and with OBE.

As explained in Section IX.B, the SCMS technical design uses a PKI framework to achieve the security goals related to establishing trust among users. Using PKI cryptography allows for creation and management of digital certificates that certify the sources of messages,

[258] Security Credentials Management System (SCMS) Design and Analysis for the Connected Vehicle System (Booz Allen Hamilton, Inc., Dec. 27, 2013). [Hereafter, "BAH SCMS Design and Analysis Report"]. See Docket No. NHTSA-2014-0022.

enabling users to trust one another and the system as a whole.[259] The use of digital certificates to establish trust among users forms the conceptual basis for the SCMS technical design.

At DOT's request, CAMP researched and developed a phased security system deployment design featuring "initial deployment" (for up to 3 years) and "full deployment." The key difference between the two is that not all SCMS functions will be available during initial deployment, and there will be no communications between OBE and the SCMS. This approach is intended to bring users into the V2V system gradually as connectivity evolves and as some of the more complex SCMS functions are developed further and readied for deployment. During initial deployment, OBE and Aftermarket devices will download and use three-year batches of certificates.

CAMP has put forth 2 options for size of certificate batches and related usage:

- Option 1: Three-year reusable, non-overlapping five-minute certificates
- Option 2: Three-year batches of reusable, overlapping,[260] five minute certificates valid for one week

CAMP compared the options by assessing implications for privacy,[261] security against Sybil attacks,[262] and certificate storage and generation costs. On the basis of its analysis, CAMP found Option 2 as technically preferable to Option 1, primarily because Option 2 protects against retrospective linkability of certificates better than Option 1. This characteristic of Option 2 makes identification of vehicles or their drivers harder and, therefore, in CAMP's view, provides less risk to individual privacy. DOT continues to work with CAMP to assess the viability and advantages/drawbacks of each option.

The security system design contemplates a hierarchical PKI containing a Root Certificate Authority and multiple Intermediate Certificate Authorities. The Root CA is the master root for all other CAs; it is the "center of trust" of the system.[263] It will issue digital CA certificates to subordinate CAs in a hierarchical fashion for use in their authentication within the SCMS so that

[259] An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues (Nov. 2011, DOT, OST-R, JPO, White Paper). See http://ntl.bts.gov/lib/43000/43500/43513/FHWA-JPO-11-130_FINAL_Comm_Security_Approach_11_07_11.pdf (last accessed Jan. 30, 2014).

[260] "Overlapping" means a certificate can be used at any time during the validity period – continuously until it expires.

[261] How well each option's specifications prevent a user from being tracked, concurrently or retrospectively – which is promoted by using certificates for a limited time without reuse.

[262] A Sybil attack involves an attacker using certificates to create the illusion of multiple cars on the road, which can be dangerous to OBEs – prevented by allowing only one certificate to be valid at a given time.

[263] CAMP, Task 5 Extension: Security Credentials Management System (Draft 0.5, April 2013). See Docket No. NHTSA-2014-0022

all other users and functions know they can be trusted. The Root CA is the only entity that can self-sign a certificate – the CAs cannot. All trust for the system components and users is inherited and delegated from the Root CA through certificate issuance.

The basic premise is that just as vehicles and infrastructure in the system need to be "trusted" through the use of short-term certificates that accompany V2V messages, the SCMS functions need to be "trusted" by the vehicles or infrastructure when receiving certificate batches from that SCMS function. SCMS functions also need to trust one another. For these reasons, most SCMS functions receive their own digital certificates, referred to as "CME certificates." An OBE will examine the CME certificate of any digitally signed message it receives before it accepts the message as valid to ensure:

- The certificate has not expired,
- The CME that issues the certificate is trusted, and
- The certificate is not listed on a Certificate Revocation List.

CME certificates do not need to be short-lived like the 5-minute certificates intended for the OBE, as trip tracking is not a risk for the SCMS function, because privacy is not an issue there. Additionally, not all SCMS functions require CME certificates.

DOT brought Booz Allen Hamilton on board as its consultant to: (1) assess the extent to which the evolving security design satisfies mission-based needs and DOT's Principles for a Connected Vehicle Environment, described above; and (2) develop and analyze different organizational models for the SCMS and its component CME entities based on the limited and full deployment scenarios.[264] As part of this work, BAH analyzed alternative CME models, taking into account the need for security and appropriate user privacy. BAH also identified and evaluated options related to parts of the security system not fully developed, as well as estimated preliminary costs associated with the current design. Finally, BAH identified topic areas for which further exploration is needed prior to SCMS implementation. The agency agrees that these areas represent additional research that will be needed to move forward with an SCMS.

[264] BAH SCMS Design and Analysis Report.

Research Need IX-3 Independent Security Design Assessment[265]

Research Activity: Independent Evaluation of Vehicle-to-Vehicle Security Design

Description: Independent evaluation of CAMP/USDOT security design to assess alignment with Government business needs, identify minimum requirements, assess the security designs ability to support trusted messages and appropriately protect privacy, identify and remove misbehaving devices, and be flexible enough to support future upgrades.

Target Completion: 2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:

The Independent Evaluation of the Vehicle-to-Vehicle Security Design will be a comprehensive evaluation of the design to identify minimum requirements, assess if and or how USDOT requirement are or can be incorporated into the design, assess the design's security capacity, identify security threats the design currently addresses, and identify possible modification to improve the design.

Whereas the discussion of SCMS functions in Section IX.B focused on activities and communications within the SCMS, the current section discusses the DOT research performed by BAH (with input from CAMP/VIIC) on development and analysis of SCMS organizational options. The purpose of BAH's research was to generate organizational options for the SCMS by grouping the SCMS functions in CAMP's design into legally/administratively distinct entities, in order to enable secure and efficient communications and protect privacy appropriately while minimizing cost. BAH's analysis of the organizational options for the SCMS, detailed below, focused primarily on organizational connections and separations, as well as the closely-related process of characterizing functions as "central" or "non-central" (which is intimately tied to the issue of system ownership and operation). It also examined the cost, security risk, and/or operational/policy implications of the different SCMS models.

BAH began by identifying multiple organizational models that, together, captured all possible configurations of the SCMS functions identified by CAMP. DOT initially selected a small number of these organizational models for BAH to flesh out. As CAMP's technical design evolved, DOT instructed BAH to reconfigure the models being fleshed out to reflect additional SCMS functions added to the SCMS design by CAMP, as well as CAMP's new categorization of functions as either "central" or "non-central." Based on its independent PKI research, as well as

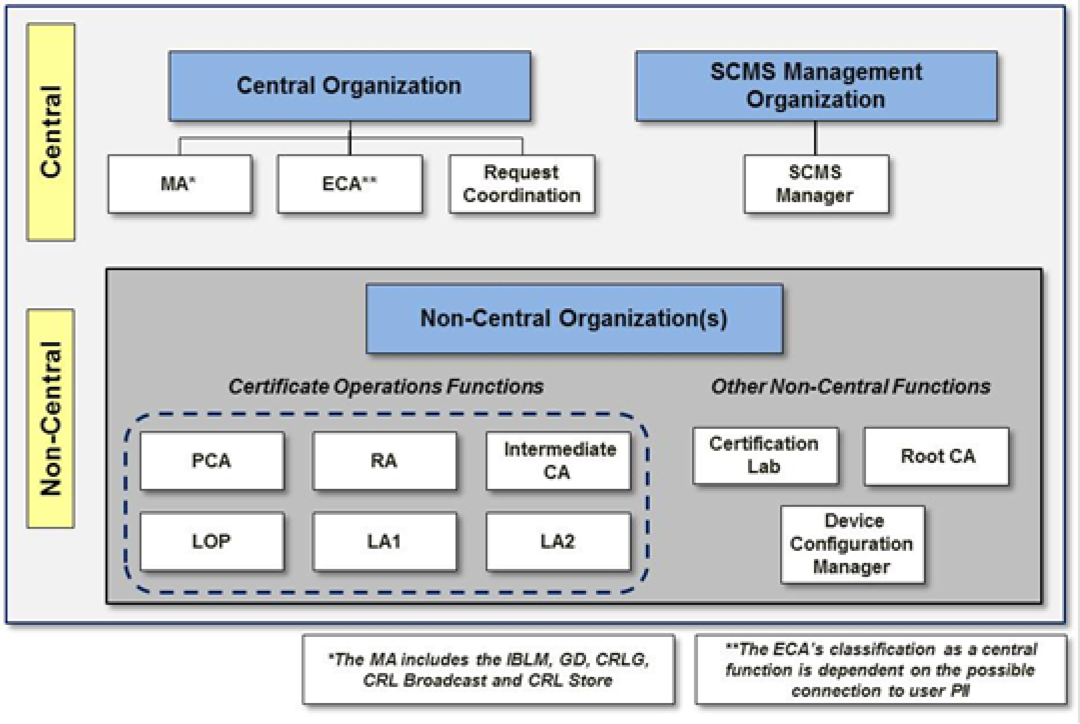
[265] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

new insights into the security design communicated by CAMP, BAH then simplified the initial organizational design proposed by CAMP to remove certain organizational separations of functions that BAH determined were not necessary for security or privacy reasons. CAMP/VIIC subsequently agreed that several pseudonym functions (e.g., linkage authorities and RA), initially viewed by CAMP/VIIC as needing to be housed in separate legal/administrative entities, may reside in the same CME organization without compromising privacy or security requirements.

Ultimately, the organization of the SCMS– the final grouping of functions and estimates of any efficiencies -- will be controlled by the organization(s) that manage the SCMS and own and operate the component CMEs. However, NHTSA anticipates being able to influence the organization and operation of the SCMS (and thereby ensure adequate separation to assure secure, privacy appropriate V2V communications) through agreement or MOU with the SCMS Manager or through participation on an SCMS "governance board," as discussed further in the governance section below.

BAH's SCMS organizational model/analysis is based on CAMP's latest SCMS technical design and represents BAH's perspective of how functions within the SCMS may be grouped.

Figure IX-4 Security Certificate Management System Organizational Model


Central
Central Organization
MA*
ECA**
Request Coordination
SCMS Management Organization
SCMS Manager
Non-Central
Non-Central Organization(s)
Certificate Operations Functions
PCA
RA
Intermediate CA
LOP
LA1
LA2
Other Non-Central Functions
Certification Lab
Root CA
Device Configuration Manager
*The MA includes the IBLM, GD, CRLG, CRL Broadcast and CRL Store
**The ECA's classification as a central function is dependent on the possible connection to user PII

DOT/BAH and CAMP/VIIC have somewhat different perspectives on whether certain functions with the SCMS should be categorized as "central" (functions that need to be owned and operated by a single legal entity) or "non-central" (functions that may be owned and operated by multiple legal entities). The issue of whether a function is central or non-central has significant policy implications both for SCMS Organization and for SCMS Ownership/Operation.

CAMP/VIIC has taken the position that the SCMS Manager, Request Coordination and MA functions all are intrinsically central. CAMP/VIIC also uses the term “central-by-choice” to refer to functions that *can* be owned and operated by more than one legal entity, but for simplicity reside in only one operator/owner. It is our understanding that CAMP believes that the same organization(s) that run non-central functions *also* can operate central functions. CAMP’s technical design for the SCMS reflects their division of functions into “intrinsically central,” “central by choice,” and “non-central.”

By contrast, focusing more on concepts of organizational modeling rather than on technical requirements, and analyzing from a legal/administrative perspective, BAH does not distinguish between “central-by-choice” and “intrinsically central.” Instead, it defines “central functions” as those that must be owned and/or operated by a single organization *that does not own or operate any non-central functions*. BAH defines “non-central functions” as those that may be owned and operated by multiple distinct organizations. BAH’s organizational model reflects its determination, based on conflict of interest principles and PKI best practices, that organizations that own own/operate central functions (e.g., the SCMS Manager, ECA, MA) should not own/operate non-central functions (such as the PCA, RA, LAs, Intermediate CA, LOP, Root CA, certification lab or DCM).[266]

CAMP/VIIC has classified the ECA as non-central, while BAH would classify it as central if the ECA is involved in collecting any personally-identifying information that could link a long-term enrollment certificate to short-term certificates used to authenticate V2V messages. This is probably due to the fact that CAMP’s technical security design, in order to achieve the CAMP/VIIC’s stated privacy and consumer acceptance goal of “end-to-end” anonymity, does not contemplate collection of any information that could link or be used to link short-term certificates to an OBE, vehicle or driver. That being said, DOT specifically instructed BAH to incorporate into its organizational models various options for linking short-term digital certificates to production runs of OBE, OBE, VINs, and drivers for purposes of identifying, investigating, and/or recalling potentially-defective V2V equipment.. CAMP also has agreed to incorporate into its work technical and organizational options, respectively, that would enable collection of information to permit such linkage for these purposes

Currently, NHTSA believes that collection of information linking long-term enrollment certificates to production lots of V2V equipment in connection with the bootstrapping process

[266] BAH SCMS Design and Analysis Report, Chapter 5 at 45.

will satisfy its mission-based information needs (i.e., investigation and recall of defective vehicles or V2V equipment). This would require some of the CME organizations to work together in a way not currently contemplated by CAMP's latest technical security design, to combine information that will link short-term certificates implicated in certain misbehavior reports and processes (and therefore emanating from potentially-defective V2V OBE) to enrollment/long-term certificates.

As part of its work for DOT, CAMP/VIIC are exploring options for specific processes to accomplish this end. Once CAMP proposes such options, NHTSA will work with CAMP and VIIC to determine whether the proposed collection and storage processes meet the agency's informational needs and, if so, the extent to which the process options implicate designation of the ECA as central or non-central. BAH has emphasized that should linkage with individually-identifying information take place, the information collected should exist only within a central ECA and should be separated from the Root CA to decrease the possibility of a malfeasant insider linking identifying information in the enrollment certificates with the short-term certificates used for V2V communications. The agency will analyze the extent to which organizational separation of the CME functions required to link enrollment certificates to production lots will mitigate any privacy risks stemming from such linkage as part of its comprehensive privacy risk analysis, discussed in Section VIII.B.

Organizational separation of functions is an example of a policy control often used to mitigate privacy risks in PKI systems – but such separations come with increased costs and may negatively impact the system's ability to identify and revoke the credentials of misbehaving devices. Ultimately, other functions may be co-located within the same SCMS component organization. However, grouping of SCMS functions and any resulting efficiencies/risk trade-offs will depend, in large part, on the system's ownership and operational structure, as well as system governance, and on the preferences of the entity or entities that own and operate the SCMS Manager and CME component entities.

The SCMS Manager is intended to serve as the entity that provides system management, primarily by enforcing and auditing compliance with uniform technical and policy standards and guidance for the SCMS system-wide. The uniform standards/guidance will need to establish and ensure consistency, effectiveness, interoperability, and appropriate security and privacy protection across the CMEs to facilitate necessary communications, sharing of information, and operational connections. The SCMS Manager will need to have mechanisms to ensure that all CME entities have policies, practices, technologies, and communications consistent with system-wide standards and guidance. The SCMS Manager may (but need not) be the body that develops the standards, guidance, or policies applicable system-wide, and would be the entity charged with overseeing standards and policy compliance by the CME entities that, together with the SCMS Manager, make up the SCMS. Technical standards and guidance exist applicable to PKI industry-wide that likely will form the basis for many of the policies and procedures applicable across the SCMS.[267]

2. SCMS ownership and operation

SCMS ownership and operation is inextricably linked to SCMS governance, discussed in more depth below. In essence, there are three basic organizational models that apply *both* to SCMS ownership and operation and to SCMS governance: public, public-private and private. Due to the lack of Federal funding available to support an SCMS, DOT research to date has focused on the likelihood of private ownership and operation of the SCMS "industry," with governance being largely "self-governance" by private industry participants and stakeholders, except to the extent that operational requirements may stem from Federal law, regulation, contract or agreement.

As discussed in Section XI below, our preliminary cost estimates for a V2V system include the assumption that a private entity would own and operate the SCMS, and impose costs that would be covered by increases in the purchase price of new vehicles. For this reason, the SCMS organizational structure discussed in the prior section – the organizational separations and groupings of functions into legally/administratively distinct CME component entities -- may not necessarily be realized in any private SCMS eventually implemented to support connected vehicle communications. In the context of a private SCMS "industry," the organizational structure and operation of the SCMS will be determined by private owners and operators of CME components, under the oversight of an SCMS Manager (ideally an industry-wide coalition of CME owners and other stakeholder representatives who, together, agree on the terms of self-governance and system-wide SCMS policies).

DOT and its consultants have identified numerous potential private and public owners and operators who could play a role in running one or more of the SCMS functions. However, at this point in time, the extent to which any entity would be interested in running one or more SCMS functions remains unclear. The list includes:

- OEMs,
- Industry groups (e.g., the American Association of Motor Vehicle, Administrators (AAMVA)),
- PKI Security organizations and companies,
- Telecommunications companies,

[267] BAH SCMS Design and Analysis Report, at 29.

- State and local government agencies, and
- Academic institutions.

BAH pointed out in its research that ownership and operation of non-central functions could take different forms. While there are advantages of having different owners (e.g., individual OEMs) oversee large CMEs comprised of all non-central functions, the BAH team has suggested that running such an overarching CME should not be a *condition* of ownership. Thus, for example, an entity that wants to own and operate one or more LOPs should not necessarily be required to operate *all* of the other non-central functions.[268]

BAH's research also has emphasized that qualifications for ownership and/or operation of non-central functions may be very different from those required for ownership and/or operation of central functions. For example, due to the critical importance of the security and effectiveness of operation of the Root CA, BAH has suggested that the owner/operator of this function should have expertise in PKI technology appropriate for the role. BAH also has explored the possibility that the OEMs could have a role in the system manager function/organization, but in a manner that is legally distinct from ownership/operation of the non-central functions that individual OEMs might want to own and operate (e.g., the RA functions involving interface with their clients). Shared governance by the OEMs, as through a legally/administratively distinct coalition or body, could be consistent with BAH's recommendations for separation of central and non-central SCMS ownership/operation, and would have distinct advantages, such as assurance of uniformity in standards and interoperability of equipment.[269]

Should the agency move forward with regulatory action, DOT will need to work with CAMP, BAH and potentially others (consultants, interested potential CME owners and stakeholders) to perform additional analysis of ownership/operation requirements and candidates, and to address the following questions:

- Who will set the various standards, policies, procedures, auditing processes, and other related industry-wide processes?
- Who are the appropriate candidates for ownership for central and non-central functions?
- What are the conditions of ownership?
- Can multiple central functions be combined or operated by the same organization
- To what extent should SCMS owners be required to support V2V and V2X needs as the system connected vehicle environment expands?

[268] BAH SCMS Design and Analysis Report, at 45. See Docket No. NHTSA-2014-0022

[269] BAH SCMS Design and Analysis Report, at 45.

3. “Enforcement” of system integrity/SCMS manager

Enforcement of “system integrity” is closely related to the general area of SCMS governance. In the context of CAMP’s SCMS technical design, envisioned by NHTSA as a privately owned and operated “industry,” a private SCMS will enforce system integrity within the SCMS through self-regulation and binding agreements with the entities agreeing to be regulated. Organizationally, enforcement is the primary responsibility of the SCMS Manager. The SCMS Manager provides critical system management by enforcing and auditing compliance with uniform technical and policy standards and guidance applicable system-wide. The uniform standards/guidance will need to establish and ensure consistency, effectiveness, interoperability and appropriate privacy protection across the CMEs to facilitate necessary communications, sharing of information, and operational connections, and most likely will be based in large part on existing technical standards applicable to PKI systems.

4. “Enforcement” of system integrity/Federal role

In the context of the SCMS technical design, envisioned as a privately owned and operated “industry,” we view the Federal role by NHTSA in “enforcing” or otherwise ensuring system integrity as fairly limited. Primarily, the agency would perform its traditional regulatory role. In addition, NHTSA’s agreement with the CME entities that constitute the SCMS, or the SCMS Manager on behalf of those CMEs (if they are inclined to sign an agreement), could provide supplemental enforcement or oversight mechanisms, consistent with our authority. Other Federal entities also likely will have some “enforcement” jurisdiction over aspects of system integrity, including the jurisdiction of the Federal Trade Commission over compliance by the SCMS entities that interact with end users with their own privacy policies.

Consequently, the specific elements of Federal “enforcement” relating to system integrity would include:

- NHTSA compliance and enforcement of the security aspects of a potential FMVSS via development of compliance testing procedures and enforcement via the manufacturer’s self-certification and NHTSA selection of some items for testing in relation to devices identified as motor vehicle equipment;
- NHTSA ODI investigation and recall of potentially defective V2V equipment;
- NHTSA enforcement of Agreements with SCMS Manager (and SCMS entities), if the SCMS is willing to enter into an agreement with NHTSA;
- FTC enforcement of the terms of privacy policies against SCMS entities interfacing with end users; and
- FCC enforcement of use of spectrum.

Other than as noted here, neither DOT nor NHTSA would assume any new “enforcement” responsibilities in the context of the envisioned privately-owned and selfregulated PKI "industry" that could support V2V communications in a secure, efficient privacy-appropriate way with minimal Federal involvement.

D. System governance and why it is important

Although heavily dependent on context, the term "governance" generally refers to the way rules are established, implemented, and enforced. Governance can mean formal regulatory oversight by a Federal, State, or local governmental entity. NHTSA's issuance and enforcement of FMVSSs under the Safety Act is an example of governance by a Federal entity. However, governance does not always require the participation of a "government" (i.e., a geo-political entity). In the context of corporate entities, governance typically refers to consistent management, cohesive policies, guidance, processes, and decision-rights for given areas of responsibility.

Deployment of V2V technologies will require governance of a wide range of complex functions and legal issues. For purposes of this discussion, we have divided these functions and issues into two categories: those outside the purview of the SCMS, and those inside its purview. Areas of governance falling outside of the SCMS (most notably, performance standards and requirements, FCC certification requirements, device communications interoperability, and spectrum allocation and management) are addressed substantively elsewhere in this decision paper. For this reason, the following discussion of "system governance" focuses solely on the important policy area of governance of the security system required to support the SCMS.

As used in this discussion:

- **"SCMS System"** is defined as all the needed functions associated with security certificate management for the connected vehicle system – from the SCMS Manager down to the individual functions and the component CME entities in which they may reside.

- **"System Governance"** refers to the body or set of bodies/entities that determine standards, policies, compliance requirements, and expectations for all organizations that have a role to play in certificate management as part of the SCMS that will be needed to support deployment of V2V technologies.

System governance encompasses:

- How decisions are made about various policies, standards, requirements, and practices;

- Who has the authority to mandate and enforce compliance with the policies, standards, and industry requirements;

- Who makes up the overseeing financial, legal, management, and executive operations of the entities in the SCMS;

- How various entities interact with each other;
- How the system addresses privacy issues;
- How risk and liability are allocated across the organizations;
- Who will own the intellectual property (data and software) of the system; and
- How the system‘s intellectual property will be licensed or otherwise allocated among and between internal and external entities.

The SCMS technical design and related work of the VIIC call for an SCMS made up of a central SCMS Manager and various CME component organizations together performing all functions required for certificate management. As discussed in detail above, the SCMS Manager will define and oversee certain standards, policies, procedures, and operational practices applicable to the SCMS component entities. The potential scope or extent of authority and operations of the SCMS Manager are still under development, but as in all industries, there are three fundamental options for organizational structure from which to choose for SCMS industry governance (the same three apply to the inextricably-related issue of SCMS ownership and operation):

- **Public**: governance structure determined and administered by the government, either directly or indirectly (as via a contractor)
- **Public-Private Partnership (PPP)**: any organizational structure authorized by law within the range between a purely government organization and a purely private organization, established and administered in accordance with the authorizing partnership or similar document (typically a grant, cooperative agreement or other agreement)
- **Private**: governance structure established and administered by a purely private organization or organizations, without direct government involvement

These governance options have different implications for the level of involvement of the Federal Government and stakeholders in the oversight, setting of policies, rules, standards, procedures, operational practices, liability/risk sharing, funding, and nature of compliance/enforcement within the SCMS industry.

From a Federal perspective, each option also may have certain pros and cons as it relates to authority, appropriations, safety, privacy, risk management, and continuity of operations. These are briefly summarized below. However, due in large part to the absence of Federal funds to support a public SCMS, DOT research on SCMS development to date has primarily focused on fleshing out a largely private model of SCMS governance. Based on this research, which has generated multiple examples of existing private sector governance organizations, we believe that a private model could be a viable mechanism for system governance of the SCMS. NHTSA’s existing legal authority will accommodate use of a grant, cooperative agreement, or other agreement to facilitate stakeholder – and even DOT -- input into governance of a private SCMS, assuming willingness on the part of the private entity to enter into such an agreement.

The VIIC, under a cooperative agreement with DOT, also has examined the viability of each of these models from industry's perspective, applying the following high-level principles, considered by its members as foundational for any governance entity:[270]

- Participation/voice,
- Accountability,
- Representation,
- Transparency,
- Efficiency,
- Flexibility, and
- Fairness and decency.

While it has not identified a preferred option, based on its governance work for DOT to date, the VIIC has taken the position that a private governance organization, without *any* government involvement (i.e., not under government contract, agreement or MOU), will lack sufficient authority to make all of the decisions and determinations necessary for appropriate system governance of the SCMS.[271] The VIIC also has expressed other concerns about a purely private governance model, including what it views as lack of stakeholder voice, accountability and government oversight; antitrust risks; potentially increasing costs; and "massive liability exposure."[272] The VIIC seems open to exploring various PPP models involving minimal "authority" passed on by NHTSA via contract, grant, cooperative agreement, MOU, or other agreement that would enable the SCMS Manager to conduct appropriate governance.

DOT will continue to use existing cooperative agreements with CAMP and the VIIC to further explore and develop SCMS governance models. Should NHTSA move forward with V2V regulatory action, additional research should include exploration of use of a private governance model (as the third option above), with some limited government involvement under

[270] In support of these principles, the VIIC cited the DOT June 2011 Governance Roundtable Proceedings (available at http://ntl.bts.gov/lib/43000/43100/43129/GovRoundtableProceedingsFINAL_9_22_11_v4.pdf , with Section 2.1 of the UNECE Guidebook on Promoting Governance in Public-Private Partnerships (2008).
[271] VIIC Assessment of Key Governance Policy Considerations for a Connected Vehicle Cooperative Safety Communications System – Part 1, delivered to DOT on March 13, 2013, at 9. See Docket No. NHTSA-2014-0022. Of specific concern to the VIIC are lack of authority to: (1) "compel universal participation"; "set or enforce rules applicable to external users and participants"; and "compel[ ] vehicle owners to maintain the ir vehicles in compliance with security protocols." VIIC, SCMS Organizational Policy Study, Interim Report, Dec. 11, 2012, at 16-17. See Docket No. NHTSA-2014-0022.
[272] Id.

an agreement with the private entity, assuming the entity's willingness to enter into such an agreement. This could facilitate stakeholder input into governance in the context of a privately owned/operated and governed SCMS, as this may be a variation on the private governance model that addresses some (albeit not all) of the VIIC's concerns about, and makes more palatable to industry the prospect of a privately owned, operated, and governed SCMS.

1. Public model

Under a public governance model, NHTSA would directly house or procure the SCMS system required to support deployment of V2V technologies. It most likely would do so through one or more service contracts with entities to serve as the SCMS Manager and CME component entities. Whether run by NHTSA or by NHTSA service contractors, the IT infrastructure and related business processes would be governed by Federal law, as appropriate, including but not limited to the Federal Information Systems Management Act, the Privacy Act, the Administrative Procedure Act, and the Federal Tort Claims Act. To the extent not already determined by applicable Federal laws, governance of the SCMS system would be NHTSA's direct responsibility, the specifics of which would be memorialized in NHTSA's contracts or agreements with its service providers. Such contracts or agreements would need to include specific provisions to ensure adequate market access, privacy and security controls, data rights, reporting, and continuity of services. Stakeholder input into governance of the security system would need to comply with the Federal Advisory Committee Act.

The FAA's air traffic control system is an example of a direct public governance model. It has a statutory basis, is funded largely by Federal appropriations, and its ownership, control, and operation are subject to Federal laws and procedures. As part of the air traffic control system, the FAA has a service contract (one of many with different private entities supporting its operations) with a private entity to provide data communications services for the NextGen program (including provision of the IT infrastructure required for NextGen communications -- but without such infrastructure becoming Federally-owned). The contractor has a nonexclusive legal right to consolidate and sell the data generated by the NextGen communications system. To the extent that it does so, the FAA receives a credit against reimbursed costs. The contract contains other provisions implementing Federal oversight and control, including oversight over security and data rights.

Currently, we believe that NHTSA has sufficient legal authority (under the Vehicle Safety Act and the "necessary expense" doctrine) , albeit insufficient appropriations, to enter into contracts related to the operation of the Security System required to deploy V2V technologies, if NHTSA were to regulate the V2V technologies in vehicles. Arguably, direct Federal operation or operation via service contracts would be the most effective mechanisms to ensure appropriate security, privacy, and long-term, stable continuity of operations, thereby reducing some of the more significant risks stemming from deployment of V2V technologies via an FMVSS dependent on a security system not directly regulated by the agency. However, absent substantial new appropriations – which NHTSA has no plans to seek at this time – NHTSA lacks the resources to contemplate public ownership, control, or administration of a system the size and scope of the SCMS, as currently conceived. For this reason, DOT research to date has not fully explored a public governance model for the SCMS. Due to the current fiscal environment it does not seem plausible.

2. Public-private partnership model

Under a public-private partnership model, NHTSA would work with the private sector to form a Public Private Partnership (PPP) to operate and/or govern the security functions required to support deployment of V2V technologies. Depending on the scope of the agreement, the PPP could be limited to the SCMS Manager functions identified in the current CAMP/DOT security system model. Alternatively, the PPP could be responsible for owning, financing, and operating the Security System, as a whole, including the SCMS Manager and CME component entities. As yet another alternative, as discussed below, the PPP could be limited to forming a governance board of stakeholders to provide input, binding or not, to the SCMS owners/operators.

DOT and its stakeholders have identified multiple models of PPP entities to help inform our research on potential ownership, operation, and governance options for an SCMS. Examples include: publicly or privately owned utility models,[273] which are complex, highly regulated, and require significant public resources to administer: the Internet Corporation for Assigned Names and Numbers, which operates pursuant to an Memorandum of Understanding with the Department of Commerce that retains in DoD unilateral oversight for some functions and some but not all liabilities;[274] the End-of-Life Vehicle Consortium operated under MOU among the vehicle manufacturers, steelmakers, vehicle dismantlers, vehicle crushers, auto shredders, brokers, the environmental community, State representatives and the Environmental Protection Agency.[275]

Due primarily to a lack of current or foreseeable appropriations to support a PPP, DOT research to date has not fully explored development of a PPP governance model for the SCMS and, instead, has focused on a private model or ownership/operation and governance.

3. Private model

Consistent with our current resources, NHTSA has focused on working with stakeholders and DOT consultants to develop a viable model of private governance for the SCMS and its CME component entities. Ideally, the basis for the private oversight structure would be a

[273] Id. at 9-11.
[274] Id. at 4-6.
[275] Id. at 13.

coalition of CME component entities who, together, constitute and empower an SCMS Manager to decide on and enforce standards and processes applicable to the SCMS as a whole.

All organizations within the "industry," or all organizations that make up different parts of the SCMS environment, could be represented. The coalition of SCMS "industry" participants, together, could decide on standards, codes of conduct, expectations, and other norms in order to maintain and protect communications security, appropriate user privacy, and required operational functions within the system, under the auspices of the SCMS Manager and/or another coalition-type body. In addition, this group likely would decide on and participate in recommendations about resource management and costs for the industry and its governing body.

Many commercial industries today operate under this model of private governance, establishing private, industry-specific organizations to develop and enforce ethics, standards, code-making, and enforcement functions not specifically required by law. The largest benefit of this kind of governance structure is that it reduces the involvement of the government and therefore reduces the cost to the taxpayers for managing, administering, and enforcing rules within and across the CMEs, although the cost will be passed to the consumer at some point. It also provides more efficiency and flexibility in decision-making than typically is available in the context of a government or PPP model.

The positive and negative implications of a private governance structure include:

- Lower costs and more streamlined implementation/operational processes, due to the lack of Federal workplace regulations and processes

- Need for clear monitoring and enforcement standards and processes, potentially with an additional level of oversight or review/audit

- Need for agreements across jurisdictions, organizations, and areas of oversight so as to ensure smooth operations and reduced communications or collaboration challenges

The private model accommodates some limited Government involvement. Once a coalition or other private entity to serve as SCMS Manager is established voluntarily by a private SCMS "industry,"[276] NHTSA could enter into an agreement with that governance entity to ensure that SCMS functions required for V2V safety are delivered by CME entity organizations in a way that is consistent with DOT's Principles for a Connected Environment, discussed above -- and that such services are made available to all market participants in a secure, ongoing, nondiscriminatory, and privacy-appropriate manner. Such agreement also would provide the

[276] SIGNIFICANT CAVEAT: This governance analysis hinges on DOT successfully reaching a consensus agreement with a willing collation of OEM or another market participant to serve as SCMS Manager or otherwise ensure provision of the security system necessary for deployment of V2V technologies.

SCMS, as a whole, with the assurance that its activities would be, and would be perceived to be, in accordance with those principles.

Assuming willingness by the private entity to enter into such an agreement with the Government, either NHTSA or JPO authority might be used to support a mechanism for stakeholder input into SCMS governance, formal or informal. This kind of DOT-funded “governance” board is similar to what DOT envisions for governance of the NAS-owned SHRP2[277] databases: no Federal ownership or operation of the data but a group of interested stakeholders, including NHTSA and FHWA, on a governance board to establish high-level terms of access, security and privacy controls and similar aspects of operation.

Numerous real-world examples exist of organizations/systems in industries that self-govern through internal, binding contracts and agreements. Typically, such private governance is grounded in oversight and inter-organizational practices and agreements that provide the governing organization with adequate legal authority to establish and enforce industry-wide standards and maintain strong centralized functions, when appropriate. Often industries subject to self-governance also are subject to governance by local, State or Federal entities. Examples include:

- Aeronautical Radio, Incorporated (ARINC), the sole licensee for the airline communications frequency, is an example of a private governance organization identified by the VIIC, funded by membership and sponsorship annual dues.[278]

[277] The second Strategic Highway Research Program (SHRP 2) was authorized by Congress to address some of the most pressing needs related to the nation’s highway system: the high toll taken by highway deaths and injuries, aging infrastructure that must be rehabilitated with minimum disruption to users, and congestion stemming both from inadequate physical capacity and from events that reduce the effective capacity of a highway facility. These needs define the four research focus areas in SHRP 2: (1) the Safety area is conducting the largest ever naturalistic driving study to better understand the interaction among various factors involved in highway crashes—driver, vehicle, and infrastructure—so that better safety countermeasures can be developed and applied to save lives; (2) the Renewal area is developing technologies and institutional solutions to support systematic rehabilitation of highway infrastructure in a way that is rapid, presents minimal disruption to users, and results in long-lasting facilities; (3) the Reliability area is developing basic analytical techniques, design procedures, and institutional approaches to address the events—such as crashes, work zones, special events, and inclement weather—that result in the unpredictable congestion that makes travel times unreliable; and (4) the Capacity area is developing a web-based tool to provide more accurate data and collaborative decision-making in the development of new highway capacity in order to expedite the provision of that capacity while simultaneously addressing economic, community, and environmental objectives associated with new construction. SHRP 2 is administered by the Transportation Research Board of the National Academies under a Memorandum of Understanding with the Federal Highway Administration and the America Association of State Highway and Transportation Officials. For more information, see www.trb.org/StrategicHighwayResearchProgram2SHRP2/Blank2.aspx (last accessed Jan. 30, 2014).

[278] VIIC, SCMS Organizational Policy Study, Interim Report, Dec. 11, 2012, at 15-16. See Docket No. NHTSA-2014-0022

- Payment Card Industry's governance via an agreement to adhere the Payment Card Industry Data Security Standard. Compliance with the 12 requirements of PCI DSS is necessary for merchants to be able to accept cards bearing the logos of the major payment card brands. The PCI Security Standards Council maintains PCI DSS, but enforcement of the standard is the responsibility of individual payment brands. The ATM Industry Association (ATMIA) is an independent, non-profit trade association that supports members of the ATM sub-industry through advocacy and education. Although critical for doing business, agreement to the PCI DSS is voluntary.[279]

Other than enforcement of those aspects of governance embodied in any agreement between the SCMS Manager and NHTSA, and any input provided via NHTSA's participation in a stakeholder board, as discussed above, under the private coalition model, NHTSA would play no further role in the self-governance of the SCMS "industry." The rules and obligations of industry participants would therefore depend on the entities that constitute and subject themselves to governance by the organization. A slightly different, potentially less inclusive (with regard to decision making) private governance model would result if an individual entity in the ITS marketplace, rather than a coalition group, agreed to serve as system manager overseeing the CME entities required for V2V safety; an individual entity could be an academic, State, or private (for profit or non-profit) organization. Either private governance model could be supplemented by a stakeholder "governance board" to establish or suggest policies and practices for the SCMS Manager to apply system-wide, to the extent that the private CME owners/operators agree to consider or be bound by such input.

With a private system owner/operation, ultimately, the details of internal governance (like the details of internal organization) would be up to that private CME entity/entities – in particular, the entity serving as SCMS Manager -- and the Federal Government's role would be limited to ensuring that entities honored the terms of their agreement with DOT or NHTSA, if an agreement exists. As noted above, that DOT agreement primarily would include a provision that the private SCMS's delivery of security functions required for V2V communications would be consistent with DOT's Principles for a Connected Environment, provide adequate market access, incorporate appropriate protection of privacy and security, and involve reporting and sufficient continuity of services obligations to ensure the long-term stability and availability of the SCMS. However, as noted above, the private model could be supplemented with a stakeholder governance board to advise on governance issues that NHTSA or JPO likely could support under a cooperative agreement or grant for that limited purpose.

[279] BAH SCMS Design and Analysis Report, at 35-36. See Docket No. NHTSA-2014-0022

While the private model possesses considerable benefits, it also carries certain risks that the Federal model does not. The primary risk of a purely private model involves continuity of SCMS function. With no Federal involvement, the party or parties owning and operating the SCMS theoretically could choose to stop doing so at some point. A V2V system needs an SCMS to function; if the SCMS owner/operator ceases to provide the security required for V2V communications, the V2V system will no longer work. Even with some amount of Federal involvement, it remains difficult to compel specific performance if the performing party chooses to stop performing. One option for minimizing the not insignificant risk associated with a private model, should NHTSA enter into an agreement with a private SCMS owners/operator, is to include certain contractual provisions in the agreement. NHTSA can structure the agreement so that the private SCMS owners/operator is required to provide sufficient notice of its intent to cease providing V2V security services and to continue operating the SCMS until NHTSA can identify another entity to assume operations, or so that the Federal Government receives liquidated damages in the event of non-performance. Of course, "lights out" also could be a risk under a Federal model if Congress suddenly withdraws funding after NHTSA establishes the SCMS. In any event, a thorough consideration of contingencies for risks such as this seems highly advisable.

4. Scope of the SCMS system governance

In order to define governance policy, it is first necessary to identify the SCMS functions that need governing in order to deploy V2V technologies, and why. Please note that there may be Federal, State, and local laws applicable to various areas discussed below as appropriate for governance. Where relevant, we have attempted to identify the applicable legal authority. However, as used in this discussion, the term "governance" focuses primarily on those aspects of the SCMS and SCMS activities *not* already addressed by existing laws.

To set the stage for this analysis, following is a brief summary of the industry perspective on governance needs, as represented by the VIIC,[280] and of NHTSA's somewhat different perspective.

a) The VIIC perspective

Pursuant to a cooperative agreement funded by DOT, the VIIC has provided to DOT a series of white papers summarizing their members' consensus views on various policy issues relating to V2V technologies. Also pursuant to that agreement, the VIIC has provided policy support to CAMP in its development of the technical and organizational/operational designs for the SCMS. As detailed above, CAMP has designed and the VIIC views the SCMS as a collection

[280] DOT funded the VIIC's research specifically to obtain industry's views on V2V policy issues such as privacy, liability, SCMS governance and data ownership.

of functions consisting of multiple organizational groups, specifically, a central SCMS Manager and central and non-central CME component entities.[281] Unlike DOT consultants, the VIIC does not regard as problematic a single CME entity conducting functions that are both central and non-central in nature, as long as select functions reside in separate legal entities. The VIIC sees a pressing need for a single SCMS Manager with governance authority over the CME component entities and the functions that make up the SCMS, listed above.

The mission of the SCMS Manager would be to:

- Set SCMS organizational structure
- Establish operational rules and processes
- Define means of separation of functions
- Provide mechanisms for certification, audit, enforcement and adjudication
- Establish funding mechanisms
- Provide adequate risk management, and
- Have ability to address cross-border issues

The VIIC has indicated that certain key functional areas, both outside and inside the SCMS, require the oversight, control and consistency of governance, Table IX-3[282]

Table IX-3 VIIC Concept of Security Certificate Management System Functional Area Distribution

Functions outside of the SCMS:	**Functions Within the SCMS:**
Performance requirements and standards (to be established by NHTSA FMVSS)	Security system (SCMS) internal operations and management Rules of operation and maintenance Rules of use and access to the SCMS for devices beyond V2V safety
Device certification and enforcement (under an FMVSS and the Motor vehicle Safety Act)	Device security interoperability
What messages and broadcast on what channels (FCC/NTIA/Spectrum Manager)	Privacy
Device communication interoperability (FCC/FMVSS)	Device certification with the SCMS
Spectrum Management (FCC/NTIA/Spectrum Manager)	Cross-border acceptance and international harmonization
Data access and ownership – usage, security and privacy*	Oversight/administrative functions
Liability Risk Management*	Funding

*According to VIIC but not NHTSA

[281] VIIC Assessment of Key Governance Policy Considerations for a Connected Vehicle Cooperative Safety Communications System – Part 1, at 16 (delivered to DOT on March 13, 2013). See Docket No. NHTSA-2014-0022.

[282] Id. at 10 *et seq.*

The VIIC has suggested that the functional areas falling outside of the SCMS, listed above, are those that likely will be governed by an FMVSS, the Motor Vehicle Safety Act, a spectrum manager, or other standards or entities.[283] The additional notes in parentheses identifying the likely sources of external governance outside of the SCMS that did not originate from the VIIC but were added by NHTSA for purposes of clarity.

b) NHTSA perspective

NHTSA generally agrees with the VIIC's characterization of the functions that need governance outside of the SCMS, with two significant exceptions marked by asterisks in the left column of the VIIC chart above: data access and ownership, and liability. To the extent not already addressed by existing Federal, State, and local law, we see data access and ownership to be squarely *within* the scope of the SCMS's governance of privacy and intellectual property/data rights through its Privacy Policies – not as an external function. Placement by the VIIC of access/ownership and privacy outside of the SCMS is, however, consistent with the VIIC's previously-expressed position that data access/ownership and privacy should be the subject of new Federal legislation and regulation designed to implement stringent restrictions on access to and use of BSM data broadcast by OBE. The VIIC position is grounded in the OEMs' concern that inadequate privacy protection will adversely affect consumer acceptance of V2V technology and, ultimately, new car sales. NHTSA understands that concern but believes privacy can adequately be protected through the SCMS.

A second area that NHTSA does not see as needing active or new forms of governance outside of the SCMS is that of liability/risk management. In our view, the liability of participants in the envisioned V2V warning system already is governed by existing Federal, State, and local laws and legal authority, including but not limited to those establishing tort/product liability for government and non-governmental entities and individuals.[284] The VIIC and NHTSA agree that how risk is allocated *within* the SCMS would be a matter for internal governance under the auspices of the system manager function.

NHTSA also agrees with CAMP and the VIIC about the key functional areas within the SCMS that will require the oversight, control, and consistency of a sole, central internal governance structure. In our view, the critical SCMS functional areas that will need internal governance and management are:

- **Organizational Structure/Ownership**: requirements for functional separation/groupings and expertise/viability requirements

[283] Id. at 12.
[284] Section X.

- **Operational Policies and Processes:** mechanisms for certification, audit, enforcement, and adjudication
- **Interoperability**: standards for device communications and security interoperability
- **Security/Privacy Assurance**: certificate policy, including physical, procedural, and technical controls
- **Privacy/Data Ownership Policy:** a policy applicable CME-wide that protects individual privacy and data that can be linked appropriately to an individual

However, we note that the latest SCMS design refers to the central internal management function as the "SCMS Manager." For consistency, throughout this discussion we, too, use the term SCMS Manager to refer to the function that would undertake internal operations and management of the CME component entities by providing policy and technical standards for the entire CME "industry." The SCMS Manager function could be carried out a number of different ways. As is often the case in large commercial industries, a volunteer industry consortium could take on this role. In other industries, or in public or quasi-public industries, a regulatory agency or other legal or policy entity often performs the central management role. In the context of the SCMS, we expect that a single legal/administrative entity will take on the SCMS Manager role – but, as noted above, that entity could function with input from a "governance board" funded by DOT via a cooperative agreement or grant, assuming available funds, if the private SCMS Manager entity consents to accepting such input on an advisory or ideally a binding basis.

X. Legal Liability

A. Overview

Legal liability is a policy issue frequently identified by industry -- and to a lesser extent by other stakeholders -- as a potential impediment to deployment of V2V technologies. The Federal Government has multiple available tools to limit legal liability, when Congress deems it appropriate to do so. If NHTSA moves forward with regulating V2V technologies, the agency will need to work with the Department to determine whether to support liability limiting or sharing mechanisms that would limit the legal exposure of industry, some or all parts of the SCMS, or potentially other stakeholders. However, ultimately, it will be up to Congress to determine whether such liability limiting mechanisms are appropriate in the context of V2V communications.

The decision options currently under consideration by NHTSA involve safety warning technologies -- not control technologies.[285] As discussed below, 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 does not view V2V warning technologies as creating new or unbounded liability exposure for industry. The agency, therefore, does not see a current need to develop or advocate the liability limiting agenda sought by industry in connection with potential deployment of V2V technologies via government regulation.

One factor that will contribute to NHTSA's assessment of the degree to which liability could be an impediment to development of a private SCMS is the extent to which the primary and secondary insurance markets make insurance coverage available to CME entities. Another factor will be the extent to which CME entities are able to limit their legal liability via terms of use or similar contractual mechanisms applicable to individuals or entities participating in the connected vehicle environment.

B. Industry's liability concerns and solutions

Throughout the V2V research process, DOT has accessed information about the positions of industry members on various V2V policy issues two primary ways: (1) through a cooperative agreement between JPO and the VIIC designed specifically to obtain industry's views on various

[285] To the extent that future regulatory action by NHTSA contemplates requiring safety control technologies, NHTSA will revisit the appropriateness of advancing liability limiting measures protective of industry and/or other stakeholders.

policy issues, and (2) through discussions with individual industry members. While the following discussion of liability references primarily the positions and views expressed by the VIIC, the concerns expressed informally by individual OEMs and manufacturers to DOT officials have been largely consistent with that of the VIIC. Not surprisingly, industry is worried that deployment of V2V technologies may increase its liability exposure.

The VIIC readily has acknowledged that manufacturers regularly address risk management as an integral part of designing and manufacturing vehicles for the real world.[286] However, it has suggested that cooperative crash avoidance safety applications present an "unprecedented challenge to risk management."[287] VIIC's position has been that "the design, development of ultimate deployment of DSRC-based V2X communications systems creates unique risk allocation concerns among the wide range of partisans (both public and private sector)" and that risk allocation is "further complicated by the introduction of aftermarket devices, the potential for system tampering/hacking, and the risk of unauthorized access to networks and to sensitive data."[288] As stated by VIIC, it may be difficult to determine who is liable for a V2V system failing to perform as the driver expected, due to the complexity of the system and the number of parties involved.[289] The VIIC also has noted that a NHTSA regulation promulgated under the Safety Act would not provide industry with adequate risk management because such regulations do not expressly preempt common law tort liability.[290]

In support of its position, the VIIC has compared DSRC communications designed to enable low-latency safety applications to convenience services provided over commercial wireless networks.[291] It concluded that "the potential risk implications for low latency safety warnings are substantially higher than exist today for convenience services."[292] The VIIC's liability assessment seems to be based, in large part, on the expectation that there will be no contract allocating risk among individuals and entities involved in the V2V environment. In the context of convenience services, such contracts control the relative distribution of risk among the multiple entities involved in providing services. By contrast, as envisioned by CAMP and the VIIC, presumably participants in a mandatory V2V safety system would not be required to enter into contracts with the security or communications service providers or other participants. In the

[286] White Paper on Risk Management Issues, Vehicle Infrastructure Integration Program, VIIC Deployment Analysis and Policy Work Order #4, Task 13 General Policy Support, at 2 [Hereafter, "VIIC Risk Management White Paper"], delivered to DOT on 4/18/2012. See Docket No. NHTSA-2014-0022.

[287] VIIC Risk Management White Paper, at 2.

[288] Id., at 1.

[289] Task 14 Aftermarket Device Research Addendum (06-30-2010 v3) p. 54, Nov. 8, 2011.[Need Docket #]

[290] VIIC, SCMS Organizational Policy Study, Interim Report, Dec. 11, 2012, at 2. See Docket No. NHTSA-2014-0022

[291] Risk Management White Paper, at 1.

[292] Id.

VIIC's view, there would be no contract, legal mechanism, or case law to provide courts with guidance on risk allocation.[293]

In addition to the lack of contractual limitations and legal precedent, other primary liability issues identified by the VIIC[294] include:

- Whether and, if so, how V2V warning applications increase the risk of liability for OEMs, operators, and drivers;
- The need for Congress to put in place one or more legal mechanisms for distributing risk among OEMs, operators, drivers, and other public and private stakeholders;
- Whether V2V warning applications will change the way the legal system assesses driver versus equipment error;
- Whether owners may be held legally accountable for shutting off or failing properly to maintain V2V warning systems; and
- Whether the human machine interface required for V2V warning systems will increase driver distraction in a way that will affect legal liability.

The VIIC has identified as examples of Federal liability limiting mechanisms preemption (explicit or implied), immunity (as with 911 services), indemnification (for Federal contractors), and other types of limitations on damages or ways to allocate risk to government and away from industry (other examples of which are detailed in a risk assessment report prepared by the Dykema law firm for the VIIC[295] under the JPO cooperative agreement).[296] The VIIC also has noted that "the nature and extent of desired liability protections will depend on the governance model chosen and reasonably anticipated legal risks."[297] VIIC has asserted that the greater the involvement of the government, the less likely it is that the SCMS's activities will be challenged or exposed to liability for harm to property or persons.[298] In discussions, both the VIIC and some specific industry members have tied their support for deployment of V2V safety technologies to the Federal Government's willingness to put in place liability limiting mechanisms. However, NHTSA does not believe this is a uniform industry position, in that not all OEMs consider liability protection as a condition precedent to going forward with V2V implementation.

[293] Id.

[294] Id., at 2.

[295] Dykema, Risk Assessment Report, under contract to VIIC (Policy work order, Task 6, Deliverable 1), Mar. 12, 2009, at 38-65. [Hereafter, "Dykema Risk Assessment Report"]. See Docket No. NHTSA-2014-0022.

[296] VIIC, SCMS Organizational Policy Study, Interim Report, Dec. 11, 2012, at 19. See Docket No. NHTSA-2014-0022

[297] Id.

[298] Id., at 26.

C. Liability concerns specific to the SCMS

Specifically with respect to the SCMS, the VIIC has indicated that it views liability risk management within the SCMS as a key functional area requiring internal governance.[299] The VIIC identified the SCMS Manager as the entity with responsibility not only for *governing* liability risk management within the SCMS but also for *providing* liability risk protections to all CME entities making up the SCMS.[300] The VIIC has taken the position that the Federal Government will need to grant to the SCMS broad governance authority (through statute, Executive Order, regulation, contract, or other means) – possibly cross-border authority -- and has stated that the mechanism through which legal authority is conveyed could provide liability protections for central or non-central SCMS elements.[301]

D. Federal liability limiting mechanisms

The Federal Government has at its disposal a range of mechanisms to limit the liability of private and public entities and individuals, when Congress deems it appropriate. Some examples of liability limiting mechanisms include:

- **Explicit/Implicit Preemption**, e.g., under the Federal Motor Vehicle Safety Act;
- **Contractual Indemnification via contract or agreement**, e.g., indemnification for contractors providing hardware and software to update the FAA's air traffic control system under its En Route Traffic Computer Replacement Program; Public Law 85-804, the indemnification authority primarily used by the Department of Defense;
- **Statutory Immunity,** e.g., Federal Volunteer Protection Act, extending immunity protections to volunteers affiliated with non-profits provided they do not receive compensation in excess of $500 per year;
- **Capped Liability,** e.g., Amtrak Reform and Accountability Act of 1997, limiting overall damages from passenger claims to $200 million from a single railway incident and explicitly authorizing passenger rail providers to enter into indemnification agreements; Oil Pollution Act of 1990, passed after the *Exxon Valdez* accident, making oil companies responsible only for the first $75 million of liability claims from businesses and organizations affected by a spill; and
- **Risk Transfer, Insurance Pools, and Reinsurance Programs**, e.g., Price-Anderson Act, providing for two-level insurance pool covering nuclear power industry;

[299] VIIC Assessment of Key Governance Policy Considerations for a Connected Vehicle Cooperative Safety Communications System -- Part 1, at 5 (Mar. 12, 2013). [Hereafter, "VIIC Governance Paper"]. See Docket No. NHTSA-2014-0022.

[300] Id., at 15 and 20.

[301] Id., at 19.

Commercial Space Launch Act of 1984, requiring insurance up to 500 million cap with 500 million to 1.5 billion in coverage provide by Federal Government.

These are just a few examples of liability limiting or risk shifting mechanisms. Many such programs are hybrids created to address specific catastrophic risks or to encourage development and/or deployment of new technologies.

All such programs require Congressional approval. The question for NHTSA is whether public and private entities that may be involved in provision of V2V communications, including but not limited to the OEMs, will agree to move forward with deployment of V2V communications if DOT does not seek and Congress does not approve some form of liability limiting/risk sharing program.

E. NHTSA's assessment of industry liability

Will industry concerns about liability be a stumbling block to regulation of V2V technologies? We think not – at least not to the dramatic extent that some industry stakeholders have suggested.

Under traditional product liability tort law theories,[302] OEMs will be responsible if they manufacture and sell a defective product that causes harm to a person or property.[303] This includes liability for design defects, manufacturing defects, and defects due to inadequate warnings.[304] According to one legal analysis, there are a number of different potential product liability claims that could be associated with V2V technologies.[305] As stated above, the VIIC has suggested that it may be difficult to determine who is liable for a V2V system failing to perform as the driver expected, due to the complexity of the system and the number of parties involved.[306]

However, the V2V technology currently under consideration results in safety warnings - not motor vehicle control. For this reason, ultimately, it is the driver who remains responsible for failing to avoid a crash. It will be difficult for a driver to prove that an accident would have been avoided had the V2V system functioned properly. Potential liability based on V2V defects,

[302] Product liability laws vary from State to State, but a good overview of the relevant common themes in State product liability tort law is set forth in the Dykema Risk Assessment Report, at 21-34.
[303] Restatement (Third) of Torts Ch. 1 § 1.
[304] Restatement (Third) of Torts Ch. 1 § 1.
[305] The Dykema Risk Assessment Report identified four groups of likely product liability claims stemming from to V2V: (1) OEM failure to deploy V2V; (2) improper installation or location of technology; (3) failure to maintain OBE; and (4) claims associate with operation and use of OBE, including OBE failures and claims involving operator-OBE interaction.
[306] Task 14 Aftermarket Device Research Addendum at 54 (06-30-2010 v3, Nov. 8, 2011). See Docket No. NHTSA-2014-0022

therefore, will be limited substantially by lack of causation due to drivers' roles in failing to avoid crashes.

A lawsuit also might allege that a crash was caused, in whole or in part, by a failure in the communications infrastructure supporting V2V (e.g., an RSE). However, as evidenced by the numerous lawsuits claiming that failure of a traffic light contributed to an accident, such cases typically are brought against public or quasi-public entities and not against vehicle manufacturers.[307] For this reason, we would not expect alleged failures in V2V infrastructure to impact OEM liability in a significant way.

Significantly, V2V safety warnings are not very different in terms of application or interaction with the driver than on-board safety warning systems found in many of today's motor vehicles. Under the existing product liability tort law framework, manufacturers have the ability to take steps to limit their legal liability stemming from such on-board systems through a variety of mechanisms (e.g., compliance with applicable safety standards, contractual indemnification by OBE suppliers, dispute resolution/arbitration clauses applicable to supplies and consumers[308]). One important mechanism is provision by the OEM of adequate consumer warnings and instructions for using V2V equipment. Such consumer warnings and instructions would emphasize the limited role of V2V safety warning technology and explain the limitations of the system in the foreseeable operating environment.[309] As specifically noted in the Dykema Risk Assessment Report:

> This approach does not call for a new or unprecedented effort. Newer vehicle models currently on the market that are equipped with systems such as lane-departure warning, backover detection warnings, and forward vehicle detection typically follow this approach in carefully describing the operation and limitation of these systems.
>
> We would expect that manufacturers would follow this same approach to limiting their potential liability in connection with V2V warning systems.[310]

F. NHTSA's assessment of SCMS liability

Will industry concerns about liability be a stumbling block to creation and operation of a private SCMS "industry?" For the reasons discussed below, we think probably not – and certainly not to the extent suggested by the VIIC and certain members of the industry.

[307] Dykema Risk Assessment Report, at 33.
[308] Dykema Risk Assessment Report, at 34-38.
[309] Dykema Risk Assessment Report at 35 ("these systems differ from traditional technologies because of the manner and degree of interdependence on systems outside the host vehicle (other vehicles, RSEs, communications systems) and also because they may be affected by roadway, environmental, and other variables over which the OEM has little or no control").
[310] Id.

As discussed elsewhere in this report, to date, NHTSA has focused on a private model of SCMS governance that would not involve Federal funds or a Federal grant of formal legal authority to the SCMS or SCMS Manager -- but instead would result from the CME entities themselves agreeing to "self-governance" by a central SCMS Manager pursuant to binding contracts or agreements. Such industry self-governance by an SCMS Manager likely would involve the SCMS Manager establishing minimum insurance requirements and/or negotiating, on behalf of members, for system-wide insurance coverage. The SCMS Manager also might work with the CME entities to determine the appropriate distribution of liability for harm. However, the SCMS Manager would not necessarily be the entity responsible for *providing* liability protection to individual CME entities, whether central or non-central, as has been suggested by the VIIC. Unless the SCMS Manager worked with the CME entities to distribute risk among participants in a way that provides indemnity to some entities, the agency presumes that individual CME entities would carry liability insurance sufficient to ensure adequate coverage, in accordance with the insurance requirements established by the SCMS Manager.

The agency also anticipates that any contract or agreement between NHTSA and the SCMS Manager and/or SCMS entities would be limited primarily to ensuring adequate system security and privacy, periodic reporting, and ready access to information need by NHTSA to investigate and recall defective vehicles or V2V equipment. Additionally, at this time NHTSA does not see the need for a formal grant of legal authority to a private SCMS, either with or without some form of contractual liability limitation.

As discussed above, the V2V technology under consideration results in safety warnings - not motor vehicle control – and, ultimately, it is the driver who remains responsible for failing to avoid a crash. For this reason, it will be difficult for a driver to prove that an accident would have been avoided had the SCMS security system functioned properly. Potential liability based on failures in the SCMS, therefore, will be limited substantially by lack of causation due to drivers' roles in failing to avoid crashes. It also is not clear to the agency why an SCMS Manager could not require that individuals and entities participating in an SCMS agree to terms of use that would limit the liability of the SCMS and its component entities, either explicitly or via the same type of instructions and explanations of system limitations that the OEMs would use to limit liability.

Additionally, the automotive industry seems to have significant incentives to help stand up and operate several elements of the SCMS, as currently designed, including the RA and SCMS Manager. As the only outward facing component of the SCMS, the RA is critical to the ability of individual OEMs to maintain control over its customer relationships. As the entity charged with establishing and enforcing policies and procedures applicable to all CME entities making up the SCMS, the SCMS Manager presumably will promulgate policies directly implicating the financial interests of OEMs and other manufacturers, such as liability distribution and intra-CME fees (i.e., the costs to motor vehicle and device manufacturers of obtaining certificates and certificate-related services (e.g., device type certification and bootstrapping)).

While the organizational structure of the SCMS will need to be consistent with anti-trust laws and sound conflict of interest principles, the VIIC's governance deliverables to date consistently have reflected industry's interest in having a strong voice in SCMS governance (which, in the context of the CAMP SCMS design, means a strong voice in the operation of the SCMS Manager). Industry's voice in governance cannot be assured unless it plays a significant role in standing up and operating a private SCMS.

Nevertheless, the agency believes that it is premature to take a position on the need for liability limiting mechanisms applicable to some or all CME components of the SCMS in order to encourage the establishment and operation of a private SCMS to provide security for V2V communications. As noted by the VIIC, the appropriateness of such liability limiting/risk sharing measures will turn on the constitution and governance of the SCMS. Another factor affecting NHTSA's assessment of whether liability could be a stumbling block to development of a private SCMS will be the extent to which the primary and secondary insurance markets will make insurance coverage available to CME entities.

XI. Preliminary Cost Estimates of V2V Implementation

A. Overview of preliminary estimated V2V costs and benefits

The preliminary estimates explored in this and the following sections are based on currently emerging, prototype V2V technologies and existing data. The agency would expect these estimates to be revised when more advanced technologies and additional data are available for inclusion in an analysis. This and the following sections on benefits and cost-effectiveness are considered a minimal analysis of three potential scenarios with current, prototype V2V technology. The agency would need to conduct a more comprehensive regulatory impact analysis if there was a need to support any such action.

This section details the process of how the agency estimated preliminary costs for potential V2V technology deployment. The following section, Section XII, describes the preliminary benefit analysis.

The preliminary cost and benefit estimates are provided for three pre-determined technology implementation scenarios. These estimates provide a wide range of cost and benefits of a potential V2V implementation. The cost in this analysis comprises four categories: vehicle equipment, fuel economy impact, communications costs, and SCMS. Together, we estimate that the total cost per vehicle to the consumer for each vehicle will be approximately $341 to $350 in 2020 (across the 3 percent to 7 percent discount rates and three scenarios). This amount is projected to decrease over time to an approximate range of $209 to $227 by 2058. Of the four cost categories, the initial vehicle component cost is estimated separately for new vehicles and old vehicles. The component cost is $329 per new vehicle in 2020, and it will decline progressively to $186 to $199 in 2058. The fuel economy impact is estimated to be $9 to $18 per vehicle. The communications costs range from $3 to $13 per vehicle, with an average cost of $8.30 to $8.50. The component cost (i.e., aftermarket safety devices) per old vehicle range from $160 to $387. The SCMS costs range from $1 to $6 per vehicle with an average of $3.14. The SCMS cost will increase over time due to the need to support an increasing number of vehicles with the V2V technologies.

The total preliminary annual costs (the sum of the four categories of costs) of the V2V system fluctuates year after year but generally show a declining trend. The estimated total annual costs range from $0.3 to $2.1 billion in 2020 with the specific costs being dependent upon the technology implementation scenarios and discount rates. The costs peak to $1.1 to $6.4 billion between 2022 and 2024, and then they gradually decrease to $1.1 to $4.6 billion.

B. Discussion of V2V preliminary cost estimates

Based on the agency's preliminary assessment, the total annual costs of the V2V system will vary substantially from year to year. In addition to the on-board equipment (OBE) costs of a V2V system (i.e., the components that need to be installed on a vehicle to support the V2V safety applications operating in the system), there are also costs for fuel economy impacts, the SCMS, and communication between the SCMS and OBEs. These cost estimates are highly influenced by the technology implementation pace. Therefore, the agency used three different implementation scenarios (i.e., the rate at which new vehicles and aftermarket devices are purchased each year) to illustrate the potential total costs and the annual impact of establishing a V2V system. These three scenarios range from an aggressive implementation schedule that includes aftermarket devices and 100 percent implementation for new vehicles in three years, to a relatively slower implementation schedule that does not have aftermarket devices and with a maximum of 25 percent of full implementation. Across the three scenarios and two discount rates (3 percent and 7 percent), the estimated total costs rise from $0.3 to $2.1 billion in 2020 to a total of $1.1 to $6.4 billion in 2022, and gradually decrease to a relatively stable level of $1.1 to $4.6 billion.

Breaking down those annual cost estimates, NHTSA currently estimates, based on our preliminary information, that the on-board equipment necessary to support the V2V safety applications would cost $329 per vehicle in 2020, with the possibility that these costs will decrease over time as manufacturers gain experience producing this equipment (a phenomenon known as the "learning curve"). Given the various sales scenarios considered, we believe that the price per vehicle could be as low as $260 in 2022 and $186 in 2058, as discussed in more detail below.

In addition to the cost of purchasing/installing the V2V equipment, there are fuel economy costs due to the weight of the V2V equipment. The agency estimated that V2V equipment will increase each vehicle's total weight by approximately 3.45 pounds. Consequently, it will increase fuel costs by between $9 and $12 for passenger cars over the lifetime of the vehicle, and $11 to $18 for light trucks.

The next cost category is the secure communications cost which is the cost of ensuring secure communications between vehicles and the SCMS and among the SCMS operations. For the first 3 years, based on our assumptions about certificate issuance and delivery, no communications will occur to renew certificates. Further, due to the low overall V2V penetration rate among the operational vehicles, the agency believes that the probability of misbehavior is extremely low and thus the need for a secure communication is not critical. There are, therefore, no communication costs for the first three years. In year 4, the average per-vehicle cost to pay for communication is estimated to be $8.58 to $10.74, with the price potentially as low as $3.37. At its peak, the per-vehicle cost increases to $12.39 to $12.97, with an average fee that could be charged to vehicles sold from year 4 through the next 37 years ranging from $8.30 to $8.50.

The final cost is that of the SCMS itself, which will ensure that vehicles will be able to distinguish trustworthy message sources from those that are not, and, thereby, ensure that the V2V system operates most effectively. We anticipate that the initial and ongoing cost of this SCMS can be covered with a one-time fee of $3.14 per new vehicle sold. In other words, supporting the functions of the SCMS would add an additional $3.14 to the cost of each vehicle sold.

In summary, supporting the functions of the SCMS and communications would add an estimated additional $11.44 to $12.64 to the average cost of each vehicle sold.

Table XI-1 Summary of Preliminary Costs per Vehicle

Cost category	**Amount in dollars**
Vehicle Equipment Costs	$329 in 2020, decreasing to $186 to $199 in 2058
Fuel Economy Impact	$9 - $18
Security Credentials Costs	$3.14
Communications Costs	$8.30 - $8.50
Total Costs	$341 to $350 in 2020, decreasing to $209 - $227 in 2058

C. Projected vehicle equipment costs

To fully evaluate the vehicle equipment costs, we first estimate the costs for the following potential system configurations.

- Original Equipment Manufacturer:
  - Full V2V system installed in new passenger vehicles (passenger cars and light trucks)
- Aftermarket:
  - Retrofit: connects to the vehicle's data bus, sends and receives BSM, and provides advisories/warnings
  - Self-contained: does not connect to the vehicle's data bus and only uses a wire to get power from the vehicle, sends and receives BSM, and provides advisories/warnings
  - Vehicle Awareness Device: uses a wire to get power from the vehicle, sends out but does not receive BSM, and does not provides advisories/warnings

Second, we consider three technology sales scenarios that represent potential rates at which these V2V systems can be adopted into the vehicle fleet. Finally, we apply our knowledge of learning (the potential savings that manufacturers can realize due to their experience producing the equipment), based on the three sales scenarios, to show what potential final equipment costs can be.

1. OEM devices

For V2V systems installed on vehicles as original equipment, our preliminary estimates are based on confidential information provided by two suppliers. Relying on that information, NHTSA estimates that the cost to install the supplier equipment into the vehicle will result in a per-vehicle cost to the consumer of $342.80 ($327.13 + $15.67) in 2012 dollars. As shown in Table XI-2, below, we anticipate that the equipment at the supplier level will cost $216.79, while the installation will cost $10.38. After accounting for the retail price equivalent of 1.51, which includes the additional costs necessary before the product reaches the consumer, and also for the reduction in costs due to the current installation rate of GPS units (meaning that if GPS is already present on a vehicle, the addition of V2V technology does not require another GPS unit), we estimate the increase in per-vehicle cost will be $329.14 in 2020. We further explain our estimates for the supplier costs, installation costs, and GPS market penetration in separate sections below.

We anticipate that manufacturers and suppliers will realize cost savings over time due to additional experience in manufacturing V2V safety equipment; however, any potential cost savings due to this additional experience are not included in cost tables until after these effects are discussed in the section titled "Learning," below.

Table XI-2 Summary of Likely Costs in Year 1 for New Vehicles (2012 dollars)

	Variable Costs[311]	**Consumer Costs**[312]
Supplier Costs	$216.79	$327.13
Installation Costs	$10.38	$15.67
Minus Current GPS Installation	$9.20	$13.89
Total	$217.97	$329.14

a) Variable costs to OEMs

As shown in the "Total" row in Table XI-3, below, our current preliminary estimate is that the V2V equipment that suppliers provide to OEMs will cost $216.79.

As discussed in Section V.B.2, we assume that two DSRC radios and two DSRC antennas are necessary: One DSRC to send and receive the BSM, and a second to handle security aspects of receiving certificates, the certificate revocation list, etc. The supplier cost estimate of $130 for 2 DSRC transmitters and receivers is composed of $70 for the first DSRC and $60 for the second. The $10 reduction in cost for the second DSRC was based upon the assumption that

[311] "Variable costs," in the table, refer to the direct cost – that is, the cost of the parts and materials – to the manufacturer to include this technology in a vehicle.

[312] "Consumer costs" refer to the variable costs plus the fixed costs that the manufacturer incurs and passes forward to the consumer.

the two DSRCs would be packaged together, thereby resulting in lower labor in assembling this combined package at the supplier, as well as lower parts costs to package them together rather than individually. No such assumption was made for the antenna, since these have to remain physically separate in order to avoid interfering with each other.

Table XI-3 Likely Supplier Costs to OEM

Component	Weight[313]	Cost
	(in lb.)	(2012 dollars)
DSRC Transmitter/Receiver (2)	0.65	130
DSRC Antenna (2)	0.44	10
Electronic Control Unit	0.55	45
GPS		14
GPS Antenna	0.22	4
Wiring	1.20	9
Displays	0.17	4.79
Total	3.23	216.79

Our information on the variable costs to OEMs, when they are purchasing supplies, is based on data received from two suppliers in response to a voluntary request for cost information sent to eight suppliers of V2V equipment. In order to help ensure consistent production estimates, we asked the suppliers to prepare their cost estimates based upon the assumption of high-volume production (i.e., meaning at least 250,000 sales per make/model), in order to model the expected production that would result if, sometime in the future, the agency required V2V and if all light vehicle sales were thus affected. This assumption helped ensure consistent estimates across suppliers who responded, since low volume sales result in very high initial prices, and if each responding supplier had picked a different volume of sales, the responses would not have been easily comparable. Again, assumptions regarding the learning curve will be applied later in the analysis.

We made several adjustments to the information we received from the two suppliers to arrive at the above estimates. First, the agency has changed some of its assumptions since requesting information from these suppliers (e.g., we now believe that two DSRC radios and two DSRC antennas are necessary, rather than one DSRC radio and one DSRC antenna). Second, the suppliers provided estimates relating to costs of equipment they supplied, but these estimates did

[313] Because this table is the first time we break out the costs of the individual pieces of in-vehicle V2V equipment, we also use this table to roster the weight of each of the individual pieces as well as the cost of each of the individual pieces. See Section XI.C.1.b) below for discussion of the impacts to consumer benefits of increasing vehicle weight.

not necessarily include costs for driver warnings for the safety applications that would use V2V, nor did they include labor and wiring necessary for the OEM to install the equipment into the vehicle. The information from the suppliers was thus incomplete for our current purposes, and more assumptions were needed in order to provide a more complete estimate of costs.

We also assumed that all vehicles would already have the FCW application in them by the time V2V was required in vehicles, given that the agency anticipates counting the costs and benefits for that application as part of a separate regulatory effort.[314] Thus, additional costs for displays and wiring to displays were not assumed for FCW for purposes of this analysis, meaning that the preliminary costs (and benefits) associated with requiring V2V technology are slightly lower (albeit only $1-$2) than they would have been without this assumption.

b) Preliminary Consumer costs

The costs in Table XI-3 reflect the preliminary estimated costs that the OEM pays to the supplier to obtain these components. However, they do not reflect the cost of these systems to consumers. Table XI-4 provides preliminary consumer costs for these supplier parts. To obtain consumer costs, the costs to the OEM for each variable are multiplied by 1.51 to estimate a retail price equivalent (i.e., consumer cost). The agency uses the 1.51 markup to represent fixed costs (research and development, selling and administrative costs, etc.), as well as OEM profits, transportation costs, and dealer costs and profits. Additional costs to consumers (e.g., installation costs) are estimated separately and further discussed later.

Table XI-4 Preliminary Consumer Costs (for just supplier parts) Per Vehicle (2012 dollars)

Component	Consumer Cost
	(2012 dollars)
DSRC Transmitter/Receiver (2)	196.3
DSRC Antenna (2)	15.10
Electronic Control Unit	67.95
GPS	21.14
GPS Antenna	6.04
Wiring	13.59
Displays	7.24
Total	327.13

[314] This assumption may change. If NHTSA does not require FCW in a regulatory action prior to any V2V regulatory action, the costs of benefits of FCW may, at least in part, be attributed to V2V.

c) *Additional Detail on Preliminary Display Costs*

A further breakdown of costs that are already included in Table XI-3 and Table XI-4 is provided in Table XI-5 below, where additional detail on our estimates for weight and costs of displays are shown. Cost information gathered for displays include both manufacturer-produced and supplier-provided displays, as well as different types of displays (e.g., display lights, malfunction lights) that can be used by the safety applications to inform drivers of potential dangers identified by V2V communications. One such display, a heads-up display (i.e., one displayed on the windshield in the driver's field of vision), is a more expensive system, as shown in the cost tear-down results for two heads-up display systems (see Table XI-5 below).

Table XI-5 Preliminary Estimates of Display Costs (2012 dollars)

	Weight (lb.)	Variable Costs	Consumer Costs
Five display lights[315]	.05	$1.00	$1.51
Malfunction light[316]	.01	$1.29	$1.95
Light bar	.20	$2.50	$3.78
Total	.26	$4.79	$7.24
Info. not used			
Heads-up display Volvo S8[317]	.17	$6.91	$10.43
Heads-up display Ford Taurus[318]	.16	$12.67	$19.13

Warnings can be presented to the drivers via different modalities (e.g., auditory, visual, haptic) and for our analysis, the following assumptions and inclusions were made:

- Auditory Displays: We did not include any cost for audible warnings at this time, based on the assumption that any audible warnings required for a V2V system would use existing audible warning equipment already in the vehicle at that point. If more refined warnings were to be required, that would add costs.
- Visual Displays: We assume very simple visual display lights for five applications, including EEBL, DNPW, BSW/LCW in the A-pillar or side view mirror (one display for both, but one on each side), and LTA. Wiring to these displays is considered separately. We assume a much more complex light bar for IMA (like one used in a

[315] Five display lights is an assumption for purposes of analysis.

[316] Cost and Weight Analysis of Advanced Frontal Airbag Systems (Final Report, Volume 1, Docket number NHTSA-2011-0066-0001). See www.regulations.gov/#!documentDetail;D=NHTSA-2011-0066-0001 (last accessed Jan. 29, 2014).

[317] NHTSA FCWS Final Report, at 61/103 (May 16, 2012). See www.regulations.gov/#!documentDetail;D=NHTSA-2011-0066-0011 (last accessed Jan. 29, 2014).

[318] Id., 49

V2V demonstration vehicle that would be situated along the top of the dash next to the windshield and run up the A-pillar a little), that would attract the driver's eyes toward the direction of the encroaching car.[319] We also assume that a malfunction light would be required to tell you that the V2V system is not working and you should have your vehicle serviced.[320]

- Haptic Displays: It is also possible that some manufacturers might choose a haptic display. Even though the agency has no cost estimates for haptic displays, we believe haptic displays would typically be more costly than the displays we have included in this analysis.

d) Preliminary Installation cost estimates

The main installation cost is labor, but there are also some costs for materials used in the installation of the vehicle equipment (e.g., minor attachments such as brackets or plastic tie downs to secure wires). In the table below, estimates for installation costs are separated into "Material Costs" (for the minor attachments), "Labor Costs," and "Variable Burden" (i.e., other costs that are not direct labor or direct material used in the part, but are costs that vary with the level of production, such as set-up costs, in-bound freight, perishable production tools, and electricity). We estimate that the variable cost to OEMs to install the V2V equipment is $10.38 and that the cost to consumers will be $15.67 given the 1.51 RPE (See Table XI-6, below). Note that the weight of the installation materials is assumed to be 0.1 pounds.

Table XI-6 Preliminary Installation Cost Estimates (2012 dollars)

Part	Material Cost	Labor Cost	Variable Burden	Total Variable	Total Consumer Cost
DSRC Transmitter/Receiver	0.03	1.25	0.81	2.10	3.17
DSRC Antenna	0.03	0.10	0.07	0.20	0.30
Electronic Control Unit	0.02	1.78	1.15	2.95	4.45
GPS	0.03	0.10	0.07	0.20	0.30
GPS Antenna	0.03	0.10	0.07	0.20	0.30
Wiring	0.18	0.88	0.57	1.63	2.47
Five Displays + Malfunction Disp.	0.00	0.61	0.39	1.00	1.51
Light Bar	0.03	1.25	0.81	2.10	3.17
Total	0.36	6.07	3.94	10.38	15.67

[319] Some manufacturers might choose to use a heads-up display system for V2V warnings, but the agency does not consider it necessary at this time, and it has therefore not been included for purposes of the current analysis. See Section XI.C.1.c) for further heads-up display costing information.

[320] The agency notes this would be a minimal approach to malfunction indication and that other, more explicit, malfunction warnings could potentially be developed.

Generally, the ideal source of information for installation costs is a cost teardown study. However, we do not have a teardown study for V2V parts, in part because there are no production-volume systems yet to analyze: it is difficult to tear down something that does not exist. Thus, we examined a similar installation cost-estimation teardown analysis. Installation costs were taken from a 2012 report titled "Cost, Weight & Lead Time Analysis of Lane Departure Warning Systems and Lane Keeping Systems Technology Associated with Passenger Vehicles," by Lieberman & Associates.[321] While the parts are not the same, we believe that the process for installing these parts would have similar material, labor, and variable burden costs. The cost estimates in this report are in 2011 dollars, so they were multiplied by the GDP deflator (115.338/113.369 = 1.0178) to bring them up to 2012 dollars.

Specifically, in this report, costs are estimated for installing back-up systems (e.g., a camera, ECU, displays) into six different make/models of vehicles. While the system examined in the Lieberman & Associates report contains different components from the V2V system (e.g., the V2V system uses a DSRC radio instead of a camera), we believe that the installation burden for these components is similar. With both systems, manufacturers receive these components from suppliers and are installed using similar tools.

In addition to using the cost estimates from the Lieberman study, a few assumptions were made in our analysis. For wiring, we assumed a variable labor cost of $21.14.[322] We also assumed that these new wires would be combined with other wiring harnesses, so the incremental cost would be the time to identify and hook up the wires, at 10 seconds per wire to hook up both ends and with a total of 15 separate wires that would need to be installed (seven for displays and malfunction lamp and eight between the two DSRC radios, two DSRC antenna, GPS, GPS antenna, amplifier, and ECU).

e) Current GPS installation rate

While the supplier costs and the installation costs are both costs that are incurred in order to install the components necessary to support V2V safety applications, many vehicles are already being equipped with GPS units. For those vehicles, the GPS component of the V2V system is not a cost that is attributable to the V2V system, since the current information available

[321] Docket No. NHTSA-2011-0066-0033. See www.regulations.gov/#!documentDetail;D=NHTSA-2011-0066-0033. Available at www.regulations.gov/contentStreamer?objectId=09000064811e9b8c&disposition=attachment&contentType=pdf [Note: There is a discrepancy in the title of this report, one version of which omits the word "Weight."]

[322] Production Occupations, 51-2099 Assemblers and Fabricators, Motor Vehicle Manufacturers (Bureau of Labor Statistics, May 2012). See www.bls.gov/oes/current/oes512099.htm (last accessed Jan. 28, 2014).

to the agency indicates that navigation-grade GPS units are sufficient for the V2V safety applications.

For MY2011, NHTSA estimates that about 50 percent of the new light vehicle fleet has GPS (and a GPS antenna) in their vehicle (see Table XI-7 below). This estimate is based on: (1) information about vehicles with navigation systems, which is contained in Wards Automotive Yearbook 2012 that has MY2011 data on factory-installed equipment such as navigation (NAV); and (2) assumptions about OEM Automatic Collision Notification systems (like OnStar), which have GPS as part of the system. An estimated 18 percent of MY2011 light vehicles have navigation systems. In addition, a high proportion of BMW, Ford, and GM vehicles have ACN, and other manufacturers (Toyota and Hyundai) have similar systems. However, we do not have information on what percent of their vehicles are covered now. It is nevertheless likely that more than 50 percent of the new light vehicle fleet already have GPS, and would not need to spend additional money on GPS for V2V. This estimate of the current market penetration of GPS systems is, therefore, subtracted from the total costs of equipping all vehicles with V2V safety applications in this analysis. However, if the data indicate that more advanced GPS systems are necessary, then we would need to revisit these cost assumptions.

Table XI-7 Estimated Percentage of GPS in the New Vehicle Fleet

Passenger Cars			LTV			TOTAL		
MAKE	NAV %	NAV + ACN EST.	MAKE	NAV %	NAV + ACN EST.	MAKE	NAV %	NAV + ACN EST.
BMW	22%	100%	BMW	39%	100%	BMW	31%	100%
CHRYSLER	24%	24%	CHRYSLER	24%	24%	CHRYSLER	24%	24%
FORD	5%	80%	FORD	14%	80%	FORD	11%	80%
GM	7%	90%	GM	18%	90%	GM	14%	90%
HONDA	12%	12%	HONDA	38%	38%	HONDA	25%	25%
HYUNDAI	8%	8%	HYUNDAI	7%	7%	HYUNDAI	8%	8%
JAGUAR	100%	100%				JAGUAR	100%	100%
			LAND ROVER	84%	84%	LAND ROVER	84%	84%
MAZDA	6%	6%	MAZDA	35%	35%	MAZDA	15%	15%
MERCEDES	54%	54%	MERCEDES	66%	66%	MERCEDES	61%	61%
MITSUBISHI	8%	8%	MITSUBISHI	14%	14%	MITSUBISHI	10%	10%
NISSAN	15%	15%	NISSAN	39%	39%	NISSAN	24%	24%
PORSCHE	35%	35%	PORSCHE	37%	37%	PORSCHE	36%	36%
SAAB	10%	10%				SAAB	10%	10%
SUBARU	6%	6%	SUBARU	41%	41%	SUBARU	28%	28%
SUZUKI	6%	6%	SUZUKI	0%	0%	SUZUKI	5%	5%
TOYOTA	8%	8%	TOYOTA	24%	24%	TOYOTA	15%	15%
VW	10%	10%	VW	48%	48%	VW	14%	14%
VOLVO	35%	35%	VOLVO	35%	35%	VOLVO	35%	35%
TOTAL	11%	36%	TOTAL	23%	59%	TOTAL	18%	49%

f) Summary of new vehicle V2V weight and cost estimates

Table XI-8 summarizes the variable and consumer costs for original equipment manufacturers for the first year. Costs are assumed to decrease in years after the initial year based on the learning curve.

Table XI-8 Summary of Cost Estimates in Year 1 for New Vehicles

(2012 dollars)

	Weight (lb.)	Variable Costs	Consumer Costs
Supplier	3.23	$216.79	$327.36
Installation	0.36	$10.38	$15.67
Subtotal	3.59	$227.17	$343.03
Minus Current GPS Installation	0.14	-$9.20	-$13.89
Total	3.45	$217.97	$329.13

2. Aftermarket devices

Preliminary costs are estimated for the three possible aftermarket V2V systems described in Section XI.C: Retrofit, Self-contained, and Vehicle Awareness Device (VAD).

The same two suppliers provided cost estimates for these three types of aftermarket devices. NHTSA asked them to provide estimates assuming both that they were sold individually, and in groups of 1,000 units to retailers or to other large purchasers. NHTSA developed likely estimated costs for these three types of aftermarket devices, using these estimates and other NHTSA estimates based on the same rationales used previously to estimate new vehicle costs. The next three tables show the estimated consumer costs.

Basic assumptions used in each of these estimates are:

- For aftermarket devices sold individually, we assumed a markup factor of 1.5 from variable costs to consumer costs;
- For aftermarket devices sold as an order of 1,000 or more products, we assumed a markup factor of 1.3 from variable costs to consumer costs;
- That the learning curve will apply to aftermarket devices also, since their main components will be the same as the OEM components of DSRC transmitter/receiver and antenna.

Table XI-9, Table XI-10, and Table XI-11 provide the estimated consumer component costs and weight for all three aftermarket device types. These are just equipment costs and do not include the costs of installing the equipment into used vehicles.

Table XI-9 Estimated Consumer Cost of Aftermarket Equipment – Retrofit Device (2012 dollars)

Component	Weight	Cost Per Unit for	
	(in lb.)	1 Unit	1,000 Units
DSRC Transmitter/Receiver (2)	0.65	$144	$124.8
DSRC Antenna (2)	0.44	15	13
Electronic Control Unit	0.55	67.5	58.5
GPS	0	21	18.2
GPS Antenna	0.22	6	5.2
Wiring	0	15	13
Displays	0	22.5	19.5
Total	1.86	291.00	252.20

Table XI-10 Estimated Consumer Cost of Aftermarket Equipment – Self-Contained Device (2012 dollars)

Component	Weight	Cost Per Unit for	
	(in lb.)	1 Unit	1,000 Units
DSRC Transmitter/Receiver (2)	0.65	$114	$98.8
DSRC Antenna (2)	0.44	15	13
Electronic Control Unit	0.55	67.5	58.5
GPS	0	21	18.2
GPS Antenna	0.22	6	5.2
Wiring	0	12	10.4
Displays	0	10.5	9.1
Total	1.86	246.00	213.20

Table XI-11 Estimated Consumer Cost of Aftermarket Equipment – Vehicle Awareness Device (2012 dollars)

Component	Weight	Cost Per Unit for	
	(in lb.)	1 Unit	1,000 Units
DSRC Receiver	0.325	$52.5	$45.5
DSRC Antenna	0.22	7.5	6.5
Electronic Control Unit	0.55	0	0
GPS	0	16.5	14.3
GPS Antenna	0.22	4.5	3.9
Wiring	0	0	0
Displays	0	0	0
Total	1.32	81.00	70.20

a) Installation of aftermarket equipment

We believe that a trained technician is likely to be needed to install aftermarket equipment properly, since, as learned during the Safety Pilot Model Deployment, it is not so easy to determine where to attach antennas on the vehicle to ensure their effectiveness.[323] Typical installation times would depend on the type of aftermarket equipment. For this analysis we estimated one hour for a VAD, one hour and fifteen minutes for a self-contained device, and one hour and 30 minutes for a retrofit device. These time estimates were derived from installation times from the Safety Pilot Model Deployment. We also assume that a dealership would be the typical place where aftermarket devices could be installed. We estimate that the average charged wage rate at a dealership is about $90 per hour;[324] installation costs would likely be different if the devices were installed somewhere else.

b) Summary of aftermarket cost estimates

Table XI-12 presents preliminary consumer costs for Aftermarket in year 1, including both equipment cost and installation costs. The equipment costs will be affected by the learning curve, but installation costs (which are just labor) will not be affected by the learning curve.

[323] Somewhere near the center of the roof, near the center of the vehicle appears to be the ideal location for the antenna to be able to pick up GPS and to talk to each other. The angle of the antenna is also important for receiving and appropriately transmitting information. This becomes difficult to determine when the shape of the roof of each make/model is different.

[324] Based on Service Repair Facility Average Hourly Labor Rates. See www.mechaniconduty.com/MapGraphic_email.pdf (last accessed Jul. 14, 2013). These appear to be repair rates from a 2009 phone survey of rates charged in particular cities, one per state. No national estimate was provided. Thus, this is a rounded number considering that we expect repair rates in rural areas to be less and rates for 2012 to be higher than the survey results.

Table XI-12 Aftermarket Consumer Cost Estimates for Year 1 (2012 dollars)

	Equipment	Installation	Total
Retrofit	252.20	135	387.20
Self-contained	213.20	112.5	325.70
VAD	70.20	90	160.20

3. How the preliminary projected vehicle equipment cost estimates were developed

a) Technology implementation scenarios

As mentioned above, we assume that the costs of the equipment needed to support V2V safety applications will decrease over time due to learning (the ability of manufacturers to realize cost savings due to their experience manufacturing the product). Thus, the costs that were estimated without including learning in the earlier sections will decrease over time if learning is considered. Because the effect that learning has on equipment prices is based on the cumulative production of the system (i.e., the total number of systems that have been produced since the system first became available for sale), we need to know what the projected sales of these systems will be in the future.

For the purposes of this analysis, we examined three scenarios of future V2V technology sales/implementation using MY2020 as the base vehicles that first have the technology. Scenario 1 presents a relatively aggressive technology implementation schedule that includes the installation of aftermarket devices. These aftermarket installations are assumed to be made on the existing relatively recently-sold model year (i.e., MY2015-2021) vehicles, but these aftermarket installations are not applied until year 2022 for a subsequent 5-year time period.

Scenario 2 presents a slower pace of technology implementation than that in Scenario 1. Furthermore, Scenario 2 does not have aftermarket device installation. Scenario 3 presents the slowest implementation and lowest among the three scenarios. Scenario 3 not only does not include the aftermarket device, its implementing rate also reaches only to a maximum of 25 percent as opposed to the 100 percent for Scenarios 1 and 2. These scenarios were all based on the projected future new vehicle sales developed by the agency. The projection starts at approximately 17 million per year in 2020 and increases to 20 million in 2050, remaining flat at the 2050 level thereafter. This projection is based on historic R.L. Polk registration data and vehicle sales from 1973 to 2012 using a linear regression statistical process.

The following summarizes the three scenarios. We note that the dates selected here are simply assumptions made for the convenience of this analysis, and reflect no judgment by the agency on timing or phase-in requirements.

(1) Scenario 1:

- 35 percent -70 percent-100 percent vehicle equipment phase-in starting in MY2020
- 100 percent installation of two safety applications for those with vehicle equipment

- Aftermarket deployment for MY2015-2021 vehicles (applicable vehicles)
    - Starting 2022 and continuing for a total of 5 years
    - 5 percent of applicable vehicles for 2022 and 2023
        - For example, for year 2022, applicable old vehicles include the survived MY2015-2019 vehicles, 65 percent of the survived MY2020 vehicles, and 30 percent of the survived MY2021 vehicles. Five percent of these vehicles would be equipped with an aftermarket device
        - For year 2023, the applicable old vehicles include 95 percent of those applicable old vehicles that were defined for year 2022 and would survive in year 2023.
    - 10 percent of applicable vehicles for 2024-2026
    - The estimated number of aftermarket sales for the 5 implementation years in this scenario are:
        - 4.70 million in MY2022,
        - 4.37 million in MY2023,
        - 8.09 million in MY2024,
        - 7.06 million in MY2025, and
        - 6.11 million in MY2026.
- ASD and VAD are assumed to have an equal penetration rate each year.

(2) Scenario 2

- 35 percent-70 percent-100 percent vehicle equipment phase-in starting in MY2020
- 50 percent installation of two safety applications for MY2020-2022 vehicles that have vehicle equipment, 60 percent for MY2023, 70 percent for MY2024, 80 percent for MY2025, 90 percent for MY2026, 100 percent for MY2027 and later.
- No Aftermarket deployment

(3) Scenario 3

- 5 percent vehicle equipment for MY2020, 15 percent for MY2021, 25 percent for MY2022 and newer vehicles
- 100 percent installation of two safety applications for those vehicles that have vehicle equipment
- No Aftermarket deployment

In order to keep preliminary costs consistently applied, when we summarize costs, aftermarket costs will be applied in the year that the aftermarket equipment is purchased even though it will not line up with the model year. For example, in 2023, we assume that aftermarket equipment will be purchased for a certain percentage of MY2015 through 2021 vehicles. That cost is spent in calendar year 2023, and will look like it is spent on MY2023 vehicles in the summary costs. The preliminary benefits will be applied by model year, since scrappage (i.e., the scrapping of discarded objects) is dependent upon model year, not when aftermarket equipment is purchased. This has a very small impact on overall costs by model year and only affects Scenario 1.

Table XI-13 below shows the number of sales of V2V equipment in new vehicles by model year (starting in 2020) for the three scenarios. As described earlier, Scenarios 1 and 3 assumed that the V2V equipment would already have the IMA and LTA applications. Scenario 2 has a separate rate for V2V equipment and applications.

Table XI-13 V2V Technology Sales Assumptions in New Vehicles (Millions of Vehicle)

Year	Model Year	Scenario 1*	Scenario 2 Equipment	Scenario 2 Applications	Scenario 3*
1	2020	5.96	5.96	2.98	0.85
2	2021	11.94	11.94	5.97	2.56
3	2022	17.21	17.21	8.61	4.30
4	2023	17.32	17.32	10.39	4.33
5	2024	17.41	17.41	12.19	4.35
6	2025	17.56	17.56	14.05	4.39
7	2026	17.65	17.65	15.89	4.41
8	2027	17.78	17.78	17.78	4.45
9	2028	17.94	17.94	17.94	4.49
10	2029	18.05	18.05	18.05	4.51
11	2030	18.22	18.22	18.22	4.56
12	2031	18.37	18.37	18.37	4.59
13	2032	18.50	18.50	18.50	4.63
14	2033	18.61	18.61	18.61	4.65
15	2034	18.79	18.79	18.79	4.70
16	2035	18.97	18.97	18.97	4.74
17	2036	19.14	19.14	19.14	4.79
18	2037	19.31	19.31	19.31	4.83
19	2038	19.47	19.47	19.47	4.87
20	2039	19.66	19.66	19.66	4.92
21	2040	19.88	19.88	19.88	4.97
22	2041	20.17	20.17	20.17	5.04
23	2042	19.51	19.51	19.51	4.88
24	2043	19.62	19.62	19.62	4.91
25	2044	19.72	19.72	19.72	4.93
26	2045	19.83	19.83	19.83	4.96
27	2046	19.94	19.94	19.94	4.99
28	2047	20.05	20.05	20.05	5.01
29	2048	20.16	20.16	20.16	5.04
30	2049	20.27	20.27	20.27	5.07

31	2050	20.38	20.38	20.38	5.10
32	2051	20.38	20.38	20.38	5.10
33	2052	20.38	20.38	20.38	5.10
34	2053	20.38	20.38	20.38	5.10
35	2054	20.38	20.38	20.38	5.10
36	2055	20.38	20.38	20.38	5.10
37	2056	20.38	20.38	20.38	5.10
38	2057	20.38	20.38	20.38	5.10
39	2058	20.38	20.38	20.38	5.10

*for both equipment and safety applications

b) Learning

As stated earlier, the preliminary cost estimates we listed above for originally-equipped V2V systems and aftermarket systems do not take into account the potential cost savings that manufacturers will realize over time. As we show in the following paragraphs, the effect of learning can lead to a significant reduction in the costs over time. If we use any of the technology sales scenarios described in the previous section (i.e., the differences between them would be slight) and assume that V2V equipment production begins in 2020 with a price of $329, the costs can range from $249 to $273 in 2022, and $185 to $199 in 2058. The estimated effect of learning to prices for aftermarket devices would decrease by 12 percent in 5 years, from $387 to $341 for a retrofit device, $326 to $287 for the self-contained device, and $160 to $141 for a VAD.

D. Projected fuel economy impact – fuel costs for increased weight

In addition to the cost of the equipment itself, the new equipment on vehicles will increase the vehicle weight. Since the increase in weight is relatively small, the increased weight will have only a small impact on the fuel economy of the individual vehicles on which the V2V equipment is installed. Nevertheless, over the lifetime of these vehicles, this impact on fuel economy will create a cost for society. Our preliminary estimates indicate that (depending on the discount rate) the fuel economy impact on passenger cars will be between $9 and $12 over the lifetime of the vehicle. For light trucks, we believe the impact will be a cost of $11 to $18 over the lifetime of the vehicle.

The impact of added weight on lifetime fuel economy is a function of mileage, survival probability (i.e., the percentage of the vehicle fleet that will not be scrapped due to an accident), the price of gasoline, the change in vehicle fuel economy due to the added weight, and the discount rate chosen to express lifetime impacts in their present value. A sample calculation for passenger cars is:

Equation XI-1 Projected Fuel Economy Impact Calculation

$$\sum_{n=1}^{37}[(V_n * S_n)/(w/(w+1))^{.8} * fe * .80 - (V_n * S_n)/fe * .80]p_n * d_n$$

Where:

n = Year

V = Vehicle miles traveled

S = Survival probability

w = Baseline vehicle weight

i = Incremental weight from adding V2V – 3.45 pounds

fe = Baseline EPA fuel economy

.80 = Factor to derive on-road fuel economy from EPA fuel economy

p = Fuel price

d = Mid-year discount factor

Each of the aforementioned variables is determined by different sources.

1. Fuel price and estimated miles per gallon

The projected price of gasoline was taken from the Energy Information Administration Annual Energy Outlook 2013 early release. This source enables us to project the likely price of fuel between now and 2057. In our cost estimates, fuel taxes are excluded since these are a transfer payment and not a cost to society. Gasoline prices and baseline fuel economy levels are projected to increase steadily throughout the time period, which means that the impact of the additional weight due to installation of V2V systems will change with every model year.

However, unlike with fuel prices, we do not have baseline fuel economy estimates past 2025. Thus, estimates of the impact on fuel prices over the lifetime of the model year were examined for 2020 and 2025. For years beyond 2025, we assume that vehicles will have the same baseline fuel economy and weight as the vehicles from MY2025. The baseline miles per gallon figures for passenger cars and for light trucks are shown in Table XI-14. These estimates reflect a weighted average based on standards in effect for those years.

Table XI-14 Estimated Miles per Gallon (MPG) Values

2020	Passenger Cars	Light Trucks
Baseline mpg on EPA test	45.1	32.8
Baseline weight (lb.)	3240	4397
2025		
Baseline mpg on EPA test	52.1	37.6
Baseline weight (lb.)	3240	4397

2. Vehicle miles traveled and survivability

NHTSA uses VMT by age of vehicle and survivability tables to model the retirement of older vehicles as time passes and to estimate the impact of fuel economy changes over the lifetime of a model year. Both VMT and survivability data differ between passenger cars and light trucks.[325]

3. Incremental weight from V2V equipment

In addition to receiving preliminary information on the vehicle equipment costs (as discussed above) from the confidential business information submissions by suppliers, we also received information on how much the V2V equipment is likely to weigh. As discussed in Table XI-3, above, the V2V equipment is likely to weigh approximately 3.23 pounds. In addition (as shown in Table XI-15), we estimate that the warning display components and installation materials will weigh approximately 0. 36 (= 0.26 + 0.1) pounds. Thus, our current estimate is that the V2V equipment necessary to support the V2V safety applications will increase the vehicle weight by 3.59 pounds. Taking into account the reduction of GPS, the net increase in weight is estimated to be 3.45 pounds. The increased weight is the same for both passenger cars and light trucks.

[325] The survival rates (see Table A-6) were derived using the 1997-2010 R.L. Polk, National Vehicle Population Profile (NVPP). The methodology for deriving these survival rates was published in NHTSA's technical report "Vehicle Survival and Travel Mileage Schedules," Office of Regulatory Analysis and Evaluation, NCSA, Jan. 2006 (Docket No. NHTSA-2005-22223-2218). See www.regulations.gov/#!documentDetail;D=NHTSA-2005-22223-2218 (last accessed Jan. 29, 2014). Polk's NVPP is an annual census of passenger cars and light trucks registered for on-road operation in the United States as of Jul 1 each year. Survival rates were averaged for each vehicle age and up to 30 years. A polynomial model was fitted to these data using regression analysis to establish the relationships between age and the proportion of cars or light trucks surviving to that age.

For vehicle miles traveled, data from the 2009 National Household Travel Survey (NHTS) was used for this analysis. Approximately 300,000 vehicles were included in the 2009 NHTS to estimate the average number of miles driven by household vehicles at each vehicle age. An earlier survey, 2001 NHTS, was used in the 2006 NCSA technical report cited above.

Table XI-15 Summary of Incremental Vehicle Weight Due to V2V Equipment

Category	Weight
V2V Equipment Weight	3.23 lb.
Warning Display Weight	0.26 lb.
Installation Materials	0.10 lb.
Minus Current GPS Installation	-0.14 lb.
Total Incremental Weight	3.45 lb.

4. Summary of fuel economy impact

Based on all the above information (i.e., on vehicle miles traveled, survivability, projected fuel prices, projected fuel economy, and estimated increased weight), we believe that the impact on fuel economy will be as follows. For MY2020 passenger cars, we estimate that there will be a $12 increase in fuel used over the lifetime of the vehicle at the 3 percent discount rate, and $9 at the 7 percent discount rate. For MY2020 light trucks, we estimate that there will be an $18 increase in fuel used over the lifetime of the vehicle at the 3 percent discount rate, and $11 at the 7 percent discount rate. See Table XI-16, below.[326]

Table XI-16 Impact of weight increase on fuel economy over the lifetime of the model year vehicle (per vehicle cost for 3.45 lb. increase)

MY2020	**Passenger Cars**	**Light Trucks**
3% Discount Rate	$12.38	$18.56
7% Discount rate	$9.51	$11.90
MY2025		
3% Discount Rate	$11.76	$17.70
7% Discount rate	$9.04	$11.36

It appears that the improvement in fuel economy from 2020 to 2025 results in a decrease in the fuel costs, even though there is an increase in the price of fuel during the time period. While we do not have estimates of fuel economy levels or average baseline weights of vehicles in the fleet past MY2025, we will assume that the impact of the weight increase on fuel economy will stay relatively constant over the time frame.

E. Preliminary system communication costs

The DOT's Intelligent Transportation Systems Joint Program Office contracted Booz Allen Hamilton to perform a cost estimate for the communication costs. BAH provided the

[326] We have not calculated any improvements to fuel economy that may result from potential V2V and V2I applications. As briefly discussed in Section II.B.5, however, the agency expects there will be V2I mobility applications that provide fuel economy benefits. These benefits would be likely to significantly exceed these costs.

following report: "Communications Data Delivery System Analysis for Connected Vehicles: Revision and Update to Modeling of Promising Network Options."[327] In addition, BAH provided a Microsoft Excel file, titled "Cost Model for Communications Data Delivery System (CDDS)," that lays out the cost estimates (based on preliminary information) in a spreadsheet format, which allowed NHTSA to make changes to assumptions as needed and calculate costs accordingly.[328] This report takes the BAH technical report and focuses on the cases we feel are most reasonable, and presents them in a more plain language format. The next several paragraphs lay out the assumptions behind these estimates.

When a V2V-equipped vehicle is on the road, it will give a computerized message stating, "I am here, this is how fast I'm going, and so on . . . *You can trust me*." That last part of the message, where the vehicle says "*You can trust me*," is important. At the same time, the other vehicle's V2V system will be listening for the message, and it needs to know that the message is from a good source. In order to meet the agency's security needs, BAH assumed that PKI will be used.

As part of PKI, each vehicle is given a set of digital certificates, and the certificates broadcast by the device are assumed not to contain codes that could uniquely identify a vehicle like a license plate would. These anonymous certificates were assumed to last for only 5 minutes, so even if someone wanted to track a device by its certificate with sophisticated and expensive equipment, it would be even more difficult to do so for longer than 5 minutes, when the vehicle starts using a completely different certificate. This makes the system harder to break into and makes it very hard to track vehicles.

Also, under the current security model,[329] every vehicle's V2V system would keep a list of "misbehaving" certificates that it encounters. While the approach to misbehavior has not been decided, one method could be that any time bad V2V information is sent, due to an error or due to intentional human tampering, the certificate tied to that bad V2V data would be recorded and later uploaded when the vehicle transmits data to the SCMS. This way, the SCMS that handles the certificate knows which vehicle is misbehaving, and is able to put together a list of all the certificates that vehicle currently has available. Then, when vehicles connect to the system, they will be warned about these misbehaving vehicles with a list of certificates to avoid trusting. That list is called the Certificate Revocation List.

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

[328] *Cost Model for Communications Data Delivery System (CDDS)* (Excel File) at Docket No. NHTSA-2014-0022.

[329] As discussed in Section IX, NHTSA plans to continue researching security options, including those that may be significantly less costly due to decreased reliance on burdensome distribution of CRLs.

Assuming a PKI system is used and based on the preliminary security system design used in this report, communications between the OBE and to the SCMS or “phone home” include the following activities.

- UPLOAD - a request for new certificates
- DOWNLOAD - new certificates
- UPLOAD - a misbehavior report
- DOWNLOAD – a full/partial CRL
- and conduct other data functions or system updates

The next several paragraphs detail the cost factors for these communication activities.

1. Certificate revocation list

The CRL is a list created by the SCMS that identifies vehicles that are sending out messages that are misbehaving. These vehicles could be sending out messages that erroneously alert drivers of other vehicles, either intentionally or from misbehaving sensors. BAH has outlined several ways by which vehicles may be added to the CRL, as presented below.[330]

- Administrative revocation, which would be based on a pre-determined set of criteria, not based on actual misbehavior. For example, vehicles that are formally retired, or otherwise determined to be removed from the system for non-misbehaving reasons, could make up entries on the CRL.
- Vehicles that observe other vehicles distributing obviously erroneous messages report those vehicles. These observations would be based on plausibility checks that would verify if the message content made physical sense.
- All vehicles report any received message that results in a positive application action (i.e., any message that provides an alert to the driver and a commensurate action). For example, if an in-vehicle application issued a warning to the driver based on a received message, that message would be sent to the Misbehavior Authority (MA). This approach would identify as misbehaving vehicles that were emitting messages that passed plausibility checks but were potentially erroneous to the extent that they were causing a large number of warnings.
- Vehicles randomly select received messages to send to the MA, and the MA would seek to identify trends and patterns from the randomly sampled messages.[331]

[330] BAH CDDS Final Report at 47 at Docket No. NHTSA-2014-0022

[331] Unless the sampling rate is high, the overall effectiveness of this approach is uncertain. If the misbehavior rate is 1% (maximum assumed level), and the sample rate is 1%, the n this approach will, on average, detect 0.01% of the misbehaving vehicles, assuming the detection process is 100 percent effective. If the sample rate is higher, the n the sampling process will represent a greater data load than the CRL.

- It is also possible that a vehicle could self-report if it determines that it is not operating properly, and this might also result in a revocation.

BAH has outlined several problems that could arise as a result of misbehaving messages. If a message is received from a vehicle that is on the CRL, that message is ignored. However, if it is not on the CRL, the message would need to be checked for misbehavior. BAH has outlined the responses to these scenarios.[332]

- The result of receiving a message from a legitimate, non-misbehaving vehicle will depend on the vehicle situation.
  - If the data in the message indicates a danger, then the vehicle warning system will take positive action (warn the driver).
  - If the data in the message indicates no danger, then the system will take no action (no warning will be issued).
- The result of receiving a message from a misbehaving vehicle that is not on the CRL and which passes the plausibility tests will also depend on the vehicle situation.
  - If the data in the message indicates a danger, then the system will take positive action (warn the driver).
  - If the data in the message indicates no danger, then the system will take no action (no warning will be issued).

Attacks on the CRL have been considered by BAH. The BAH CDDS final report recognizes four types of attackers.[333]

- A1 (Clever Outsider): A talented engineer and/or cryptographer who does not possess any inside knowledge.
- A2 (Knowledgeable Insider): An insider who possesses detailed knowledge about the system (security and non-security related) and has access to its specifications.
- A3 (Funded Organizations): An organization that has access to substantial resources and furthermore possesses the capabilities of attacker A2.
- A4 (Certificate Authority insider): An insider who possesses detailed knowledge about the system and has access to confidential information at the CA level. A4 is an insider at the CA and as such compromises the root of trust of the V2V communication system.
  - Because it is the CA's responsibility to guard against such an attacker, A4 is considered out of scope.

[332] BAH CDDS Final Report at 49 at Docket No. NHTSA-2014-0022
[333] BAH CDDS Final Report, at 51 at Docket No. NHTSA-2014-0022

Finally, BAH referenced a DOT report that identified two primary security risks:[334]

- **Attacks on the user/risks to safety and user acceptance:** these attacks are aimed at users and directly impact user safety and indirectly impact system acceptance.
- **Attacks on the communications system/risks to privacy:** these attacks could either (1) track the location and driving routes of a person; (2) cause the a vehicle to be falsely reported for misbehavior, causing a valid driver to be removed from the system.

Other types of attacks, such as cyber-attacks across the entire vehicle fleet, have been considered but not yet addressed. These attacks will be addressed at a later date.

For the Communications Data Delivery System (CDDS), CAMP and BAH have made several considerations regarding design and implementation. CAMP has considered a two-phased deployment strategy, with the first phase being "initial deployment" and the second phase being "full deployment." Initial deployment refers to the first three years of SCMS implementation. The key distinction between the two phases is that in the initial deployment stage, "communications between devices and SCMS will not be generally available…" [335] because the communication network will not be established.

Initial deployment is assumed to last for three years, and requires that OBEs on newly manufactured vehicles download a three-year batch of certificates. These batches would include reusable, overlapping five-minute certificates valid for one week. The term "overlapping" in this context refers to the fact that any certificate can be used at any time during the validity period. The batches would be good for one week and at this point are assumed to be around 20 certificates per week, which equates to 1,040 for one year of certificates. As the frequency of the certificate download batch changes for full deployment, the number and therefore size of the certificate batches also changes accordingly.[336]

Certificate Updates – the download frequency of certificates at full deployment has yet to be determined. However, BAH did consider download size. For option 1, the largest download would be 3,000 certificates (for any frequency of downloads), and the largest download for

[334] *An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues* (FHWA, Nov. 2011) at http://ntl.bts.gov/lib/43000/43500/43513/FHWA-JPO-11-130_FINAL_Comm_Security_Approach_11_07_11.pdf (last accessed Jan. 29, 2014).
[335] BAH CDDS Final Report, at 22 at Docket No. NHTSA-2014-0022.
[336] BAH CDDS Final Report at 15 at Docket No. NHTSA-2014-0022.

option 2 would be 6,000 certificates (with a three-year download). BAH also considered 2-year downloads.

Misbehavior Detection – the BAH preliminary cost analysis assumed that the device would perform a plausibility check on incoming messages. If the message is deemed implausible, the device would report it as misbehaving. This report would then be checked by the Misbehavior Authority of the SCMS, which would revoke the misbehaving vehicle's certificates if the report was deemed to be accurate.

Certificate Revocation and Certificate Revocation List – the revocation process has not yet been finalized. The BAH analysis assumed that any devices that are misbehaving would be added to the CRL, which would be sent to the OBE at regular intervals. After certificates expire, they would be removed from the CRL.

Internal Blacklist – This would be used by the SCMS to make sure that an OBE asking for new certificates is not on the revoked list. If a vehicle or device is on the list, no certificate updates will be issued.

2. Alternative communication systems

Two definitions are needed to prevent confusion among terms:

- Roadside Equipment (RSE) – refers to communication equipment on the side of the road designed to receive and send communications between vehicles and the SCMS regarding certificates, CRL, etc.
- Infrastructure Equipment (I) – refers to equipment on curves or at intersections designed to communicate information about the road or whether a light is green or red, etc. to a vehicle.

For system design specifications, BAH considered three network protocols, cellular, hybrid, and DSRC for the CDDS. The three protocols are based on different combinations of network technology that may be used by the CDDS.

- **Cellular.** This protocol would use an almost-all cellular network for the communications between the SCMS and the OBE on the vehicle. BAH also included an option to use satellite communication for a way to distribute the CRL. However, satellite communication is even more expensive than cellular, and was not considered further. BAH also noted that this protocol does not use RSE. It uses DSRC for V2I (if the infrastructure already has the DSRC antenna in it) and V2V safety communications.
- **Cellular/Wi-Fi/DSRC - Hybrid.** The second protocol would use combinations of more technologies – OBE, RSE, cellular, and satellite. DSRC and Wi-Fi would be

used when beneficial, while cellular technology would be the most used. It also uses DSRC for V2V and V2I communications.

- **DSRC.** The third protocol would use no cellular technology, and uses DSRC for V2V communications and for OBE to SCMS communications through RSE.

BAH concluded that both the cellular and hybrid protocols, the latter of which included cellular as an option, would not meet the recommend security level for the purposes of the study. Additionally, it was determined that any estimated costs to bring these two options to the required security requirements were not considered. More discussion on the estimated costs for the three network protocols is addressed later in this section.

3. System requirements/network options

This section will discuss in more detail the technology considered and the requirements that BAH assumed the system must meet. As previously mentioned, the BAH research considered three protocols for the CDDS. While the cellular and hybrid protocols were deemed not to meet the security requirements necessary for the system, this section will still discuss cellular, Wi-Fi, satellite, and DSRC technologies.

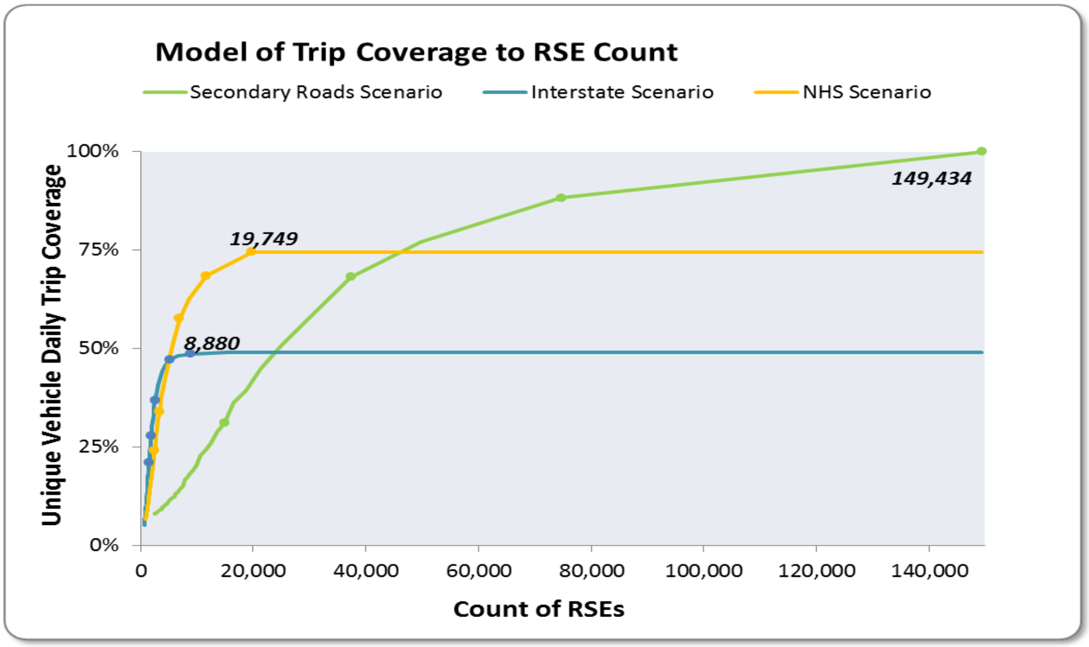
DSRC is a technology that provides local, low latency network connectivity. It allows nearly instant network connections and broadcast messaging that requires no network connection. BAH stated in its report that DSRC cannot support a full CRL update (assuming a large fleet of vehicles with a misbehavior rate of 0.1 percent) if the vehicle passes an RSE at more than a few miles per hour. In order for a vehicle to receive a full CRL update, it must therefore pass by more than one RSE per day, and any update process would have to support incremental updates. BAH suggested that a typical system would require 40 seconds to complete a full CRL update, and a vehicle would only be in the footprint for 14 seconds in the absence of congestion. However, the DSRC technology would be able to support incremental updates.

Of course, any DSRC protocol requires RSE to connect to. In order to determine how many RSE would appear to be optimal for DSRC communications, BAH considered three types of deployment options for "CRL" and "no CRL" scenarios. Deployment of RSEs was considered on three different types of roads: secondary roads, interstate highways, and National Highway System roads. Each type is defined by BAH as the following:[337] Secondary roads refer to collector roads, State highways, and county highways that connect smaller towns, subdivisions, and neighborhoods. Interstate highways are the network of freeways that make up Dwight D. Eisenhower National System of Interstate and Defense Highways. The NHS roads are the collection of interstate highways, principal arteries, strategic highways, major network connectors, and intermodal connectors. The usage of NHS roads (with 19,749 sites) was deemed

[337] BAH CDDS Final Report, at 27. See Docket No. NHTSA-2014-0022.

the most logical because it achieves greater coverage than the interstate option (with 8,880 sites) while also requiring fewer RSE than secondary roads (with 149,434 sites) to achieve the same coverage, as shown below in Figure XI-1.

Figure XI-1 Coverage of RSE by Road Type



BAH used spatial optimization and information from the 2009 National Household Transportation Survey (NHTS) to estimate the required number of RSE to achieve the desired amount of coverage. As shown, NHS roads are the most realistic scenario, though secondary roads could achieve more coverage given more resources. Ultimately, the NHS road deployment method was deemed to be the most realistic.

Cellular technology was also considered for the CDDS system. Cellular systems are very common throughout the nation and are continuing to expand. In particular, the advancement of LTE (long-term evolution) technology is helping to deliver larger amounts of data to cellular users more quickly. However, BAH stated that this is less effective when a user is moving, and that the data rate for LTE is often much lower than what is theoretically possible. Although LTE would be able to support the full download of CRL due to the expansiveness of cellular networks, there are areas where cellular networks are not available, and coverage can experience dead spots at times. Another issue that may arise is the fact that any LTE system may suffer from capacity issues in any area that has many LTE users. Though cellular could potentially be a viable option for coverage, the BAH research concluded that cost and security issues make it an unrealistic option for the CDDS.

Wi-Fi technology supports wireless connectivity and generally higher data rates. The main drawback of Wi-Fi is its design for stationary terminals. Though Wi-Fi offers higher data rates than other options, it does not work nearly as well with moving terminals. In addition, any vehicle that enters the Wi-Fi hotspot must give its MAC (media access control) address and obtain the MAC address of all other vehicles in the hotspot before it can send communications. Though it uses the same basic radio system as DSRC, DSRC eliminates the need for users to gather MAC addresses before communication. In general, this means that Wi-Fi cannot support data exchanges with vehicles moving at road speeds. The costs and security risks associated with cellular also apply to Wi-Fi.

Satellite radio, or Satellite Digital Audio Radio Service (SDARS), uses satellites to provide digital data broadcast service. SiriusXM claims the following coverage capability.[338]

- 3,717,792 mi^2 (9,629,044 km^2) of "seamless" nationwide coverage (approximately 98% of the U. S. land mass)
- 200 miles (322 km) off-shore coverage
- Comparison with terrestrial radio coverage of 50-100 miles (80-160 km)

However, BAH suggested that SDARS could not support the download of a full CRL because the download time would be longer than the average trip. If an incremental system is used, however, it could support updates. The costs and security risks associated with cellular also apply to satellite.

BAH considered misbehavior rates at three levels: 1 percent, 0.5 percent, and 0.1 percent. There is no way to accurately predict the misbehavior rate. The capabilities of the system to deliver the required amount of data to vehicles on a daily basis can be influenced by a change in the misbehavior rate and its influence on the size of the CRL. In a heavy data-requirement scenario (1 percent annual revocation rate, 3 year certificate lifetime, CRL updated daily), the BAH analysis estimated that the system would need to be able to deliver 150 MB of data to each vehicle every day. This could lead to a significant difference in costs if using commercial services such as cellular instead of DSRC. Because of the potential of significant cost increases due to data volume, BAH considered three ways to reduce CRL distribution communication load.

1. Balance certificate lifetime with CRL size. When certificates expire, there is no need for them to be retained on the CRL. As a result, reducing the lifespan of certificates would also reduce the size of the CRL.

[338] SiriusXM Web site. See www.siriusxm.com/whatissiriusxm (last accessed Jan. 29, 2014).

2. Eliminate redundancy in the distributed CRL. If a vehicle can observe and report its own misbehavior, it would be able to stop transmitting messages and would be ignored by other vehicles without needing to check the CRL.
3. Incremental CRL updates. Theoretically, a vehicle would only need to download the changes to the CRL since its last update, rather than the entire CRL each time. A vehicle driven every day would only have to receive a single day's worth of updates. However, if a car has not been driven in a longer period of time, the update will be larger, and will be susceptible to receiving bad messages until it is fully updated, though the small size of the updates would likely mean that these vehicles could be updated quickly.

a) Transmission method

There are many communication systems that could be used to update the on-board equipment on a vehicle. This includes using DSRC, Wi-Fi, satellite, and cellular. Each one requires its own special antennae on the OBE in order to work.

By using the RSE, small base stations could be set up that would allow the vehicles to "phone home" using DSRC, but in order to make sure that the V2V system can constantly be listening for safety component update related communications, a separate DSRC antenna will be used exclusively for communicating updates. We also assume a separate DSRC and antennae will be used for communication when vehicle talk to other vehicles and send the basic safety message.

An alternative would be to install a Wi-Fi, cell, or satellite receiver that does the communication part of the work. In this case, the major factors that affect the cost are the capital needed up front to install the RSE, and the continuing fixed costs to make sure that they are running correctly.

b) Cost model

The cost model has to take into account a lot of choices based on preliminary information on how the V2V equipment can update itself, what needs to be updated, and how often it needs to update itself. BAH has developed a cost model that relies on a set of assumptions to estimate costs for 40 years. Unless otherwise stated, all cost calculations have been made with the assumptions from Table XI-17.

Table XI-17 Cost Assumptions

Component	Current Assumption Choice
OBE Deployment Scenario	Technology Sales Scenario 1
Discount Rate	0%
Certificate Option	Option 2
Certificate Phase-In Period	3 years
CRL Type	Full CRL
Misbehavior Rate	0.10%
Cellular Data Price	$4.00/GB
Cellular Component Cost on the Vehicle	$10.00
Fraction of Data Shifted from Cellular in Hybrid	67%
RSE Phase-In Period (Years)	15 years
# Nationwide RSEs	19,750
RSE Replacement Cost	$22,719
RSE Life	15 years

Below, the preliminary costs of each protocol are broken down. For cellular and hybrid we include the cost of OBE to allow the system to receive and transmit either through cellular or Wi-Fi. For the DSRC option the cost of OBE (DSRC) has already been accounted for in a previous cost section.

The costs of an OBE for cellular are estimated at $10, the cost for Wi-Fi is estimated at $2 per vehicle, and the OBE costs for a satellite system are estimated at $20. The total OBE costs for cellular are $10 per vehicle, and for hybrid are $12 to cover both cellular and Wi-Fi.

Table XI-18 OBE Subcomponent Cost Estimate

		Included in:		
OBE Subcomponents	**Cost**	**Cellular**	**Hybrid**	**DSRC**
Cellular	$10	1	1	
Wi-Fi	$2		1	
Satellite	$20	0	0	0
	Total Cost	$10.00	$12.00	$0.00

c) Cellular

Using cellular technology for the CDDS yields two primary cost drivers. The first is an estimated $10 per vehicle for cellular capability to be added to new vehicles and the second is the communication cost for cellular data. At $4.00/gigabyte,[339] data prices for cellular based system such as the CDDS end up being very high. Table XI-19 below shows total estimated costs for using a cellular protocol.

Table XI-19 Total Estimated Costs - Cellular

Cellular Costs	Year 1	Year 10	Year 20	Year 30	Year 40
RSE	$0	$0	$0	$0	$0
OBE	$171,592,000	$214,975,560	$250,550,574	$263,808,243	$269,308,171
Cellular Data	$0	$444,704,378	$1,088,849,075	$1,398,075,958	$1,607,213,512
Satellite	$0	$0	$0	$0	$0
Total	$171,592,000	$659,679,938	$1,339,399,649	$1,661,884,202	$1,876,521,682

d) Hybrid

The hybrid protocol uses both cellular technology and opportunistic use of Wi-Fi networks. The estimated data costs using this protocol are lower for cellular, but total estimated costs still remain high, as shown in Table XI-20.

Table XI-20 Total Estimated Costs - Hybrid

Hybrid Costs	Year 1	Year 10	Year 20	Year 30	Year 40
RSE	$0	$0	$0	$0	$0
OBE	$205,910,400	$257,970,671	$300,660,689	$316,569,892	$323,169,805
Cellular Data	$0	$148,234,793	$362,949,692	$466,025,319	$535,737,837
Satellite	$0	$0	$0	$0	$0
Total	$205,910,400	$406,205,464	$663,610,380	$782,595,212	$858,907,642

As indicated in the table, the estimated cellular communication costs are lower for this protocol than a pure cellular protocol, but the OBE costs are higher due to the increased per-OBE cost which would need to contain Wi-Fi capability. For the cellular approach, each OBE is estimated to cost $10, but in the hybrid approach, each OBE is estimated at $12. The hybrid approach offers an interesting alternative to the pure cellular approach, but total costs remain high. As a result, it is a less attractive option than DSRC.

[339] BAH CDDS Final Report, Table 37 at 86 at Docket No. NHTSA-2014-0022

e) DSRC

DSRC communications are allowed by the installation of RSEs on highways. The DSRC protocol option has total estimated costs that are much lower than the other two protocol designs, as shown in Table XI-21.

Table XI-21 Total Estimated Costs – DSRC

DSRC Costs	Year 1	Year 10	Year 20	Year 30	Year 40
RSE	$0	$135,137,904	$177,681,184	$177,681,184	$177,681,184
OBE	$0	$0	$0	$0	$0
Cellular Data	$0	$0	$0	$0	$0
Satellite	$0	$0	$0	$0	$0
Total	$0	$135,137,904	$177,681,184	$177,681,184	$177,681,184

The only cost driver for using the DSRC protocol is the installation of RSEs on highways. There is no usage of cellular, Wi-Fi, or satellite data, and as a result costs are much lower. RSE costs are broken down below in Table XI-22. There are three costs relating to RSEs. The initial installation cost is estimated at $8,839 per site. It is assumed that each site would have to be replaced 15 years later, and there is an annual recurring maintenance cost of $7,482 per site.

At this point, we assumed that RSEs will get a linear phase-in over 15 years. For the first three years, there will be no RSE installations. We assume that the initial vehicles will be sold with 3 years of certificates and they will not need updates until the end of year 3. In addition, there will be so few vehicles on the road with DSRC that a CRL will not be particularly valuable, and there will be little need to communicate a CRL. The work is therefore divided into 15 parts. For the first three years, no RSE will be installed; during year four, 4/15ths of the RSEs will be installed; and 1/15 of the RSEs will be installed every year after that, until by year 15, all RSEs in the design will be installed. Assuming full deployment, the estimated number of necessary RSEs would be 19,750. That number of RSEs would be able to cover 74 percent of the nation's population every day.

Table XI-22 Road Side Equipment Cost Estimates

Average Costs per RSE	Cost
Average One-Time Cost	$8,839
Average Regular Replacement Cost	$22,719
Average Annually Recurring Cost	$7,482

If we examine just the likely communication costs on a per-vehicle basis, the cellular communication costs grow significantly over time as the number of vehicles that must be communicated with grows. Costs per vehicle are shown in Table XI-23.

Table XI-23 Communication Data Cost Estimate per Vehicle

Cellular Data Cost per Vehicle	Year 10	Year 20	Year 30	Year 40
Cellular	$2.58	$4.04	$4.57	$4.90
Hybrid	$0.86	$1.35	$1.52	$1.63
DSRC	$0.00	$0.00	$0.00	$0.00

The RSE per vehicle costs in each technology sales scenario were calculated in Table XIII-1 in Appendix A. It is assumed that these costs would be paid for at the time the vehicle is purchased or at the time the aftermarket equipment was purchased. Because 4/15ths of the RSEs are assumed to be installed in year 4 and RSEs would be replaced every 15 years, the replacement costs are higher in year 19 and year 34. Total costs increase over time for a number of years because more RSEs are working and they encounter maintenance costs.

Table XI-24 provides the total preliminary costs for each communication protocol. As indicated in the table, the costs using the DSRC protocol are considerably lower than costs under the other two protocols. Furthermore, DSRC communication is believed to meet security requirements, thus it becomes a realistic choice for CDDS.

Table XI-24 Total Communication Cost Estimates per Year by Scenario

	Cellular	Hybrid	DSRC
Year 1	$172 M	$206 M	$0 M
Year 2	$218 M	$262 M	$0 M
Year 3	$221 M	$265 M	$0 M
Year 4	$316 M	$332 M	$186 M
Year 5	$366 M	$346 M	$86 M
Year 6	$430 M	$365 M	$96 M
Year 7	$453 M	$326 M	$106 M
Year 8	$518 M	$352 M	$115 M
Year 9	$587 M	$379 M	$125 M
Year 10	$660 M	$406 M	$135 M
Year 11	$735 M	$435 M	$145 M
Year 12	$811 M	$464 M	$155 M
Year 13	$886 M	$492 M	$165 M
Year 14	$959 M	$519 M	$175 M
Year 15	$1,031 M	$546 M	$184 M
Year 16	$1,100 M	$573 M	$169 M
Year 17	$1,166 M	$598 M	$148 M
Year 18	$1,228 M	$621 M	$148 M
Year 19	$1,286 M	$643 M	$252 M
Year 20	$1,339 M	$664 M	$178 M
Year 21	$1,390 M	$683 M	$178 M
Year 22	$1,439 M	$703 M	$178 M
Year 23	$1,468 M	$708 M	$178 M
Year 24	$1,502 M	$721 M	$178 M
Year 25	$1,533 M	$732 M	$178 M
Year 26	$1,561 M	$744 M	$178 M
Year 27	$1,586 M	$753 M	$178 M
Year 28	$1,612 M	$763 M	$178 M
Year 29	$1,638 M	$773 M	$178 M
Year 30	$1,662 M	$783 M	$178 M
Year 31	$1,684 M	$791 M	$163 M
Year 32	$1,702 M	$798 M	$148 M
Year 33	$1,718 M	$803 M	$148 M
Year 34	$1,734 M	$809 M	$252 M
Year 35	$1,748 M	$814 M	$178 M
Year 36	$1,761 M	$818 M	$178 M
Year 37	$1,772 M	$822 M	$178 M
Year 38	$1,869 M	$856 M	$178 M
Year 39	$1,876 M	$859 M	$178 M
Year 40	$1,877 M	$859 M	$178 M

f) CRL type

BAH found that one input assumption was "highly uncertain and highly impactful on the … cost analysis." That input is the type of Certificate Revocation List. By choosing a different type of CRL update to the V2V device, you can significantly change the cost to keep devices safely updated. The two types of CRL update that BAH considered were "Complete Daily CRL" update and "Incremental Daily CRL" update. For the first option, Complete Daily CRL, the entire list is downloaded to the vehicle every day. In the Incremental Daily CRL, only the *changes made to the list* are downloaded. Thus, somewhere close to only 1/365 (0.27 percent) of the Complete CRL needs to be downloaded daily for the Incremental CRL update. Because the Complete Daily CRL downloads are always much bigger than the Incremental Daily CRL download, the Complete Daily option costs more than the Incremental CRL. Since the Incremental Daily CRL cost would be almost as low as having no CRL at all, rather than speculate on the small increment in cost, the cost estimates presented here include two options: Full CRL and No CRL, describing the extreme cases of how much the CRL will cost. These CRL download costs only apply to cellular and hybrid. We assume that there is no cost for DSRC with RSE because there are no anticipated per transmission costs associated with DSRC communication, as compared to the other communication mediums used in cellular and hybrid.

Total estimated costs per year are further broken down in Table XI-25 below. There are no communication costs in the first three years in the DSRC with RSE option. The cellular and hybrid (cellular and Wi-Fi) options have costs in the first three years due to OBE costs.

Table XI-25 Total Cost Estimates Comparing Full CRL to No CRL in Millions (2012 dollars)

Total costs	Year 1	Year 10	Year 20	Year 30	Year 40
Cellular No CRL	172 M	215 M	251 M	264 M	270 M
Cellular Full CRL	172 M	660 M	1339 M	1662 M	1877 M
Hybrid No CRL	206 M	258 M	301 M	317 M	323 M
Hybrid Full CRL	206 M	406 M	664 M	783 M	859 M
DSRC With RSE No/Full CRL	0 M	135 M	178 M	178 M	178 M

4. Communication costs conclusions

Of the three scenarios considered, the DSRC with RSE ended up being the most economically viable as well as allowing for the most security. While cellular and hybrid show some merits, the costs and security concerns that they hold make them generally less attractive options for the CDDS. The implementation of a DSRC system, however, will take time. A 15 year phase-in plan has been assumed to be necessary for the RSEs, but other options may be considered. In addition, decisions on how to implement ideas such as an incrementally updating CRL must be further analyzed.

F. Security credentials management system cost modeling

Beyond the costs of the vehicle equipment and the fuel economy impact of that equipment (due to increased weight), we need to account for the costs of services that support the V2V system for the vehicle fleet. In addition to the cost of ensuring that the different elements of the V2V system are able to communicate, discussed above, another such cost is for the SCMS. The main function of the SCMS is to ensure that the communications from vehicles to other vehicles are authentic and can be trusted. Additional information on the SCMS is found in Section IX.

1. Preliminary projected costs for SCMS

In estimating the costs for the SCMS, we anticipate that a fee of approximately $3.14 per vehicle could support the SCMS for all three scenarios. This fee would most likely be a one-time fee incorporated into the purchase price of a new vehicle or aftermarket equipment. The fee collected from the new vehicle or aftermarket sales each year would support the operations of the SCMS for that year. The operation of the SCMS in the next year would be supported by the fees collected from the new vehicle or aftermarket sales for that year.

We arrived at the conclusion that a fee of $3.14 per new vehicle sold can support the SCMS by first estimating the costs of the SCMS for each year (beginning in 2020—our tentative first year for implementing the V2V system). This annual cost varies over time (with the first year being the least costly) because additional infrastructure is needed to support an increasing number of vehicles as V2V technology penetrates the fleet. We estimate the cost to support the SCMS ranges from $5 to $36 million in year 2020, whereas we estimate the cost to range from $23 to $93 million in year 2058. However, the currently available information indicates that the average *annual* cost for the SCMS over this span of 39 years (2020 to 2058) is $60 million. We anticipate that this average annual cost could be covered by a $3.14 fee collected along with the purchase of each new vehicle.

In order to understand the costs of the SCMS, we need to first define the components of the SCMS and how they interact with each other. The SCMS is made up of defined "components" that all have specified jobs and contribute to the operation of the SCMS function for V2V, including the components that make up the current system design to enable privacy while meeting system security needs. Details regarding the current system design and its components are found in Section IX.B.

a) Scenarios and assumptions used in developing preliminary projected costs

This analysis of costs is based on the latest SCMS design specifications (current as of January 2014) developed collaboratively with NHTSA and CAMP. These specifications establish parameters that the SCMS would likely need to meet in order to accomplish the aforementioned goals. It is important to note that these specifications are not finalized and could change. The following is a discussion of the assumptions that we are currently using for the purposes of estimating the potential costs of the SCMS.

(1) Technology Sales Scenario Assumptions

For the purposes of calculating the preliminary potential costs of the SCMS in this section, we will be using the same three technology implementation scenarios that we used to calculate Vehicle Equipment Costs, above. As a reminder, the three scenarios all based on a projected vehicle sale that starts at 17.04 million in 2020 and increase to 20.38 million in 2050. The sales stay flat at the 2050 level afterwards. These scenarios are briefly summarized as follows.

- Scenario 1: OBE on new vehicles with 35 percent-70 percent-100 percent phase-in starting in MY2020 with aftermarket devices
- Scenario 2: slower OBE implementation than that specified in Scenario 1, no aftermarket
- Scenario 3: the slowest OBE implementation among the three scenario and the rate would not reach the 100 percent level as did other two scenarios, no aftermarket

(2) Certificate issuance assumptions

For this analysis, we are assuming that a new vehicle will receive a three-year batch of reusable, overlapping five-minute certificates valid for one week.[340] The term "overlapping" in this context refers to the fact that any certificate can be used at any time during the validity period.[341] Key implications of this design are as follows:

- Certificates do not expire unless they are used, or the week ends. They are not time sensitive.
- Depending on the number of certificates designated for one week, they will be reused an uncertain number of times with no predetermined order.
- The certificate batch size may be 3,000, which is based on a set of approximately 20 certificates being used per week. Thus, the 3,000 certificate batch size would cover three years' of use before requiring certificate updates.
- There may be some discretion about how many certificates will be designated for a one-week period. This would be based on the choice of the user, OEMs, or SCMS owners/operators. However, the current assumption is 20 certificates per week.[342]

[340] Security Credentials Management System (SCMS) Design and Analysis for the Connected Vehicle System (Booz Allen Hamilton, Inc., Dec. 2013, at 14). See Docket No. NHTSA-2014-0022

[341] Id.

[342] Id.

Afterwards, each vehicle will receive updates with two years of certificates at two year intervals.

We note that the variable that can cause the largest changes in overall cost is the frequency of certificate downloads. The final decision on this variable has not been made, and costs could change in the future based in large part on this variable.

(3) Hardware/software assumptions

Another important cost driver is the fact that hardware and software need to be refreshed every five years in order to keep the SCMS function equipped with the latest security capabilities. This assumption has been included in the cost estimates, which show an increase in costs every five years.[343]

(4) Location assumption

The estimates are based on Richland, WA, as the baseline for all functions, in order to be consistent with the BAH cost model.[344] BAH identified cost factors for Richland, WA, as well as Denver, CO; Chicago, IL; San Antonio, TX; Washington, DC; and Gastonia, NC. Richland was chosen as a baseline given the spread of costs for the area and used to produce an initial calculation of cost for the purpose of the SCMS cost analysis.

b) Annual total preliminary cost for the SCMS

In order to estimate the cost per new vehicle sold, we first need to estimate the cost of the entire SCMS. This cost is different for each year because the number of vehicles operating with V2V capabilities will increase over time. When the number of these vehicles increases, the SCMS will need to support the functions of the additional vehicles with an increased capacity to be able to generate and issue security certificates. Table XI-26, below, shows the likely cost needed to support each SCMS function. Each column (labeled 0, 10, 20, 30, 40) show the costs for the SCMS function in that year. For example, the PCA will cost $5,541,402 in Year 0 to operate. However, that same function will cost $7,196,135 to operate in Year 10. The last row in Table XI-26 shows the total cost of the entire SCMS in each of those years. All of these costs are undiscounted. The costs in Table XI-26 also assume that vehicles are being sold at the rate described in “Technology Sales Scenario 1.” In other words, we are assuming an increasing sales volume (beginning at 17 million in 2020, and rising to approximately 20 million thereafter starting in 2050).

[343] Id., at 106.

[344] Id.

Table XI-26 Undiscounted Cost Estimates per Component for Selected Years, Scenario 1, Two Year Downloads

Component	Year				
	0	10	20	30	40
PCA	$5,541,402	$7,196,135	$11,948,687	$16,281,686	$20,257,673
RA	$6,671,907	$7,755,342	$13,636,463	$19,206,293	$24,471,619
LA	$4,918,141	$5,644,934	$9,964,652	$14,117,090	$18,048,462
MA	$3,546,999	$3,757,398	$5,514,098	$7,256,497	$8,815,887
LOP	$1,320,948	$1,829,286	$3,434,603	$5,201,161	$6,214,164
ECA	$4,079,230	$4,167,392	$4,167,392	$4,167,392	$4,167,392
Intermediate CA	$4,184,493	$4,024,319	$7,940,176	$11,856,033	$15,689,120
Root CA	$1,609,923	$1,592,732	$1,592,732	$1,592,732	$1,592,732
DCM	$4,061,098	$4,507,122	$4,507,122	$4,507,122	$4,507,122
SCMS Manager	$323,330	$679,564	$679,564	$679,564	$679,564
Total Cost	$36,257,471	$41,154,224	$63,385,488	$84,865,570	$104,443,733

The preliminary costs are generally driven by new hardware, software, facilities, and full time equivalent positions (FTEs). However, the costs do not rise in a linear fashion because new hardware and software is necessary at regular intervals (i.e., every 4 to 5 years). Thus, the costs in the first year and in every fifth year are noticeably higher in the estimates than in other years as a result. In these years, the total costs increase by a fairly significant margin but then decrease again in the next year. However, when we average the costs of the entire SCMS over this 40-year period, the estimated annual cost based on preliminary information for the SCMS is $59 million.

We note that the cost estimates above are subject to change given the uncertainty surrounding the functions of various aspects of the SCMS. The most notable uncertainty is the Misbehavior Authority (MA). As described above, this function is responsible for detecting misbehavior (i.e., systems that are not broadcasting accurate information) and publishing CRLs to notify other participants in the V2V environment that they should not trust the information from those sources. At this point, it is unclear how the SCMS will perform this function. Thus, it is unclear whether the cost estimates for this function are accurate. At the moment, we have based it on estimations of hardware, software, facilities, and employee needs according to current specifications. We intend to update our cost estimates for this function (as well as others) as the details of those functions become more definite in the future.

c) Cost methodology for component functions of the SCMS

In order to arrive at the annual and total preliminary cost estimates for the entire SCMS, we had to examine the costs for each component function of the SCMS. While this report does not present the calculations for each component function, we have selected an illustrative example to communicate the methodology that we used to arrive at the estimates for each component. Table XI-27 below shows the annual cost for the Pseudonym Certificate Authority (PCA) function in each of five different years (2020, 2030, 2040, 2050, and 2060). Table XI-27 also shows the different types of expenditures needed to support the PCA and how each is anticipated to change over time.

Table XI-27 Undiscounted Cost Estimate of PCA for Selected Years, Scenario 1, Two Year Downloads

PCA	Year				
Cost Category	**0**	**10**	**20**	**30**	**40**
Hardware Purchase	$615,472	$1,500,762	$1,968,620	$2,141,499	$2,203,241
Hardware, O&M	$0	$107,850	$179,301	$206,833	$220,324
Software Purchase	$2,311	$7,801	$10,729	$12,642	$12,854
Software, O&M	$0	$905	$1,585	$1,993	$2,314
Facilities: Initial Cost	$1,037,695	$1,620,582	$1,894,360	$2,115,775	$2,115,775
Facilities: Annual	$0	$72,310	$122,241	$145,169	$159,464
FTEs: Total Costs	$3,885,925	$3,885,925	$7,771,850	$11,657,775	$15,543,700
Total Cost	$5,541,402	$7,196,135	$11,948,687	$16,281,686	$20,257,673

2. Funding the SCMS

For such a system, there must be a cost to the user. In the case of the SCMS function, we assume that the user will have to pay a cost for their use of the SCMS system upfront, when a new vehicle is purchased (i.e., the cost of the SCMS becomes part of the new vehicle purchase price). While other payment methods are possible, it seems that including the cost of the SCMS in the price of the new vehicle or the price of aftermarket devices is the easiest way to ensure payment for (and continued participation in) the system. Other payment methods (e.g., monthly fees) may discourage users from participating in the V2V environment. If this happens, the number of on-the-road vehicles that are communicating will be reduced, and the effectiveness of the V2V system will consequently decrease. The agency emphasizes, however, that it will consider this issue further going forward as new information becomes available.

G. Conclusion of preliminary V2V implementation cost estimates

When considering all four parts of this preliminary cost analysis (vehicle equipment, fuel economy impact, SCMS, and communications costs), we estimate that the total costs to the consumer for each new vehicle will be approximately $341 - $350 (across the 3 percent to 7 percent discount rates) in 2020. We note that over time this amount will decrease to approximately $209 - $235 in 2058 (when considering the discount rates and the three sales scenarios), due in large part to cost reductions that manufacturers will realize as they gain more experience manufacturing V2V vehicle equipment (learning). We note the total costs will decrease over time even though certain costs will increase over time. While the SCMS costs will increase over time due to the need to support an increasing number of vehicles, these costs are small in comparison to the vehicle equipment costs. Thus, the effect of manufacturer learning in reducing the costs over time substantially outweighs cost increases such as the SCMS.

Preliminary costs are summarized mainly on a model year basis. For new vehicle sales, costs for the V2V system occur when the vehicle is sold. For fuel economy impacts, costs are discounted back to present value - when the vehicle is sold. For SCMS and communication costs, costs are assumed to be charged when the vehicle is sold to cover these costs that would occur in the same calendar year as the model year when it is sold. Thus, the assumption is that at the time the vehicle is sold, the price of the vehicle is increased to pay for what is needed in that year. The estimated costs per vehicle for the SCMS (ranging from $1 to $6 per vehicle) and communications (ranging from $3 to $13 per vehicle) are relatively low.

For aftermarket sales, costs occur when the aftermarket equipment is sold, which is not the same as the model year of the vehicle for which it has been purchased. Thus, the calendar year of the assumed sale is when aftermarket costs are added to the model year sales to get total costs for the model year. Here again, costs for SCMS and communication could be charged at the point of sale.

Because of the large number of variables affecting the costs of the V2V system, the preliminary total annual costs of the system fluctuates substantially from year to year. The total costs for new vehicles (over three sales scenarios and two discount rates) rise from $0.3 to $2.1 billion dollars in 2020 to $1.1 to $6.4 billion in 2022, before decreasing slowly to a relatively stable level of $1.1 to $4.6 billion.

To put the costs into perspective, we compared the passenger car costs over time in the four cost categories, using the 3 percent discount rate. The OEM costs are 95 percent of total costs initially, then decreasing slowly to 88 percent of total costs as the learning curve takes effect and other costs increase. The fuel costs (at around 5 percent) are typically higher than the communication costs (at around 4 percent) and the SCMS cost stay in the 1 to 2 percent range over the years.

H. Economic practicability

Under the Safety Act, standards set by NHTSA must be practicable. One criteria of a practicable standard is that it is economically feasible (i.e., compliance with the standard is not so burdensome [costly] so as to create a significant harm to a well-established industry). If a standard is deemed to be economically infeasible, it can be considered impracticable by a court. Therefore, the economic feasibility of V2V will need to be considered when deciding whether to mandate V2V. Our analysis is based on the information on potential costs for a V2V system that has been collected so far by the agency, even while recognizing that the information is preliminary and that additional information will come to light as the agency moves forward.

Although no V2V system currently exits other than in prototype form, we have attempted to make a preliminary estimate of costs to implement such a system based on available prototypes and projections about system deployment. Based on those costs, it appears likely that any standards to require elements of the V2V system will be economically practicable. We emphasize that these estimates are subject to substantial amendment as more information is acquired and any plan for implementation gains greater clarity. NHTSA and DOT will be constantly attentive to options that may reduce these costs. More important, these projected costs are best thought of as the price for a new and important element of the nation’s transportation infrastructure and should be considered jointly with the safety and other benefits the system would bring as discussed in the next section.

XII. Preliminary Effectiveness and Benefits Estimates of V2V

A. Analysis of preliminary benefits of V2V technology

The agency estimates the system crash avoidance and crashworthiness effectiveness by comparing crash rates and the injury probabilities of vehicles with and without V2V technology. The agency focused its evaluation on IMA and LTA, the two applications currently considered to be exclusively enabled by V2V technology. To correspond with the cost estimates, benefits were also estimated for the three technology implementation scenarios described in the cost section.

Based on the estimation methodologies described in this section, the agency estimates that IMA would help drivers avoid 41 to 55 percent of target intersection crashes[345] and reduce the severity of intersection crashes by an average of 1.17 mph delta-V.

The agency estimates that LTA would prevent 36 to 62 percent of left turn crashes. LTA is considered to have no impact on mitigating the severity of the left turn crashes that cannot be avoided. Therefore, the crashworthiness effectiveness for LTA is assumed to be zero in this analysis.

We therefore estimate that IMA and LTA together would prevent a maximum of 413,000 to 592,000 crashes, save 777 to 1,083 lives, and reduce 191,000 to 270,000 MAIS injuries under the fast technology implementation plan specified in Scenario 1.

Under Scenario 2, a slower implementation pace than Scenario 1, IMA and LTA would also accrue the maximum benefits as in Scenario 1. The primary difference between these two scenarios is that Scenario 1 would achieve other levels of benefits (e.g., 70 or 90 percent of the maximum benefit) 2 to 3 years earlier than would Scenario 2.

Under Scenario 3, the slowest implementation pace among the three, which only reaches 25 percent of the full implementation level, IMA and LTA would accrue at most 6 percent of the maximum benefits achieved by Scenarios 1 and 2. The disparity in benefits demonstrates that in order to realize the full potential of V2V technology, achieving full implementation over time is critical.

1. Analysis overview

Preliminary cost and benefit estimates vary with the V2V safety device implementation strategy. As stated in the cost section, the agency used three scenarios to examine the variation of

[345] The result of adding 15 – 24 percent for PCP-S and 26 - 31 percent for PCP-M.

the cost and benefit estimates and to understand the impact of various technology implementation schedules on the costs and benefits. The first scenario represents the most aggressive V2V implementation scenario among the three, while the third one represents the slowest and lowest implementation schedule among the three. The detailed description of these implementation scenarios are provided above in Section XI.

As stated earlier, the preliminary benefit estimates are for IMA and LTA only. The agency intends to examine the benefits of other safety applications -- FCW, BSW/LCW, and DNPW – when sufficient data are available to estimate their effectiveness.

The preliminary benefit estimates presented in this report include (1) the maximum undiscounted annual benefits (in terms of fatalities and injuries reduced and crashes avoided) when all passenger vehicles can communicate with each other, and (2) the undiscounted annual benefits for calendar years 2020 to 2058.

The benefits of a V2V safety application depend upon three primary components:

- The target population that would be impacted by the application,
- The system effectiveness of the application in preventing the crash (crash avoidance) and/or mitigating the severity of the crash (crashworthiness), and
- The probability that involved vehicles can communicate with each other (communication probability).

Of these three components, communication probability would vary with the number of V2V-equipped vehicles entering into the market each year. Therefore, at a given year *i* of a V2V implementation, the benefits of an application can be noted as:

Equation XII-1 Benefits Estimation Calculation

$$B_i = TP * E_a * C_i + TP * (1 - E_a) * E_w * C_i$$

Where, B_i = the benefit for year *i*

TP = the target population

E_a = the crash avoidance effectiveness of an application

E_w = the crashworthiness effectiveness of an application

C_i = the communication rate.

The target population (TP) includes crashes, fatalities, injuries, and property damaged only vehicles (PDOV, vehicles that only incur property damage and none of their occupants incur an injury). Effectiveness (E_a and E_w) of a safety system is derived by comparing crash rates and injury rates for vehicle with and without the system. The effectiveness can be represented by the generalized formula:

Equation XII-2 Effectiveness Calculation

$$E=1-\frac{P_{with}}{P_{without}}$$

Where, P_{with} = crash rate (or injury rate for crashworthiness) for vehicle with the system

$P_{without}$ = crash rate (or injury rate for crashworthiness) for vehicles without the system.

For crash avoidance, the effectiveness (E_a) takes into account both the reduction in exposure to conflict and the probability of a crash when a conflict occurs.

The communication rate (C_i) is the probability that two passenger vehicles can communicate with each other, which means that it depends on the number of vehicles that have V2V, and is consequently different depending on the technology implementation scenarios. Besides C_i, the benefit process represented by Equation XII-1 is identical for all implementation scenarios; meaning the other variables in the equation remain the same (e.g., the target population). The next sections discuss in greater detail the implementation scenarios and the three primary factors in determining benefits: target population, and effectiveness, and communication rates.

2. Technology implementation scenarios

Restated here for convenience, following is a basic summary of the three potential technology deployment scenarios used for the cost and benefits analysis in this report. Additional information on these scenarios is found in Section XI.C.3.a). As previously noted, the dates selected here are simply assumptions made for the convenience of this analysis, and reflect no judgment by the agency on timing or phase-in requirements.

a) Scenario 1

- 35 percent-70 percent-100 percent vehicle equipment phase-in starting in MY2020
- 100 percent installation of two safety applications for those with vehicle equipment
- Aftermarket deployment for MY2015-2021 vehicles (applicable vehicles)
    - Starting 2022 and continuing for a total of 5 years
    - 5 percent of applicable vehicles for 2022 and 2023
        - For example, for year 2022, applicable old vehicles include the survived MY2015-2019 vehicles, 65 percent of the survived MY2020 vehicles, and 30 percent of the survived MY2021 vehicles. Five percent of these vehicles would be equipped with an aftermarket device.

        - For year 2023, the applicable old vehicles include 95 percent of those applicable old vehicles that were defined for year 2022 and would survive in year 2023.
    - 10 percent of applicable vehicles for 2024-2026
    - The estimated number of aftermarket sales for the 5 implementation years in this scenario are:
        - 4.70 million in MY2022
        - 4.37 million in MY2023
        - 8.09 million in MY2024
        - 7.06 million in MY2025
        - 6.11 million in MY2026
- ASD and VAD are assumed to have an equal penetration rate each year.

b) Scenario 2

- 35 percent-70 percent-100 percent vehicle equipment phase-in starting in MY2020
- 50 percent installation of two safety applications for MY2020-2022 vehicles that have vehicle equipment, 60 percent for MY2023, 70 percent for MY2024, 80 percent for MY2025, 90 percent for MY2026, 100 percent for MY2027 and later.
- No Aftermarket deployment

c) Scenario 3

- 5 percent vehicle equipment for MY2020, 15 percent for MY2021, 25 percent for MY2022 and newer vehicles
- 100 percent installation of two safety applications for those vehicles that have vehicle equipment
- No Aftermarket deployment

3. Target population for V2V technology

The target population includes crashes, fatalities, injuries, and property-damage-only vehicles (PDOV) that are vehicles that only incur property damage and none of their occupants incur an injury. Although the preliminary benefit estimate is only for the IMA and LTA safety applications, the target population for FCW and LCW and for heavy vehicles is also provided here to offer a comprehensive illustration of the potential safety impact that could result from the V2V-based safety applications.

Overall, the agency used an average of 2010 and 2011 CDS and FARS data to determine that there are approximately 5.37 million police-reported crashes annually in the United States[346] involving approximately 32,683 fatalities and 4.29 million MAIS[347,348] 1-5 injuries. Of these crashes, 3.34 million crashes involving two or three passenger vehicles[349] would be impacted by the V2V-based safety applications. These crashes account for 62.3 percent of the total crashes.

Crashes *not* included in the 3.34 million are (a) 1.5 million single-vehicle crashes and 230,000 crashes that involved motorcycles, since these crashes are not expected to be benefited by V2V-based safety applications, (b) about 60,000 crashes where four or more vehicles were involved as they could involve more complicated and less clear interactions between vehicles and require further evaluation, and (3) about 240,000 crashes where heavy vehicles[350] were involved, because the agency is only evaluating passenger vehicle[351] crashes at this time and plans to address crashes involving heavy vehicles in a later decision. However, the V2V-based applications would affect 3.59 million crashes (66.9% of the total crashes) if heavy-vehicle crashes were included.[352]

To identify the target crash population for a specific V2V-based application, the agency starts with the 37 pre-crash scenarios as described in Section III.A. The target population for an application is categorized into major scenarios where the application might perform differently. The following describes the major scenarios for intersection crashes (affected by IMA and LTA), rear-end crashes (FCW), and lane change/merge crashes (BSW/LCW).

- Intersection crashes for IMA and LTA
  - turn-into path into same direction or opposite direction (i.e., "turn-into path, initial opposite direction" crashes are crashes where one involved vehicle is making a left turn at the intersection and the other vehicle is traveling straight through the intersection from the opposite direction)

[346] Based on 2010-2011 NASS-GES and FARS data.

[347] MAIS (Maximum Abbreviated Injury Scale) represents the maximum injury severity of an occupant at an Abbreviated Injury Scale (AIS) level. AIS ranks individual injuries by body region on a scale of 1 to 6: 1=minor, 2=moderate, 3=serious, 4=severe, 5=critical, and 6=maximum (untreatable).

[348] 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 the n 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 enabling us to create the KABCO-translator.

[349] Passenger-vehicle-to-passenger-vehicle and passenger-vehicle-to-heavy-vehicle account for 4.5 percent (241,000).

[350] Heavy vehicles include trucks and buses with GVWR greater than 10,000 pounds.

[351] Passenger vehicles include passenger cars, vans, minivans, sport utility vehicles, and light pickup trucks with gross vehicle weight rating (GVWR) 10,000 pounds or less.

[352] Passenger-vehicle-to-passenger-vehicle and passenger-vehicle-to-heavy-vehicle account for 4.5 percent (241,000).

    - straight cross passing
- Rear-end crashes for FCW
    - Lead vehicle stopped (LVS)
    - Lead vehicle moving at a slower speed or was accelerating (LVM)
    - Lead vehicle decelerating (LVD)
- Lane change/merge crashes for BSW/LCW have been defined as crashes where a vehicle made a lane changing/merging maneuver prior to the crash

Note that "intersection" in this analysis included intersection, intersection-related, driveway/alley, and driveway access areas. Rear-end crashes does not include crashes where the lead vehicle made a lane change/merge pre-crash maneuver. Furthermore, crashes involving alcohol, vehicle failure, and loss-of-control are also excluded, because we assumed that V2V-based safety applications would not produce an effective response by the driver under these conditions.[353] For the preliminary benefit analysis, the agency focused only on IMA and LTA. FCW was not included in the benefits estimation because of the significant overlap with radar-based FCW systems; BSW/LCW and DNPW were also not included because insufficient data exists at this time to assess their effectiveness.

Table XII-1 shows crash statistics for the four safety applications. As shown, annually there are 2.94 million crashes with 2,669 fatalities and 1.07 million MAIS 1-5 injuries that could be addressed by these four V2V safety applications. In addition, about 4.05 million PDOV crashes could also be addressed. Of these, 1.04 million crashes, 1,932 fatalities, 450,000 MAIS 1-5 injuries, and 1.28 million PDOVs could be impacted by IMA and LTA. Separately, IMA could impact 760,000intersection crashes and thus the 1,637 associated fatalities and 300,000MAIS 1-5 injuries. LTA could impact 280,000 crashes and the associated 295 fatalities and 150,000 MAIS 1-5 injuries.

[353] Crash scenarios were excluded based on the criteria that an impaired driver would be required to react, and the fact of their impairment would likely lead them not to react as required.

Table XII-1 Safety Target Population for FCW, LCW, IMA, and LTA - Passenger Vehicles[354]

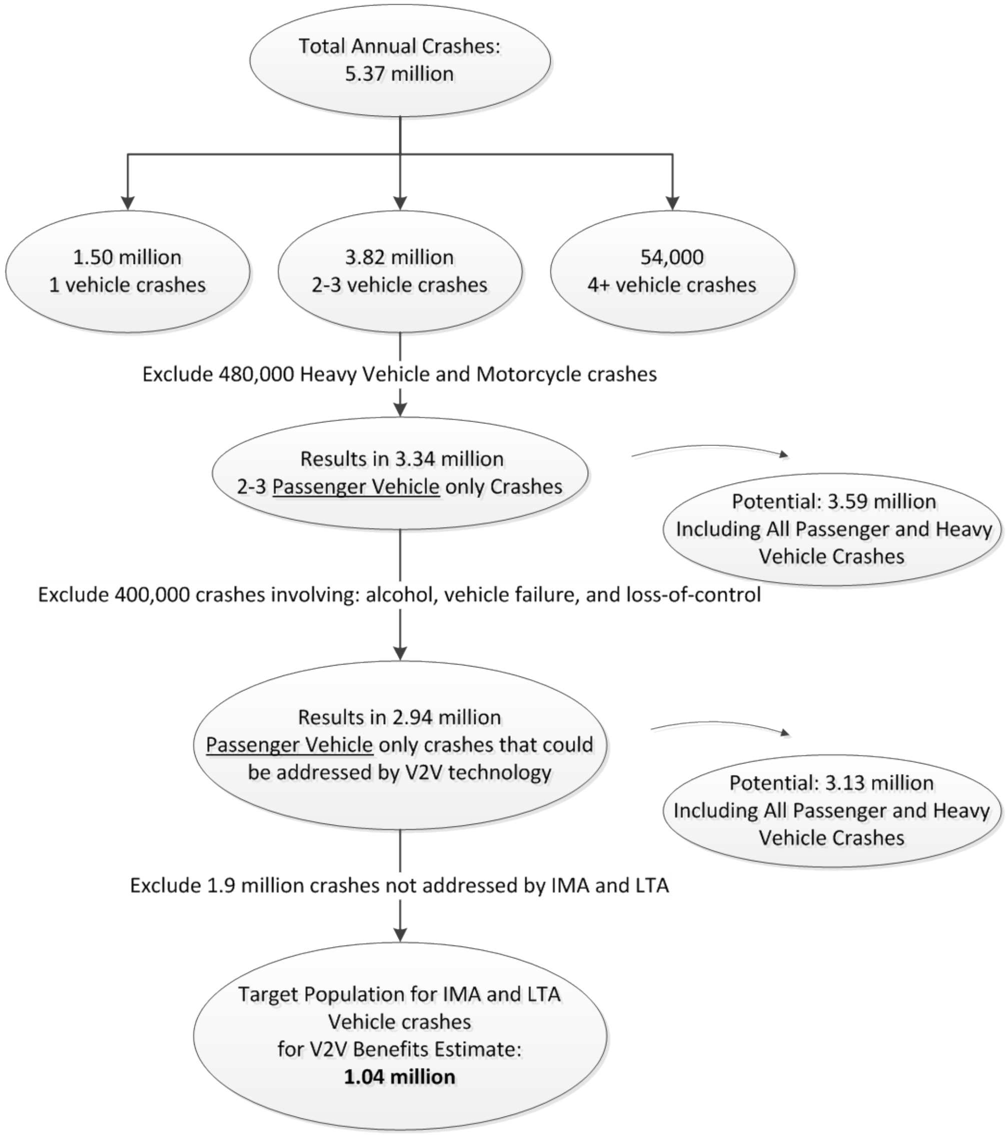
	FCW (LVS)	FCW (LVM)	FCW (LVD)	FCW TOTAL	IMA	LTA	IMA, & LTA TOTAL	LCW	GRAND TOTAL
Crashes	946,668	167,807	329,510	1,443,985	757,195	283,503	1,040,698	458,506	2,943,189
PDOC[355]	641,153	113,407	225,797	980,357	472,694	150,530	623,224	362,688	1,966,269
Injury	305,515	54,400	103,713	463,628	284,501	132,973	417,474	95,818	976,920
Fatality	161	234	47	442	1,637	295	1,932	295	2,669
MAIS 1-5 Injuries	342,516	63,350	117,425	523,291	303,987	150,674	454,661	94,430	1,072,382
PDOVs[1] in PDOC	1,321,417	233,732	465,367	2,020,516	974,223	310,242	1,284,465	747,500	4,052,481

Figure XII-1 provides a graphical breakdown of crashes and the process as discussed previously for deriving the target population for benefits estimation. The potential target population as shown is where heavy vehicle crashes are considered. The graphical breakdown begins with the total annual number of police-reported crashes of 5.37 million, and ends with the target crashes of 1.04 million for IMA and LTA.

[354] Source: 2010-2011 GES and FARS.

[355] Property-damage-only crash.

Figure XII-1 V2V Benefits Estimation Target Population (Annual) Breakdown



Total Annual Crashes: 5.37 million
1.50 million 1 vehicle crashes
3.82 million 2-3 vehicle crashes
54,000 4+ vehicle crashes
Exclude 480,000 Heavy Vehicle and Motorcycle crashes
Results in 3.34 million 2-3 Passenger Vehicle only Crashes
Potential: 3.59 million Including All Passenger and Heavy Vehicle Crashes
Exclude 400,000 crashes involving: alcohol, vehicle failure, and loss-of-control
Results in 2.94 million Passenger Vehicle only crashes that could be addressed by V2V technology
Potential: 3.13 million Including All Passenger and Heavy Vehicle Crashes
Exclude 1.9 million crashes not addressed by IMA and LTA
Target Population for IMA and LTA Vehicle crashes for V2V Benefits Estimate: 1.04 million

B. Effectiveness of the V2V safety applications

The system crash avoidance and crashworthiness effectiveness is determined by comparing crash rates and the injury probabilities of vehicles with and without V2V. Since V2V is an emerging technology and is not in production, a statistical analysis of vehicles with and without the technology using real-world crash data was not feasible. Instead, the agency developed a computer simulation model, Safety Impact Methodology (SIM), [356] and a laboratory driver simulator (MiniSim), to estimate the effectiveness and then the preliminary benefits of V2V-based safety application technologies, specifically, IMA and LTA.[357] Therefore, these two sources are the basis for estimating the crash avoidance and crashworthiness values.

1. Safety Impact Methodology - SIM

In order to obtain a crash warning using V2V technology, two V2V-equipped vehicles need to interact during a potential crash situation – if a V2V-equipped vehicle interacts with a non-V2V-equipped vehicle in a potential crash situation, no warning is to be expected, because the non-equipped vehicle would produce no BSM for the equipped vehicle to recognize and respond to. To be able to estimate the effectiveness of advanced crash avoidance technology such as V2V, NHTSA developed a methodology that uses available data and computer simulation,[358] extending current estimation capabilities and enabling V2V technology to be "exposed" to more conflict situations to make up for the lack of crashes in the real-world crash databases. This allows the agency to better comprehend the crash avoidance potential and the performance criteria of the V2V technology prior to the technology's actual deployment.

The "Safety Impact Methodology" or "SIM" estimates safety benefits in terms of the number of crashes avoided using the estimated effectiveness of the safety applications to avoid crashes. These estimates are obtained using the following set of equations:

Equation XII-3 Number of Crashes Avoided Calculation

$$\textit{Number of Crashes Avoided} = \text{Number of Target Crashes} \times \text{Application Effectiveness}$$

The application effectiveness is estimated based on the following equation:

Equation XII-4 Application Effectiveness Calculation

$$\textit{Application Effectiveness} = 1 - \text{Exposure Ratio} \times \text{Crash Prevention Ratio}$$

[356] Safety Impact Methodology (SIM): Application and Results of the Advanced Crash Avoidance Technologies (ACAT) Program (Funke, Srinivasan, Ranganathan, and Burgett, June 2011, Paper Number 11-0367, 22nd International Technical Conference on the Enhanced Safety of Vehicles). See www-nrd.nhtsa.dot.gov/pdf/esv/esv22/22ESV-000367.pdf (last accessed Jan. 29, 2014).

[357] The agency examined 50 intersection or left turn across path crashes from the NASS data base for which we had EDR information from both vehicles involved. Thus, we knew the velocity and brake activation of both vehicles from 5 seconds to 1 second before the crash. These analyses were used to determine that the SIM results did match very well with real crashes.

[358] For an overview of this methodology, see supra note 354.

Where:

Equation XII-5 Exposure Ratio Calculation

$$\textit{Exposure Ratio (ER)} = \frac{\text{Exposure Measure to Driving Conflicts } \textbf{\textit{with}} \text{ Application Assistance}}{\text{Exposure Measure to Driving Conflicts } \textbf{\textit{without}} \text{ Application Assistance}}$$

And

Equation XII-6 Crash Prevention Ratio Calculation

$$\textit{Crash Prevention Ratio (CPR)} = \frac{\text{Crash Probability in Driving Conflict } \textbf{\textit{with}} \text{ Application Assistance}}{\text{Crash Probability in Driving Conflict } \textbf{\textit{without}} \text{ Application Assistance}}$$

The Exposure Ratio (ER) is the measure of change a safety application may have on drivers being exposed to conflict.[359] In other words, V2V safety applications may change driver behavior such that a driver can better anticipate a potential conflict and adjust such that the conflict does not occur. The change to drivers' exposure to conflicts is obtained from field observations (not simulated in SIM) during a field operational test, usually over an extended period of time. However, it may be difficult to quantify the exposure to conflicts with and without the safety application with any statistical significance due to relatively short test time periods (a driver's adaptation to a safety application usually takes longer than the 3 to 24 weeks a driver [subject] experiences the safety technology in the context of the current research). In recognition of this difficulty, a conservative estimate of the ER parameter is set to one for purposes of the present analysis, meaning that there is no difference in exposure to driving conflicts whether the V2V application is present or not.

The Crash Prevention Ratio (CPR) equation accounts for whether or not a vehicle will crash with another vehicle in a driving conflict as a result of the first vehicle's crash-avoidance action, such as braking to stop. It is estimated using a SIM computer-based simulation. The SIM's primary duty in relation to estimating the CPR is to mimic, as close to real-world as possible, the actual conditions, interactions, and performance of the driver, vehicle, and safety application of target driving conflicts corresponding to major pre-crash scenarios. This simulation uses input data from national crash databases; driver, vehicle, and V2V safety application performance data from naturalistic field operational tests (Safety Pilot Model Deployment); track tests; and related driver, vehicle, or safety application evaluation studies. Outputs of the tool consist of the number of crashes avoided and impact speed reduction that can

[359] Driving conflicts correspond to the kinematics of the target pre-crash scenarios. An exposure to a driving conflict is counted when the movements of the host vehicle and the principal other vehicle match the configuration of the driving conflict and the two vehicles are on a crash course if a crash avoidance action is not taken by either vehicle.

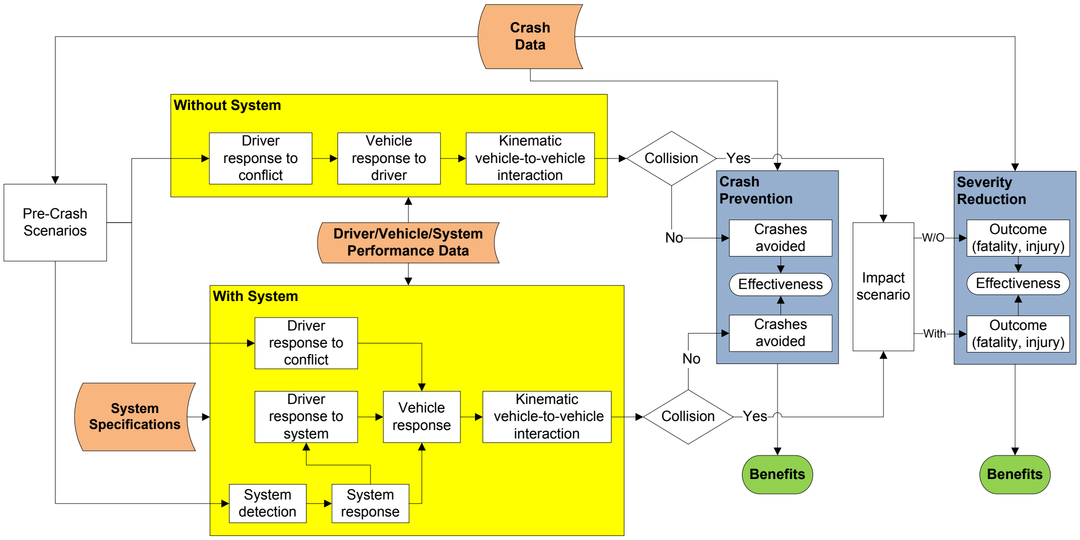
be translated into harm reduction, including savings in crash comprehensive costs and decreases in the number of persons injured at different levels of the MAIS.

To support the calculation of the CPR by the SIM, the simulation component needs to generate data on crashes both with and without the V2V safety applications. A 2010 report by Ford, Volvo, and UMTRI developed an approach to generating such data by using field trials to create a number of driving scenarios that are relevant to the technology/safety application in question, but may or may not lead to a crash.[360] Each scenario is evaluated without the V2V safety application, and then the same scenario can be evaluated again with the application in place. Each scenario comprises a number of "conflicts" generated using a Monte Carlo[361] approach, where a conflict is a specific driving situation (e.g., vehicle traveling at 50 mph detects a lead vehicle that is stopped 200 feet away) that would fall under the pre-crash scenario in question (e.g., lead vehicle stopped). Each conflict can be evaluated for whether a crash is avoided or does occur. If a crash is avoided, benefits are estimated based on the number of fatalities and injuries that are avoided. If a crash would occur, benefits are estimated in relation to reductions in fatalities and injuries due to possible mitigation of crash impact. A change in crash impact is measured by the change in velocity, delta-V, which can be translated into changes in fatalities and injuries. For this exercise, a similar approach was implemented into the SIM. Figure XII-2 illustrates the structure of the SIM developed to estimate V2V safety application benefits.

[360] Advanced Crash Avoidance Technologies (ACAT) Program – Final Report of the Volvo-Ford-UMTRI Project: Safety Impact Methodology for Lane Departure Warning – Method Development and Estimation of Benefits (Gordon et al., Oct. 2010, Report No. DOT HS 811 405). See www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print (last accessed Jan. 29, 2014).

[361] A Monte Carlo simulation is a problem solving technique that builds models of possible results by substituting a range of values – a probability distribution – for any factor that has inherent uncertainty. It then calculates results over and over, each time using a different set of random values from the probability functions. Depending on the uncertainties and the ranges specified for them, a Monte Carlo simulation could involve thousands or tens of thousands of recalculations before it is complete. Monte Carlo simulation produces distributions of possible outcome values.

Figure XII-2 SIM Logic and Structure



The SIM V2V benefit estimation process used here began with the generation of pre-crash scenarios using crash statistics from the National Automotive Sampling System General Estimate System (NASS-GES) that compiles crash data from a nationally-representative sample of police-reported motor vehicle crashes of all crash types. From each scenario, specific conflicts (a combination of driver, vehicle, and scenario characteristics) were generated using probability distribution-based historical data and Safety Pilot Model Deployment data.[362] The distributions used to generate the specific conflicts included safety system performance (system activation), driver reaction time, braking level, and the vehicle speed/distance-to-collision distributions. The distributions of various characteristics support the use of a Monte Carlo approach that was used to run thousands of conflicts that were then evaluated with and without the safety application. The results from these conflict evaluations -- crashes, crashes avoided, or crashes mitigated -- were summarized, leading to system effectiveness and harm reduction ratios for the different scenario/safety application combinations. The effectiveness and harm reduction ratios for each scenario/safety application were then applied to the target population for each scenario to estimate the level of benefits that may result from each safety application. The collective benefits from the evaluated safety application provide a total estimate of benefits that can then be compared to the estimated cost for the V2V system.

[362] Each specific conflict is a single event with only the vehicles involved in the conflict included in the simulation. Unintended consequences (e.g., a crash caused by avoiding a crash) that involve other non-conflict vehicles are not captured through the simulation.

Although the SIM can generate both effectiveness and benefit estimates, only the effectiveness outcome was used in this analysis due to some refinement to the target populations that would not be considered in the SIM. The process of deriving the system effectiveness for a safety application can be briefly summarized by the following steps:

(1) Derive the initial effectiveness for various pre-crash scenarios and speed ranges (from SIM or MiniSim)
(2) Derive the overall effectiveness for each pre-crash scenario by calculating the weighted effectiveness of initial effectiveness over all speed ranges
(3) Derive the system effectiveness by calculating the weighted effectiveness of pre-crash scenario effectiveness over all pre-crash scenarios
(4) Derive the final system effectiveness by multiplying the overall effectiveness by a factor to take into account situations that were not addressed by SIM and MiniSim.

For crashworthiness, the effectiveness E_w of an application is the effect of delta-V reduction on crash severity for those crashes that cannot be avoided by the safety application, where delta-V is the recorded change in velocity experienced during a crash.[363] E_w was estimated by MAIS injury level. As stated earlier, SIM was used to generate crash impact speed distributions separately for the baseline and treatment groups. These speed distributions were used as the proxy for delta-V to estimate E_w. SIM groups the impact speeds into 16 intervals. The first interval is from 0 to less than 3 mph, noted as [0, 3), with 3 mph increment for the subsequent intervals until 46 mph. Impact speeds of 47 mph and higher were aggregated into the last interval notes as 47+ mph. SIM treats all involved vehicles with equal mass. Therefore, half of the impact speed is a substitute for delta-V of the crash. Furthermore, the mid-point of each interval was used to calculate the average delta-V for each pre-crash scenario. The sum of the products of the mid-points and their corresponding percent of distributions derives the average delta-V for that specific pre-crash scenario. Then, applying the percent of real-world crash distribution to the average delta-V derives the weighted average delta-V for a target crash type. MAIS injury probability curves were used to locate the MAIS injury probabilities at the weighted average delta-V level both for control and treatment group. The effectiveness for a MAIS level can be noted as:

[363] The vehicle resultant change in velocity, commonly referred to as simply resultant delta-V, is the primary description of crash severity in most crash databases. "Estimating Crash Severity: Can Event Data Recorders Replace Crash Reconstruction?" For additional information, see www.nhtsa.gov/DOT/NHTSA/NRD/Articles/ESV/PDF/18/Files/18ESV-000490.pdf (last accessed: January 29, 2014).

Equation XII-7 MAIS Effectiveness Calculation

$$E_w = 1 - \frac{p_t}{p_c}$$

Where, E_w = MAIS effectiveness

P_t = injury probability for the treatment group

P_c = injury probability for the control group

The following summarizes the process for deriving E_w. A detailed description of the process is contained in each of the following sections dedicated to specific applications.

(1) Derive the delta-V distribution for each of the pre-crash scenarios for baseline (i.e., without V2V) and treatment groups (with V2V).
(2) Derive an average delta-V for each scenario for the baseline and treatment groups
(3) Derive the weighed delta-V for all scenarios combined
(4) Derive injury probability curves
(5) Estimate the MAIS injury probabilities at the weighted average delta-V level using injury probability curves

In the following sections dedicated to specific safety applications, the process of deriving crash avoidance and crashworthiness effectiveness will be discussed in detail.

2. Driving Simulator Study - MiniSim

MiniSim is a driving simulator in a controlled laboratory environment, which was used for evaluating IMA and LTA applications in avoiding crashes. Drivers were recruited to drive three IMA and two LTA pre-crash scenarios. These drivers are divided into baseline (no IMA or LTA warning given) and treatment (IMA or LTA warning given) groups. The crash avoidance effectiveness (E_a) is derived from the crash rates and reaction times of these two groups.

A total of 144 drivers successfully completed the IMA study. Table XII-2 shows the experimental design and breakdown of these drivers in this study.[364] These drivers were equally divided into three groups of 48 for each of the three driving conditions listed above. Within a group, 24 drivers received an alert (treatment group) and 24 did not (baseline group). Each group is equally divided among three age groups (18 to 24, 40 to 50, and 60 or older) and by gender

[364] Summary Report for a Simulator Study of Intersection Movement Assist (IMA) and Left Turn Assist (LTA) Warning Systems (Balk, Sept. 2013, Turner-Fairbank Highway Research Center, Internal Report). See Docket No. NHTSA-2014-0022.

(i.e., male and female) as seen in Table XII-2. Each driver experienced only one of the three driving conditions.

Table XII-2 Breakdown of Drivers in IMA Study

Alert Condition	**Age (Years)**	**Gender**	**Driving Condition**		
			PCP-M	**PCP-S Left**	**PCP-S Right**
Baseline (No Alert)	18-24	Male	4	4	4
		Female	4	4	4
	40-50	Male	4	4	4
		Female	4	4	4
	≥ 60	Male	4	4	4
		Female	4	4	4
		Subtotal	24	24	24
Treatment (Alert)	18-24	Male	4	4	4
		Female	4	4	4
	40-50	Male	4	4	4
		Female	4	4	4
	≥ 60	Male	4	4	4
		Female	4	4	4
		Subtotal	24	24	24
		Total	48	48	48

The MiniSim design for IMA is for drivers to experience one of three driving conditions at a four-way intersection.

1. The driver approaches the intersection with a green light and another vehicle approaches from the left (PCP-M)
2. The driver approaches the intersection with a stop sign and another vehicle approaches from the left (PCP-S)
3. The driver approaches the intersection with a stop sign and another vehicle approaches from the right (PCP-S)

In all conditions, the driver is traveling at 45 mph toward the intersection and attempting to drive straight through the intersection. Just before the driver crosses into the intersection, the approaching vehicle, obscured by a stationary large truck, appears coming from the perpendicular/lateral side at a constant speed of 45 mph. If no attempt to apply the brakes was taken by the driver participating in the study, the vehicles would crash in 3.3 seconds.

The MiniSim design for LTA is for drivers to experience one of two driving conditions while making a left turn at an intersection.

1. The driver had a green light and could make the turn without stopping (LTAP/OD-M)
2. The driver had a red light initially and had to stop, and then made a left turn when the light turned green (LTAP/OD-S)

In both conditions, the driver and an approaching vehicle approach each other from opposite directions. As soon the driver started to initiate the left turn and exceeded 6 mph in speed, the approaching vehicle appeared behind the stopped truck, traveling forward at a constant speed of roughly 45 mph. If no action was taken by the driver, the two vehicles would crash in about 3.3 seconds.

A total of 96 drivers were recruited for LTA. These drivers were evenly divided into two groups of 48 each and were further evenly divided into baseline and treatment.

3. Injury probability curves

Injury probability curves predict the probabilities of MAIS injuries based on delta-V. These curves were derived from 2000-2011 CDS data. CDS is a nationally-representative sampling system of passenger vehicle crashes where at least one passenger vehicle was towed. CDS was used because it is the only nationally-representative crash database that collects both delta-V and MAIS. A logistic model is the base for developing these curves. The logistic model predicts the probability of MAIS injuries that would occur at a specific delta-V level. The dependent variable of the model is MAIS+ injury severity which is dichotomy. The value is 0 when an injury is less than a certain MAIS level and 1 if an injury is equal to or greater than that MAIS level. Delta-V is the independent variable.

The derived MAIS+ injury probability curves for a delta-V level “x” thus have the form:

Equation XII-8 MAIS+Injury Probability of Risk

$$p_{MAIS+}(x) = \frac{e^{ax+b}}{1+e^{ax+b}}$$

Where, a = 0.092845, b = -1.14421 for MAIS 1+

a = 0.13527, b = -4.51842 for MAIS 2+

a = 0.16851, b = -6.33516 for MAIS 3+

a = 0.17329, b = -7.77703 for MAIS 4+

a = 0.18588, b = -9.35528 for MAIS 5+

a = 0.19471, b = -11.70930 for fatality

The probability for certain injury level is simply the difference of two MAIS+ probabilities. In other words, $p_{MAIS1} = p_{MAIS1+} - p_{MAIS2+}$, $p_{MAIS2} = p_{MAIS2+} - p_{MAIS3+}$, and etc.

4. Crashworthiness effectiveness by MAIS

For calculating the injury reduction rates, the delta-Vs produced for the baseline and treatment were input into the MAIS+ formula. Table XII-3 presents the process. As shown, given a reduction on delta-V by 1.17 mph, IMA would mitigate MAIS 1 injuries by 6 percent, MAIS 2 injuries by 16 percent, and MAIS 4 injuries by 50 percent. Note that at the delta-V level of 8.17 and 7.00 mph levels, the probabilities of having MAIS 3+ injuries are small. Therefore, the probability estimation for MAIS 3, MAIS 4, MAIS 5, and fatality might have a greater variation for these injury levels.

Table XII-3 Probabilities of MAIS Injuries and Injury Reduction Effectiveness

Injury Severity	Probability		Injury Severity	Probability		Injury Reduction Rate
	Baseline (8.17 mph)	Treatment (7.00 mph)		Baseline (8.17 mph)	Treatment (7.00 mph)	
MAIS 1+	0.405	0.379	MAIS 1	0.373	0.352	0.06
MAIS 2+	0.032	0.027	MAIS 2	0.025	0.021	0.16
MAIS 3+	0.007	0.006	MAIS 3	0.005	0.005	0.00
MAIS 4+	0.002	0.001	MAIS 4	0.002	0.001	0.50
MAIS 5+	0.000	0.000	MAIS 5	0.000	0.000	0.00
Fatality	0.000	0.000	Fatality	0.000	0.000	0.00

Source: 2000-2011 CDS

5. Effectiveness of Intersection Movement Assist - IMA

a) IMA Crash Avoidance Effectiveness (E_a)

The effectiveness for IMA was estimated based on two major pre-crash scenarios employed in the design of the MiniSim: (1) perpendicular crossing path, with the driver stopping and then proceeding and another vehicle approaching from either the right or the left without stopping (PCP-S) and (2) perpendicular crossing path, with the driver approaching the intersection without stopping and another vehicle approaching from the left without stopping (PCP-M). The drivers' measured brake reaction time and brake deceleration level collected during the study from both the baseline and treatment MiniSim groups were then used as inputs into SIM to derive effectiveness values for various speed ranges for these pre-crash scenarios.

(1) Crash Avoidance PCP-S Crash Scenario

For the PCP-S crash scenario, MiniSim data was used to simulate crash outcomes for five different traveling speed ranges for an approaching vehicle under three separate distances between the driver (of the vehicle that stopped at the intersection and then proceeded) and the point where the driver's vehicle would make contact with the approaching vehicle. The following sections describe this process.

(a) Crash Distribution by Vehicle Speed

The agency developed a series of five bins to create a crash distribution by vehicle speed. For this evaluation, the approaching vehicle speed ranges evaluated were: [10, 25), [25, 35), [35, 45), [40, 55), and 55+ mph where the pair symbol [x, y) represents that the speed is at least x mph but less than y mph, and the plus symbol x+ represents that the speed is x mph and higher. The driver speed identified for this scenario is between 0 to 9 mph, to represent a vehicle stopped and then proceeding into the intersection. The agency developed the crash distribution shown in Table XII-4 by using these identified speed ranges as parameters in the SIM tool's Monte Carlo analysis.

Table XII-4 Percent of Crash Distribution* by Approaching Vehicle Traveling Speed (p_i)

Driver Vehicle Speed	**Approaching Vehicle Travel Speed (mph)**				
(mph)	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+
[0 , 10)	11.89%	9.88%	8.76%	2.95%	1.05%

*served as weight for calculating weighted effectiveness; already adjusted for unknown speed
Source: 2010-2011 GES

(b) Vehicle to Vehicle Distances Evaluated

The distance between the driver and approaching vehicle evaluated were: 3-5 meters, 4 meters, and 5-8 meters. Furthermore, the simulation was further refined by the impact location of the approaching vehicle, i.e., the left or right side of the vehicle, based on the percentages identified in Table XII-5.

Table XII-5 Percent of Impact Location*

Left Side Impact	**53.12%**
Right Side Impact	46.88%

*served as weight for calculating weighted effectiveness; already adjusted for unknown speed
Source: 2010-2011 GES

(c) IMA PCP-S Effectiveness Calculation

The IMA PCP-S scenario thus encompassed 30 initial effectiveness values, given 5 speed ranges * 2 vehicle impact locations * 3 separating distances. The weighted effectiveness for all five speed ranges and impact locations was calculated for each separating distance. This weighted effectiveness was then applied to the percentage of PCP-S crashes that occur in all IMA crashes to calculate the weighted effectiveness (E_a) using the following mathematical formula:

Equation XII-9 IMA PCP-S Crash Effectiveness Calculation

$$E_a=R\sum_{i=1}^{5} p_i*E^i_{a1}+(1-R)\sum_{i=1}^{5} p_i*E^i_{a2}$$

Where, E_a = weighted effectiveness

R = proportion of PCP-S right side impact

P_i = proportion of PCP-S in speed range i, with i=1 for [10,25) and 5 for 50+ mph

E^i_{a1} = effectiveness for speed range I for right side impact.

E^i_{a2} = effectiveness for speed range I for left side impact.

Table XII-6 provides the 30 effectiveness values calculated for using this methodology:

Table XII-6 SIM Estimated Initial Effectiveness (E^i_{a1} and E^i_{a2})

Separating	**Remote Vehicle Travel Speed (mph)**				
Distance (m)	**[10 , 25)**	**[25, 35)**	**[35, 45)**	**[45, 55)**	**55+**
Left Side					
3-5	0.71	0.66	0.64	0.56	0.45
4	0.81	0.78	0.66	0.55	0.41
5-8	0.70	0.67	0.53	0.43	0.32
Right Side					
3-5	0.70	0.70	0.64	0.59	0.48
4	0.83	0.79	0.70	0.59	0.44
5-8	0.73	0.65	0.56	0.47	0.35

(d) Summary of IMA PCP-S Effectiveness

The agency did not employ all of these initial effectiveness estimates in developing our ultimate estimate of IMA effectiveness in the PCP-S scenario. Instead, we focused on two crash distributions that best reflected our understanding of current and future system capabilities in real-world situations. Using the two distribution results in estimating a range of effectiveness that reflects the current limitation of the current prototype (but does not limit the potential impact that IMA could have on the target population it could address).

The first distribution does not include the crashes that occur between 10 to 24 mph, [10, 25), because current prototype IMA designs (like those used in the Safety Pilot model deployment) do not issue warnings unless one of the interacting vehicles is traveling at or above 25 mph. This means that the effectiveness of IMA is treated as 0 for these crashes in the first distribution. The second distribution, on the other hand, includes the [10, 25) speed interval, in order to reflect our expectation that future improvements to IMA will allow the application to operate down to 10 mph.

Using these two distributions reduced the initial set of 30 effectiveness values to a total of 3 weighted effectiveness values (as shown in Table XII-7, the agency estimates IMA would avoid 15-24 percent of PCP-S crashes), which we used for benefits estimation.

Table XII-7 Weighted IMA Effectiveness (E_a) for PCP-S Crash Scenario

	Separating Distance		
	3-5 meters	4 meters	5-8 meters
Low	0.15	0.16	0.15
High	0.23	0.24	0.24

The three weighted effectiveness values were later combined with the weighted crash avoidance effectiveness (E_a) for the PCP-M crash scenario, discussed below, to derive the final effectiveness for IMA.

(2) Crash Avoidance PCP-M Crash Scenario

For the PCP-M crash scenario, as for the PCP-S crash scenario, data generated by the MiniSim study was used as input to the SIM. The PCP-M evaluation is slightly more straightforward than for PCP-S for two reasons: first, PCP-M involves both vehicles moving, and second, PCP-M only involves the "other vehicle" approaching the driver from the left. As a result, the full range of vehicle speeds apply to both the driver and the approaching vehicle, and no accounting for vehicle impact side or vehicle to vehicle distance is evaluated.

(a) Crash Distribution by Vehicle Speeds

The same series of five bins ([10, 25), [25, 35), [35, 45), [40, 55), and 55+ mph) were used to develop a crash distribution by vehicle speed as for the PCP-S crash scenario, but since all five speed range bins are considered applicable and evaluated for both the driver and approaching vehicles, 25 crash distribution values result instead of the 5 values for PCP-S.

Table XII-8 Percent of Crash Distribution* by Approaching Vehicle Traveling Speed (p_i)

Driver Vehicle Speed	**Approaching Vehicle Travel Speed (mph)**				
(mph)	**[10 , 25)**	**[25, 35)**	**[35, 45)**	**[45, 55)**	**55+**
[10 , 25)	13.01%	11.00%	10.76%	3.50%	0.78%
[25, 35)	5.23%	3.80%	1.87%	0.85%	0.10%
[35, 45)	3.43%	1.09%	1.73%	0.58%	0.07%
[45, 55)	1.29%	0.37%	0.44%	0.65%	0.10%
55+	0.41%	0.03%	0.24%	0.07%	0.07%

*served as weight for calculating weighted effectiveness; already adjusted for unknown speed
Source: 2010-2011 GES

(b) IMA PCP-M Effectiveness Calculation

Using the same effectiveness calculation method as that for PCP-S, a total of 25 initial effectiveness values were generated by the SIM for the IMA PCP-M scenario. The reader will remember that in PCP-M, we did not consider vehicle impact side or vehicle separating distance, so the 25 initial effectiveness values reflect only the interactions of the two vehicles depending on their speed.

As discussed above for PCP-S, the initial effectiveness for the cell "driver vehicle speed [10, 25)," "approaching vehicle speed [10, 25)" was not used (i.e., treated as 0) for the effectiveness calculation given current system limitations that cause IMA not to activate below 25 mph. This cell is therefore shaded gray in Table XII-9. The wide range illustrates the uncertainty concern on the inherent computation variations including those from SIM, MiniSim, and GES sampling errors.

Table XII-9 SIM Estimated Initial Effectiveness (E_a)

Driver Vehicle Speed (mph)	Approaching Vehicle Travel Speed (mph)				
	[10 , 25)	[25, 35)	[35, 45)	[45, 55)	55+
[10 , 25)	0.47	0.51	0.55	0.57	0.60
[25, 35)	0.41	0.50	0.56	0.59	0.63
[35, 45)	0.43	0.54	0.60	0.63	0.67
[45, 55)	0.46	0.58	0.63	0.66	0.69
55+	0.49	0.62	0.66	0.67	0.69

(c) Summary of IMA PCP-M Effectiveness

Using the same methodology as the PCP-S crash scenario, the agency developed a weighted estimated effectiveness of 26 to 31 percent for IMA when a driver is involved in the PCP-M crash scenario. However, the agency again notes that the lower bound of effectiveness reflects the current prototype design of IMA, where a warning is issued when the driver is traveling above 25 mph. As mentioned above, it is anticipated that future tuning of the IMA application would allow it to operate at speeds as low as 10 mph.

(3) IMA Crash Avoidance System Effectiveness

The overall IMA system effectiveness is calculated by combining the effectiveness values of the PCP-S and PCP-M crash scenarios. This is possible because the weighted effectiveness values for these crash scenarios took into account the corresponding crash proportion for each scenario. Therefore, the overall system effectiveness is simply the sum of these two weighted effectiveness rates.

Based on the combination of the IMA PCP-S and PCP-M effectiveness values, the agency estimates IMA has the potential to help drivers avoid 41 to 55 percent of intersection crashes.[365] In other words, the agency estimates that by providing a warning that an intersection crash is about to occur, drivers will avoid 41 to 55 percent of all target IMA intersection crashes.

b) IMA Crashworthiness Effectiveness (E_w)

The crashworthiness effectiveness (E_w) for IMA was developed using crash impact speed distributions generated by the SIM. As discussed in Section XII.B.1, these crash impact distributions were used as the proxy for delta-V distributions. Additionally, injury probability curves for this analysis were derived as described in Section XII.B.3

(1) Crashworthiness PCP-S Crash Scenario

Estimates for the IMA Crashworthiness PCP-S scenario were developed based on 15 crash conditions for each impact location – left or right side (i.e., approaching vehicle traveling speeds, left and right impact locations, three separating distances). These 15 conditions were simulated using the SIM tool to produce delta-V distributions for both the baseline and treatment groups for comparison. Details for each distribution are shown in Table XIII-2 and Table XIII-3, respectively.

Table XII-10 shows the average delta-Vs that were derived by multiplying the delta-V by its corresponding distribution percentage.

Table XII-10 Derived Average Delta-V (mph) by Simulated Crash Conditions

Separating	Baseline					Treatment				
Distance	Approaching Vehicle Speed (mph)					Approaching Vehicle Speed (mph)				
(Meter)	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+
Left Side Impact										
3-5	4.01	5.80	6.94	7.63	7.74	3.63	5.29	6.19	6.87	6.85
4	3.95	5.38	6.68	7.54	7.50	3.58	4.91	6.26	6.77	6.92
5-8	3.97	4.90	5.45	5.93	6.06	3.37	4.1	4.72	6.4	5.79
Right Side Impact										
3-5		5.78	6.98	7.68	7.72		5.29	6.19	6.87	6.85
4	4.12	5.50	6.60	7.93	7.57	3.58	4.91	6.26	6.77	6.92
5-8	3.77	4.27	4.95	5.44	5.18	3.37	4.1	4.72	6.4	5.79

Applying the crash distribution based on approaching vehicle traveling speed categories shown in Table XII-11 to the average delta-V provides the average delta-V for PCP-S crash scenarios.

[365] The result of adding 15 – 24 percent for PCP-S and 26 - 31 percent for PCP-M.

Table XII-11 Traveling Speed Distribution*

Approaching Vehicle Speed (mph)				
[10 , 25)	[25, 35)	[35, 45)	[45, 55)	55+
0.3091	0.2568	0.2277	0.0767	0.0273

*used as weight to calculate the delta-V level for an average PCP-S

As shown in Table XII-12, the average delta-V ranged from 4.16 to 4.95 mph for baseline crashes (without V2V) and 3.82 to 4.50 mph for treatment crashes (with V2V). This tells us that when a driver is stopped at an intersection, decides to go, and has a crash, the difference in the delta-V of that crash with or without a V2V warning is relatively small. The real benefit of V2V relates to the go/no go decision, and avoiding the crash by V2V warning the driver of the impending crash and the driver deciding not to go into the intersection.

Table XII-12 Delta-V for an Average PCP-S Crash

Separating Distance	Baseline	Treatment
3-5	4.53	4.08
4	4.95	4.50
5-8	4.16	3.82

(2) Crashworthiness PCP-M Crash Scenario

For the IMA PCP-M crash scenario, the process of deriving the delta-V for an average PCP-M crash is similar to that for PCP-S. The only difference between the two is the simulated crash conditions. There were 25 conditions for PCP-M, representing the combinations of five drivers and five approaching vehicles. Table XII-13 and Table XII-14show the parallel process to the PCP-S crash scenario for generating an average crash delta-V for a PCP-M crash.

Table XII-13 Derived Average Delta-V (mph) by Simulated Crash Conditions

Host	Baseline					Treatment				
Vehicle	Approaching Vehicle Speed (mph)					Approaching Vehicle Speed (mph)				
Speed	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+
[10, 25)	7.73	7.73	7.75	7.77	7.83	5.36	5.84	6.25	6.42	6.82
[25, 35)	12.68	12.75	12.87	12.96	13.1	8.52	9.74	10.48	10.85	11.5
[35, 45)	16.21	16.45	16.67	16.86	17.21	11.62	13.51	14.51	15.07	15.94
[45, 55)	19.41	19.93	20.33	20.57	21.05	14.97	17.63	18.85	19.53	20.52
55+	21.38	22.09	22.51	22.74	23.04	18.28	21.34	22.35	22.81	23.2

Table XII-14 Traveling Speed Distribution*

Host Vehicle	**Approaching Vehicle Speed (mph)**				
Speed	**[10 , 25)**	**[25, 35)**	**[35, 45)**	**[45, 55)**	**55+**
[10, 25)	21.16%	17.89%	17.50%	5.69%	1.27%
[25, 35)	8.51%	6.18%	3.04%	1.38%	0.16%
[35, 45)	5.58%	1.77%	2.81%	0.94%	0.11%
[45, 55)	2.10%	0.60%	0.72%	1.06%	0.16%
55+	0.67%	0.05%	0.39%	0.11%	0.11%

*used as weight to calculate the delta-V level for an average PCP-S

As shown in Table XII-15, the delta-V for a baseline PCP-M is estimated to be 10.43 mph and for a treatment PCP-M is about 8.06 mph. IMA would reduce the crash severity by 2.37 mph. Thus, when both vehicles are moving before an intersection crash, and the crash still occurs, providing a V2V warning does reduce the delta-V of the crash by a noticeable level of 2.37 mph on average.

Table XII-15 Delta-V for an Average PCP-M Crash

	Baseline	**Treatment**
Delta-V (mph)	10.43	8.06

c) *IMA Crashworthiness System Effectiveness*

For IMA crashes as a whole, i.e., PCP-S and PCP-M combined, the average delta-V for IMA crashes is the weighted average of individual delta-Vs for PCP-S and PCP-M. Of the IMA crashes, PCP-S comprised about 38.97 percent of the crashes and PCP-M comprised 61.03 percent of the crashes. Applying these factors to the corresponding individual delta-V shown in Table XII-12 and Table XII-15 derives the average delta-V for IMA crashes. For the baseline IMA crashes, the average delta-V is about 8.17 mph and 7.00 mph for a treatment IMA crash. IMA would reduce the severity of IMA crashes by an average of 1.17 mph delta-V.

The average delta-V of 8.17 mph and 7.00 mph for the baseline and treatment IMA crashes were then input into the injury probability curves to assess the probability that a person would receive a certain level of MAIS injuries. The resulting probabilities for the baseline and treatment groups were used to estimate the reduction rate (i.e., crashworthiness effectiveness) for each of MAIS level.

6. Effectiveness of Left Turn Assist - LTA

a) *LTA Effectiveness Analysis Overview*

LTA is designed to assist the driver of the left turning vehicle in deciding whether to proceed with a left-turn maneuver at an intersection. LTA is not expected to influence the movement of an approaching vehicle. As such, LTA is considered to have no impact on mitigating the severity of the LTA crashes that cannot be avoided and no crashworthiness effectiveness is estimated for LTA in this analysis.

The effectiveness of Left Turn Assist, E_a for LTA, is based on the MiniSim results from 96 volunteer drivers. For each condition, half of drivers experienced an alert (the treatment group) and half did not (the control group). Therefore, for each group, only one set of effectiveness was used for each of the LTA pre-crash conditions.

b) LTA Crash Scenarios

LTA target crashes were categorized into two pre-crash scenarios that correspond to the crash design of MiniSim:

- Left Turn Across Path, Opposite Direction: an approaching vehicle continues to cross straight while the driver continues to move and turns left across the path of the other. This is scenario is abbreviated as LTAP/OD – M for moving.
- Left Turn Across Path, Opposite Direction: an approaching vehicle continues to cross straight while the driver first stops and later turns left across the path of the other. This is scenario is abbreviated as LTAP/OD – S for stopped.

(1) LTAP/OD – M MiniSim Test Scenario

In the LTAP/OD – M simulation, the driver approaches an intersection and is asked to turn left through a green light. There is a stopped truck waiting to turn left, blocking the vision of the subject driver of the next lane over. As the driver enters the intersection, a vehicle approaches the intersection along the side of the stopped truck.

(2) LTAP/OD – S MiniSim Test Scenario

In the LTAP/OD – S condition, the driver approaches the same intersection but the light is red. The driver must stop and then when the light turns green and the driver initiates the turn and reaches 6 mph, the approaching vehicle appears and approaches the intersection with a constant speed of 45 mph.

c) LTA Effectiveness Analysis Assumptions

The effectiveness analysis for LTA crashes identifies some scenarios or conditions where LTA may not be effective or operate properly. In these conditions, such as where the approaching vehicle speed is less than 10 mph, LTA effectiveness is treated as 0. In this very low speed condition, there is the possibility of many false alarms being issued and manufacturers may very well choose not to implement LTA to be active in this condition.

d) LTA Effectiveness Analysis Results

Based on the 96 volunteer driver results, LTA would prevent 75 percent of LTAP-M crashes and 33 percent of LTAP-S crashes. These effectiveness rates then were weighted by their corresponding crash proportion to derive the overall E_a. As shown in Table XI-16, LTA would prevent 48 - 62 percent of LTA crashes. However, according to the current design of LTA, LTA would be activated only when the left turn signal is initiated. Otherwise, you would constantly be given a warning every time a vehicle approached from the other direction.

Based on an SAE study by Richard Ponziani, about 75 percent of drivers would use the turn single when making left turns. Therefore, the derived effectiveness at lower bound was further discounted by 25 percent to 36 percent (48*0.75 = 0.36). This serves as the lower bound of final LTA effectiveness. The agency believes that, if drivers realized the benefit of LTA over time, drivers would be more likely to use the turn single when turning.

Table XII-16 Effectiveness for LTAP-M and LTAP-S

	LTAP-M	LTAP-S
Effectiveness	75%	33%
Crash Proportion*		
Low	0.5570	0.1942
High	0.7140	0.2434

*sum does not add up to100% because some LTA crashes do not belong to either of these conditions

Therefore, the 62 percent is treated as the high bound of the effectiveness. LTA would avoid 36 to 62 percent of the LTA crashes. The wide range addresses the uncertainty for the estimate.

Table XII-17 System Effectiveness

	Low	High
Initial	48%	62%
Final**	36%	62%

**Adjusted for turn signal use but only for lower bound

7. Summary of IMA and LTA effectiveness

Table XII-18 summarizes the crash avoidance and crashworthiness effectiveness for IMA and LTA that were derived from the previous sections. As shown, IMA would prevent 41-55 percent of IMA crashes and LTA would prevent 36-62 percent of LTA crashes.

Table XII-18 System Effectiveness of IMA and LTA

Crash Avoidance (E_a)

	IMA	LTA
Low	41%	36%
High	55%	62%

Crashworthiness (Ew)

Injury Severity	IMA	LTA
MAIS 1	6%	Not Applicable (NA)
MAIS 2	16%	NA
MAIS 3	0%	NA
MAIS 4	50%	NA
MAIS 5	0%	NA
Fatality	0%	NA

C. Fleet communication rate (C_i)

The probability that two vehicles can communicate with each other depends on the number of V2V-equipped vehicles (OBE, ASD, and VAD) and the total number of on-road operational passenger vehicles (i.e., the registered vehicles). The number of V2V-equipped vehicles varies with the technology implementation scenarios. The number of on-road operational passenger vehicles was derived from the estimates of new vehicle sales and the scrappage rate of vehicles. Readers can consult Appendix A for the technology plan and the detailed process of estimating the on-road light vehicle fleet.

The communication rate C_i for two V2V-equipped vehicles encountered at the ith year can be noted as:

Equation XII-10 Communication Rate Calculation

$$\frac{N_i}{O_i} * \frac{N_i}{O_i}, \text{ i.e., } C_i = \left(\frac{N_i}{O_i}\right)^2,$$

Where N_i represents the total number of vehicles that had equipped either OBE or ASD, O_i represents the total on-road light vehicle fleet for year i. Note that any two vehicles that can communicate with each other should be treated as selection without replacement. In other words, C_i should be $\frac{N_i}{O_i} * \frac{N_i\text{-}1}{O_i\text{-}1}$. However, N_i and O_i are large. The two values, $\frac{N_i}{O_i} * \frac{N_i\text{-}1}{O_i\text{-}1}$ and $\left(\frac{N_i}{O_i}\right)^2$, are almost identical. For simplicity, the square form is used for calculating the communication rate C_i. Also note that the difference in C_i among geographic areas and driving patterns by different age of vehicles were not examined in the analysis since these factors are not expected to impact the overall communication rate at the national level.

Table XIII-5 shows the communication rates from 2020 to 2059 for the three technology implementation scenarios. As shown, the communication rates for Scenarios 1 and 2 accelerate faster as time passes. It will take 12 years to reach the 50 percent communication rate for Scenario 1, but only five years later (i.e., at year 17), the communication rate would reach 75 percent. Scenario 2 would reach the 50 and 75 communication rates three years later than Scenario 1. As expected, the communication rate for Scenario 3 is low. The disparity among these three scenarios demonstrates the impact of the implementation pace on communication rate, and thus on benefits. Note that the V2V benefit can be realized only when one of the involved vehicles is equipped with safety applications. The communication rate for Scenario 2 represents the communication rate between two vehicles where at least one of them had safety applications.

The communication rates were further segregated by vehicle type (i.e., PCs and LTVs). Communication rate for PCs is the probability for PCs communicating among PCs plus the probability that PCs are communicating with LTVs. Similarly, communication rate for LTVs is the probability of LTVs communicating among LTVs plus the probability of LTVs communicating with PCs. The communication rates for PCs and LTVs are later used to divide the overall annual benefits into PC and LTV portions of benefits for calculating benefits by vehicle model year (MY). Table XIII-6 shows the communication rates by vehicle types.

D. Projected benefits of V2V technology

This section provides the undiscounted preliminary annual maximum benefits, annual benefit by calendar years. Benefits can be derived by multiplying these three factors: target population, the effectiveness, and the communication rates as mathematically noted in using Equation XII-1. The maximum represent the benefits when all on-road passenger vehicles were equipped with DSRC and IMA and LTA safety applications. The maximum benefits would be achievable under Scenarios 1 and 2 but not Scenario 3. The maximum benefits are discussed first and followed by three parallel sections, each for a scenario, describing the annual estimated benefits per calendar year.

1. Maximum annual estimated benefits

Table XII-19 shows the non-discounted annual preliminary maximum estimated benefits based on all passenger vehicles (PVs) being equipped with only IMA and LTA and the communication rate reaches 100 percent among PVs. The maximum estimated benefit would be identical for the first two technology implementation scenarios. The difference among the two scenarios is when (i.e., how fast) the maximum estimated benefit can be achieved. The third scenario would not achieve this maximum benefit level since the communication rate for this scenario would not reach 100 percent. As shown, IMA and LTA combined would prevent 412,512 to 592,230 crashes, save 777 to 1,083 lives, reduce 191,202 to 270,011 MAIS 1-5 injuries, and eliminate 511,118 to 728,173 property-damage-only vehicles (PDOVs).

Of the above estimated benefits, IMA would prevent 310,451 to 416,458 crashes, save 671 to 900 lives, reduce 136,959 to 176,593 MAIS 1-5 injuries, and eliminate 399,431 to 535,823 PDOVs. LTA would avoid 102,061 to 175,772 crashes, save 106 to 183 lives, reduce 54,243 to 93,418 MAIS 1-5 injuries, and eliminate 111,687 to 192,350 PDOVs.

Table XII-19 Non-Discounted Annual Preliminary Maximum Estimated Benefit Summary All Passenger Vehicles Equipped With V2V Technology

	IMA		LTA		Combined	
	Low	High	Low	High	Low	High
Crashes	310,451	416,458	102,061	175,772	412,512	592,230
Fatalities	671	900	106	183	777	1,083
MAIS 1-5 Injuries	136,959	176,593	54,243	93,418	191,202	270,011
PDOV**	399,431	535,823	111,687	192,350	511,118	728,173

*Based on only IMA and LTA safety applications

**Property Damage Only Vehicles

2. Annual Estimated Benefits by Calendar Year

a) Scenario 1

Table XIII-7 shows the undiscounted preliminary estimated benefits by calendar year, separately for the three technology implementation scenarios. As expected, the potential benefits realized by IMA and LTA accrue more slowly for the first few years due to the slow build-up of communication rate among PVs. As shown, at Year 2020, the first year of technology implementation, IMA and LTA could potentially prevent 248-355 crashes and potentially avoid 412,000 to 592,000 crashes annually after 36 years of implementation.

b) Scenario 2

Table XIII-8 shows the undiscounted preliminary benefit estimates by calendar year for Scenario 2. As shown, at Year 2020, the first year of technology implementation, this scenario could potentially prevent 124 to 178 crashes, about 50 percent of the level that can be achieved by Scenario 1. After 10 years of implementation, in Year 2030, this scenario could potentially prevent 121,526 to 174,471 crashes, about 80 percent of the level in Scenario 1. Eventually, Scenario 2 would reach a similar level of annual benefits as Scenario 1, after 38 years of implementation in Year 2058 and potentially prevent 412,000 to 591,000 crashes annually.

c) Scenario 3

Table XIII-9 shows the undiscounted preliminary benefit estimates by calendar year for this scenario. As shown, Scenario 3 appears that it would have negligible impact on safety for the first year of implementation of the IMA and LTA safety applications. Starting in the second year, the benefits for this scenario are estimated to gradually increase. After 38 years of implementation, in Year 2058, a potential of 25,782 to 37,014 crashes could be prevented, 49 to 68 lives could be saved, and 11,950 to 16,876 MAIS 1-5 injuries would be reduced. The preliminary benefits from Scenario 3 are about six percent of the maximum benefits that could be achieved by Scenarios 1 and 2. The disparity in preliminary benefits demonstrates that in order to realize the full potential of V2V technology, achieving full implementation over time is critical.

XIII. Appendix A: Tables

Table XIII-1 RSE Data Cost per Vehicle

	Scenario 1	Scenario 2	Scenario 3
Year 4	$11.63	$10.74	$8.58
Year 5	$5.37	$4.93	$3.37
Year 6	$5.98	$5.45	$3.89
Year 7	$6.60	$5.98	$4.44
Year 8	$7.21	$6.49	$6.49
Year 9	$7.83	$6.98	$6.98
Year 10	$8.45	$7.49	$7.49
Year 11	$9.06	$7.96	$7.96
Year 12	$9.68	$8.43	$8.43
Year 13	$10.29	$8.90	$8.90
Year 14	$10.91	$9.38	$9.38
Year 15	$11.52	$9.81	$9.81
Year 16	$10.53	$8.88	$8.88
Year 17	$9.24	$7.72	$7.72
Year 18	$9.24	$7.65	$7.65
Year 19	$15.78	$12.97	$12.97
Year 20	$11.11	$9.04	$9.04
Year 21	$11.11	$8.94	$8.94
Year 22	$11.11	$8.81	$8.81
Year 23	$11.11	$9.11	$9.11
Year 24	$11.11	$9.06	$9.06
Year 25	$11.11	$9.01	$9.01
Year 26	$11.11	$8.96	$8.96
Year 27	$11.11	$8.91	$8.91
Year 28	$11.11	$8.86	$8.86
Year 29	$11.11	$8.81	$8.81
Year 30	$11.11	$8.77	$8.77
Year 31	$10.17	$7.99	$7.98
Year 32	$9.24	$7.25	$7.25
Year 33	$9.24	$7.25	$7.25
Year 34	$15.78	$12.39	$12.39
Year 35	$11.11	$8.72	$8.72
Year 36	$11.11	$8.72	$8.72
Year 37	$11.11	$8.72	$8.72
Year 38	$11.11	$8.72	$8.72
Year 39	$11.11	$8.72	$8.72
Year 40	$11.11	$8.72	$8.72

Table XIII-2 PCP-S Scenario - Delta-V* Distribution by Approaching Vehicle Traveling Speed Baseline (Without V2V)

	Left Side Impact					Right Side Impact				
Delta-V	Approaching Vehicle Travel Speed (mph)					Approaching Vehicle Travel Speed (mph)				
(mph)	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+
Separating Distance: 3-5 Meters										
0.75	8.0%	6.6%	6.1%	6.5%	6.6%		6.6%	6.1%	6.5%	6.6%
2.25	25.2%	21.2%	20.4%	21.7%	19.7%		21.1%	20.5%	21.8%	19.6%
3.75	43.4%	42.5%	43.0%	40.6%	41.7%		42.3%	43.2%	40.8%	41.6%
5.25	9.1%	6.6%	7.5%	9.1%	9.7%		6.6%	7.6%	9.1%	9.7%
6.75	3.8%	0.0%	0.0%	0.0%	0.0%		0.0%	0.0%	0.0%	0.0%
8.25	3.6%	0.0%	0.0%	0.0%	0.0%		0.0%	0.0%	0.0%	0.0%
9.75	3.6%	0.0%	0.0%	0.0%	0.0%		0.0%	0.0%	0.0%	0.0%
11.25	3.1%	0.0%	0.0%	0.0%	0.0%		0.0%	0.0%	0.0%	0.0%
12.75	0.2%	7.3%	0.0%	0.0%	0.0%		7.2%	0.0%	0.0%	0.0%
14.25	0.0%	7.1%	0.0%	0.0%	0.0%		7.0%	0.0%	0.0%	0.0%
15.75	0.0%	6.4%	0.0%	0.0%	0.0%		6.4%	0.0%	0.0%	0.0%
17.25	0.0%	2.3%	5.4%	0.0%	0.0%		2.3%	5.4%	0.0%	0.0%
18.75	0.0%	0.0%	7.1%	0.0%	0.0%		0.0%	7.1%	0.0%	0.0%
20.25	0.0%	0.0%	7.2%	0.0%	0.0%		0.0%	7.3%	0.0%	0.0%
21.75	0.0%	0.0%	3.2%	4.2%	0.0%		0.0%	3.3%	4.2%	0.0%
23.25	0.0%	0.0%	0.0%	18.0%	22.3%		0.0%	0.0%	18.1%	22.2%
Separating Distance: 4 Meters										
0.75	8.0%	5.7%	5.1%	4.3%	4.2%	8.3%	5.8%	5.1%	4.6%	4.3%
2.25	24.2%	21.7%	21.0%	20.5%	19.3%	25.3%	22.2%	20.7%	21.6%	19.4%
3.75	46.1%	46.8%	45.5%	44.2%	45.5%	48.2%	47.8%	45.0%	46.5%	45.9%
5.25	8.5%	6.7%	7.1%	9.7%	10.4%	8.9%	6.9%	7.1%	10.2%	10.5%
6.75	3.8%	0.0%	0.0%	0.0%	0.0%	4.0%	0.0%	0.0%	0.0%	0.0%
8.25	3.3%	0.0%	0.0%	0.0%	0.0%	3.4%	0.0%	0.0%	0.0%	0.0%
9.75	2.8%	0.0%	0.0%	0.0%	0.0%	2.9%	0.0%	0.0%	0.0%	0.0%
11.25	3.0%	0.0%	0.0%	0.0%	0.0%	3.1%	0.0%	0.0%	0.0%	0.0%
12.75	0.1%	6.3%	0.0%	0.0%	0.0%	0.1%	6.4%	0.0%	0.0%	0.0%
14.25	0.0%	5.9%	0.0%	0.0%	0.0%	0.0%	6.1%	0.0%	0.0%	0.0%
15.75	0.0%	5.4%	0.0%	0.0%	0.0%	0.0%	5.6%	0.0%	0.0%	0.0%
17.25	0.0%	1.4%	5.3%	0.0%	0.0%	0.0%	1.4%	5.3%	0.0%	0.0%
18.75	0.0%	0.0%	6.2%	0.0%	0.0%	0.0%	0.0%	6.1%	0.0%	0.0%
20.25	0.0%	0.0%	6.9%	0.0%	0.0%	0.0%	0.0%	6.8%	0.0%	0.0%
21.75	0.0%	0.0%	2.8%	3.8%	0.0%	0.0%	0.0%	2.8%	3.9%	0.0%
23.25	0.0%	0.0%	0.0%	17.5%	20.6%	0.0%	0.0%	0.0%	18.4%	20.8%
Separating Distance: 5-8 Meters										
0.75	4.9%	2.4%	1.0%	0.7%	0.0%	4.7%	2.1%	0.9%	0.6%	0.0%
2.25	23.5%	15.8%	9.4%	9.5%	10.3%	22.3%	13.8%	8.6%	8.7%	8.8%
3.75	33.6%	30.4%	31.4%	33.3%	28.4%	31.8%	26.5%	28.5%	30.5%	24.3%
5.25	31.7%	38.9%	46.7%	42.7%	45.5%	30.1%	33.9%	42.4%	39.2%	38.8%
6.75	4.2%	6.0%	4.6%	6.0%	7.9%	4.0%	5.2%	4.1%	5.5%	6.8%
8.25	0.7%	0.0%	0.0%	0.0%	0.0%	0.7%	0.0%	0.0%	0.0%	0.0%
9.75	0.7%	0.0%	0.0%	0.0%	0.0%	0.6%	0.0%	0.0%	0.0%	0.0%
11.25	0.7%	0.0%	0.0%	0.0%	0.0%	0.6%	0.0%	0.0%	0.0%	0.0%
12.75	0.0%	1.5%	0.0%	0.0%	0.0%	0.0%	1.3%	0.0%	0.0%	0.0%
14.25	0.0%	2.2%	0.0%	0.0%	0.0%	0.0%	1.9%	0.0%	0.0%	0.0%

	Left Side Impact					Right Side Impact				
Delta-V	Approaching Vehicle Travel Speed (mph)					Approaching Vehicle Travel Speed (mph)				
(mph)	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+
15.75	0.0%	2.3%	0.0%	0.0%	0.0%	0.0%	2.0%	0.0%	0.0%	0.0%
17.25	0.0%	0.4%	2.1%	0.0%	0.0%	0.0%	0.4%	1.9%	0.0%	0.0%
18.75	0.0%	0.0%	2.9%	0.0%	0.0%	0.0%	0.0%	2.7%	0.0%	0.0%
20.25	0.0%	0.0%	0.8%	0.0%	0.0%	0.0%	0.0%	0.7%	0.0%	0.0%
21.75	0.0%	0.0%	1.0%	0.7%	0.0%	0.0%	0.0%	0.9%	0.6%	0.0%
23.25	0.0%	0.0%	0.0%	7.2%	7.9%	0.0%	0.0%	0.0%	6.6%	6.8%

*equivalent to half of the crash impact speed

Source: SIM simulation output

Table XIII-3 PCP-S Scenario - Delta-V* Distribution by Approaching Vehicle Traveling Speed Treatment (With V2V)

	Left Side Impact					Right Side Impact				
Delta-V	Approaching Vehicle Speed (mph)					Approaching Vehicle Speed (mph)				
(mph)	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+
Separating Distance: 3-5 Meters										
0.75	16.7%	15.8%	16.5%	15.8%	16.3%		15.8%	16.5%	15.8%	16.3%
2.25	31.4%	30.6%	29.6%	31.5%	30.9%		30.6%	29.6%	31.5%	30.9%
3.75	29.7%	26.4%	27.5%	28.2%	27.2%		26.4%	27.5%	28.2%	27.2%
5.25	7.8%	4.5%	5.0%	3.6%	5.1%		4.5%	5.0%	3.6%	5.1%
6.75	3.9%	0.0%	0.0%	0.0%	0.0%		0.0%	0.0%	0.0%	0.0%
8.25	3.9%	0.0%	0.0%	0.0%	0.0%		0.0%	0.0%	0.0%	0.0%
9.75	3.8%	0.0%	0.0%	0.0%	0.0%		0.0%	0.0%	0.0%	0.0%
11.25	2.7%	0.0%	0.0%	0.0%	0.0%		0.0%	0.0%	0.0%	0.0%
12.75	0.2%	7.9%	0.0%	0.0%	0.0%		7.9%	0.0%	0.0%	0.0%
14.25	0.0%	7.3%	0.0%	0.0%	0.0%		7.3%	0.0%	0.0%	0.0%
15.75	0.0%	5.6%	0.0%	0.0%	0.0%		5.6%	0.0%	0.0%	0.0%
17.25	0.0%	1.9%	5.3%	0.0%	0.0%		1.9%	5.3%	0.0%	0.0%
18.75	0.0%	0.0%	6.5%	0.0%	0.0%		0.0%	6.5%	0.0%	0.0%
20.25	0.0%	0.0%	7.2%	0.0%	0.0%		0.0%	7.2%	0.0%	0.0%
21.75	0.0%	0.0%	2.4%	4.5%	0.0%		0.0%	2.4%	4.5%	0.0%
23.25	0.0%	0.0%	0.0%	16.4%	20.4%		0.0%	0.0%	16.4%	20.4%
Separating Distance: 4 Meters										
0.75	16.2%	16.1%	12.5%	13.3%	13.5%	16.2%	16.1%	12.5%	13.3%	13.5%
2.25	32.3%	31.2%	31.2%	32.5%	31.2%	32.3%	31.2%	31.2%	32.5%	31.2%
3.75	30.2%	28.0%	29.1%	28.5%	28.4%	30.2%	28.0%	29.1%	28.5%	28.4%
5.25	8.1%	5.7%	6.2%	5.8%	6.6%	8.1%	5.7%	6.2%	5.8%	6.6%
6.75	3.6%	0.0%	0.0%	0.0%	0.0%	3.6%	0.0%	0.0%	0.0%	0.0%
8.25	3.5%	0.0%	0.0%	0.0%	0.0%	3.5%	0.0%	0.0%	0.0%	0.0%
9.75	3.1%	0.0%	0.0%	0.0%	0.0%	3.1%	0.0%	0.0%	0.0%	0.0%
11.25	3.0%	0.0%	0.0%	0.0%	0.0%	3.0%	0.0%	0.0%	0.0%	0.0%
12.75	0.1%	6.9%	0.0%	0.0%	0.0%	0.1%	6.9%	0.0%	0.0%	0.0%
14.25	0.0%	5.6%	0.0%	0.0%	0.0%	0.0%	5.6%	0.0%	0.0%	0.0%
15.75	0.0%	5.2%	0.0%	0.0%	0.0%	0.0%	5.2%	0.0%	0.0%	0.0%
17.25	0.0%	1.5%	5.3%	0.0%	0.0%	0.0%	1.5%	5.3%	0.0%	0.0%
18.75	0.0%	0.0%	6.5%	0.0%	0.0%	0.0%	0.0%	6.5%	0.0%	0.0%
20.25	0.0%	0.0%	6.4%	0.0%	0.0%	0.0%	0.0%	6.4%	0.0%	0.0%
21.75	0.0%	0.0%	2.9%	4.1%	0.0%	0.0%	0.0%	2.9%	4.1%	0.0%
23.25	0.0%	0.0%	0.0%	15.8%	20.2%	0.0%	0.0%	0.0%	15.8%	20.2%
Separating Distance: 5-8 Meters										
0.75	9.5%	7.4%	4.9%	0.7%	2.1%	9.5%	7.4%	4.9%	0.7%	2.1%
2.25	35.8%	30.2%	31.5%	21.0%	22.7%	35.8%	30.2%	31.5%	21.0%	22.7%
3.75	34.9%	37.6%	31.0%	37.0%	39.2%	34.9%	37.6%	31.0%	37.0%	39.2%
5.25	14.8%	16.3%	23.4%	26.1%	22.7%	14.8%	16.3%	23.4%	26.1%	22.7%
6.75	2.2%	1.6%	1.1%	2.2%	3.1%	2.2%	1.6%	1.1%	2.2%	3.1%
8.25	1.0%	0.0%	0.0%	0.0%	0.0%	1.0%	0.0%	0.0%	0.0%	0.0%
9.75	1.0%	0.0%	0.0%	0.0%	0.0%	1.0%	0.0%	0.0%	0.0%	0.0%
11.25	0.7%	0.0%	0.0%	0.0%	0.0%	0.7%	0.0%	0.0%	0.0%	0.0%
12.75	0.0%	2.3%	0.0%	0.0%	0.0%	0.0%	2.3%	0.0%	0.0%	0.0%
14.25	0.0%	2.3%	0.0%	0.0%	0.0%	0.0%	2.3%	0.0%	0.0%	0.0%

	Left Side Impact					Right Side Impact				
Delta-V	Approaching Vehicle Speed (mph)					Approaching Vehicle Speed (mph)				
(mph)	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+	[10, 25)	[25, 35)	[35, 45)	[45, 55)	55+
15.75	0.0%	1.9%	0.0%	0.0%	0.0%	0.0%	1.9%	0.0%	0.0%	0.0%
17.25	0.0%	0.4%	3.8%	0.0%	0.0%	0.0%	0.4%	3.8%	0.0%	0.0%
18.75	0.0%	0.0%	2.2%	0.0%	0.0%	0.0%	0.0%	2.2%	0.0%	0.0%
20.25	0.0%	0.0%	1.6%	0.0%	0.0%	0.0%	0.0%	1.6%	0.0%	0.0%
21.75	0.0%	0.0%	0.5%	0.7%	0.0%	0.0%	0.0%	0.5%	0.7%	0.0%
23.25	0.0%	0.0%	0.0%	12.3%	10.3%	0.0%	0.0%	0.0%	12.3%	10.3%

*equivalent to half of the crash impact speed
Source: SIM simulation output

Table XIII-4 PCP-M Scenario - Delta-V* Distribution by Approaching Vehicle Speed

	Baseline					**Treatment**				
Delta-V	**Approaching Vehicle Speed (mph)**					**Approaching Vehicle Speed (mph)**				
(mph)	**[10, 25)**	**[25, 35)**	**[35, 45)**	**[45, 55)**	**55+**	**[10, 25)**	**[25, 35)**	**[35, 45)**	**[45, 55)**	**55+**
Driver Vehicle Speed **[10, 25)**										
0.75	0.5%	0.5%	0.2%	0.1%	0.0%	4.4%	1.6%	0.7%	0.4%	0.0%
2.25	1.8%	1.8%	1.6%	1.4%	0.9%	13.6%	8.8%	5.6%	4.5%	2.5%
3.75	5.4%	5.4%	5.6%	5.4%	5.0%	21.2%	20.2%	16.5%	15.1%	12.2%
5.25	18.2%	18.0%	18.4%	18.7%	18.7%	22.4%	24.3%	24.1%	23.6%	21.3%
6.75	20.5%	20.6%	20.9%	20.9%	21.1%	18.1%	20.9%	24.0%	25.0%	25.2%
8.25	20.3%	20.6%	20.1%	20.1%	20.4%	12.3%	14.4%	17.4%	19.0%	22.8%
9.75	18.8%	18.8%	18.5%	18.7%	19.1%	6.4%	7.6%	9.1%	9.6%	12.7%
11.25	14.1%	14.0%	14.1%	14.1%	14.2%	1.7%	2.2%	2.5%	2.8%	3.2%
12.75	0.5%	0.5%	0.5%	0.5%	0.5%	0.0%	0.0%	0.1%	0.1%	0.1%
14.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
15.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
17.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
18.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
20.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
21.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
23.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Driver Vehicle Speed **[25, 35)**										
0.75	0.1%	0.0%	0.0%	0.0%	0.0%	0.6%	0.0%	0.0%	0.0%	0.0%
2.25	0.2%	0.0%	0.0%	0.0%	0.0%	2.8%	0.1%	0.0%	0.0%	0.0%
3.75	0.6%	0.2%	0.0%	0.0%	0.0%	6.5%	0.9%	0.1%	0.0%	0.0%
5.25	1.2%	1.0%	0.5%	0.1%	0.0%	11.7%	4.8%	1.4%	0.5%	0.0%
6.75	2.3%	2.3%	1.8%	1.2%	0.3%	16.0%	12.8%	6.9%	4.2%	0.9%
8.25	4.4%	4.7%	4.4%	4.1%	2.9%	17.7%	20.6%	17.1%	14.0%	7.7%
9.75	8.4%	8.4%	8.4%	8.4%	8.0%	16.9%	23.2%	25.5%	25.1%	21.7%
11.25	15.2%	15.4%	15.7%	15.8%	16.5%	14.2%	19.1%	24.1%	27.8%	30.3%
12.75	26.7%	26.6%	27.2%	27.6%	28.3%	9.1%	12.0%	15.8%	18.1%	24.9%
14.25	22.8%	23.1%	23.3%	23.9%	24.9%	3.6%	5.4%	7.6%	8.5%	11.9%
15.75	15.4%	15.7%	16.0%	16.2%	16.3%	0.8%	1.2%	1.4%	1.8%	2.6%
17.25	2.6%	2.5%	2.7%	2.7%	2.7%	0.0%	0.0%	0.0%	0.0%	0.0%
18.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
20.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
21.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
23.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Driver Vehicle Speed **[35, 45)**										
0.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%
2.25	0.1%	0.0%	0.0%	0.0%	0.0%	0.5%	0.0%	0.0%	0.0%	0.0%
3.75	0.2%	0.0%	0.0%	0.0%	0.0%	1.6%	0.0%	0.0%	0.0%	0.0%
5.25	0.5%	0.0%	0.0%	0.0%	0.0%	3.8%	0.1%	0.0%	0.0%	0.0%
6.75	1.1%	0.2%	0.0%	0.0%	0.0%	6.8%	0.8%	0.0%	0.0%	0.0%
8.25	1.9%	1.1%	0.3%	0.0%	0.0%	10.9%	3.2%	0.8%	0.1%	0.0%
9.75	2.8%	2.7%	1.4%	0.7%	0.0%	14.5%	9.1%	3.5%	1.3%	0.0%
11.25	4.8%	4.6%	4.0%	3.1%	1.0%	16.0%	16.0%	10.5%	6.6%	2.2%
12.75	7.1%	7.6%	7.6%	7.0%	4.7%	14.2%	21.3%	19.1%	16.4%	9.1%
14.25	11.1%	11.4%	11.9%	11.9%	11.2%	13.0%	21.0%	24.7%	24.2%	21.4%
15.75	16.2%	17.2%	17.8%	18.1%	19.4%	9.6%	15.2%	20.7%	25.8%	27.4%

	Baseline					**Treatment**				
Delta-V	**Approaching Vehicle Speed (mph)**					**Approaching Vehicle Speed (mph)**				
(mph)	**[10, 25)**	**[25, 35)**	**[35, 45)**	**[45, 55)**	**55+**	**[10, 25)**	**[25, 35)**	**[35, 45)**	**[45, 55)**	**55+**
17.25	22.0%	22.2%	23.3%	24.1%	25.7%	5.6%	8.7%	12.9%	16.4%	24.0%
18.75	18.5%	18.7%	19.3%	20.1%	21.4%	2.6%	3.9%	6.1%	7.3%	12.6%
20.25	11.4%	11.7%	11.7%	12.2%	13.3%	0.8%	1.0%	1.7%	1.9%	3.2%
21.75	2.4%	2.5%	2.6%	2.8%	3.2%	0.0%	0.0%	0.0%	0.0%	0.0%
23.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Driver Vehicle Speed **[45, 55)**										
0.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
2.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
3.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.2%	0.0%	0.0%	0.0%	0.0%
5.25	0.1%	0.0%	0.0%	0.0%	0.0%	0.7%	0.0%	0.0%	0.0%	0.0%
6.75	0.4%	0.0%	0.0%	0.0%	0.0%	1.9%	0.0%	0.0%	0.0%	0.0%
8.25	0.6%	0.0%	0.0%	0.0%	0.0%	4.1%	0.0%	0.0%	0.0%	0.0%
9.75	1.3%	0.2%	0.0%	0.0%	0.0%	6.6%	0.2%	0.0%	0.0%	0.0%
11.25	2.1%	0.8%	0.1%	0.0%	0.0%	9.8%	1.8%	0.1%	0.0%	0.0%
12.75	3.3%	2.3%	0.8%	0.2%	0.0%	12.7%	5.1%	1.3%	0.4%	0.0%
14.25	4.8%	4.6%	2.8%	1.5%	0.1%	14.6%	10.9%	5.1%	2.4%	0.2%
15.75	7.0%	7.0%	6.2%	4.8%	1.9%	14.0%	17.8%	10.9%	6.8%	2.6%
17.25	9.5%	9.9%	9.7%	9.6%	6.8%	11.9%	20.0%	18.8%	15.6%	8.2%
18.75	12.9%	13.6%	14.4%	14.9%	14.3%	9.9%	17.7%	23.5%	22.4%	18.4%
20.25	16.4%	17.2%	18.7%	19.6%	21.4%	6.9%	13.2%	19.5%	25.2%	27.5%
21.75	18.6%	19.4%	20.9%	22.0%	24.2%	4.0%	8.0%	12.4%	16.4%	24.6%
23.25	23.0%	25.0%	26.4%	27.4%	31.4%	2.8%	5.2%	8.2%	10.7%	18.5%
Driver Vehicle Traveling Speed **55+**										
0.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
2.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
3.75	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
5.25	0.0%	0.0%	0.0%	0.0%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%
6.75	0.1%	0.0%	0.0%	0.0%	0.0%	0.3%	0.0%	0.0%	0.0%	0.0%
8.25	0.2%	0.0%	0.0%	0.0%	0.0%	0.9%	0.0%	0.0%	0.0%	0.0%
9.75	0.5%	0.0%	0.0%	0.0%	0.0%	2.2%	0.0%	0.0%	0.0%	0.0%
11.25	0.8%	0.0%	0.0%	0.0%	0.0%	3.6%	0.0%	0.0%	0.0%	0.0%
12.75	1.5%	0.1%	0.0%	0.0%	0.0%	5.9%	0.1%	0.0%	0.0%	0.0%
14.25	2.4%	0.5%	0.0%	0.0%	0.0%	8.5%	0.5%	0.1%	0.0%	0.0%
15.75	3.6%	1.7%	0.3%	0.0%	0.0%	10.5%	2.4%	0.2%	0.0%	0.0%
17.25	5.0%	3.8%	1.6%	0.5%	0.0%	12.5%	5.7%	1.6%	0.1%	0.0%
18.75	6.5%	6.6%	4.2%	2.4%	0.4%	13.6%	11.7%	4.3%	1.6%	0.0%
20.25	8.8%	9.2%	8.3%	6.6%	2.6%	11.9%	16.8%	10.4%	5.3%	0.4%
21.75	10.7%	11.4%	12.1%	11.4%	7.9%	9.9%	19.8%	18.2%	13.5%	2.6%
23.25	60.0%	66.7%	73.5%	79.2%	89.2%	20.2%	42.9%	65.2%	79.5%	97.0%

*equivalent to half of the crash impact speed
Source: SIM simulation output

Table XIII-5 Passenger Vehicle Fleet Communication Rates by Technology Implementation Scenarios

Year of Implementation	Calendar Year	Scenario 1	Scenario 2	Scenario 3
1	2020	0.06%	0.03%	0.00%
2	2021	0.51%	0.26%	0.02%
3	2022	2.46%	0.95%	0.09%
4	2023	5.69%	2.20%	0.22%
5	2024	11.01%	4.08%	0.39%
6	2025	17.45%	6.66%	0.61%
7	2026	24.60%	10.02%	0.86%
8	2027	29.92%	14.19%	1.15%
9	2028	35.45%	18.88%	1.46%
10	2029	41.09%	23.99%	1.81%
11	2030	46.77%	29.46%	2.17%
12	2031	52.36%	35.17%	2.53%
13	2032	57.80%	41.02%	2.91%
14	2033	62.97%	46.90%	3.28%
15	2034	67.86%	52.75%	3.64%
16	2035	72.38%	58.44%	3.98%
17	2036	76.51%	63.87%	4.30%
18	2037	80.19%	68.92%	4.60%
19	2038	83.42%	73.51%	4.86%
20	2039	86.16%	77.59%	5.09%
21	2040	88.47%	81.13%	5.28%
22	2041	90.42%	84.16%	5.45%
23	2042	92.01%	86.70%	5.57%
24	2043	93.34%	88.83%	5.68%
25	2044	94.47%	90.62%	5.77%
26	2045	95.37%	92.10%	5.85%
27	2046	96.14%	93.35%	5.91%
28	2047	96.85%	94.45%	5.97%
29	2048	97.48%	95.43%	6.02%
30	2049	98.06%	96.29%	6.06%
31	2050	98.51%	97.02%	6.10%
32	2051	98.90%	97.63%	6.14%
33	2052	99.19%	98.16%	6.17%
34	2053	99.42%	98.62%	6.19%
35	2054	99.63%	99.00%	6.21%
36	2055	99.78%	99.32%	6.23%
37	2056	99.91%	99.57%	6.24%
38	2057	99.97%	99.73%	6.25%
39	2058	100.00%	99.84%	6.25%
40	2059	100.00%	99.91%	6.25%

Table XIII-6 Passenger Vehicle Fleet Communication Rate by Vehicle Types* and Technology Implementation Scenarios

Year of	Calendar	Scenario 1		Scenario 2		Scenario 3	
Implementation	Year	PCs	LTVs	PCs	LTVs	PCs	LTVs
1	2020	0.03%	0.03%	0.02%	0.01%	0.00%	0.00%
2	2021	0.28%	0.23%	0.14%	0.12%	0.01%	0.01%
3	2022	1.34%	1.12%	0.52%	0.43%	0.05%	0.04%
4	2023	3.10%	2.58%	1.20%	1.00%	0.12%	0.10%
5	2024	6.01%	5.00%	2.23%	1.85%	0.21%	0.18%
6	2025	9.54%	7.91%	3.64%	3.02%	0.33%	0.28%
7	2026	13.47%	11.12%	5.48%	4.54%	0.47%	0.39%
8	2027	16.41%	13.51%	7.76%	6.43%	0.63%	0.52%
9	2028	19.47%	15.99%	10.33%	8.55%	0.80%	0.66%
10	2029	22.59%	18.50%	13.14%	10.85%	0.99%	0.82%
11	2030	25.74%	21.02%	16.15%	13.31%	1.19%	0.98%
12	2031	28.85%	23.51%	19.30%	15.87%	1.39%	1.14%
13	2032	31.87%	25.93%	22.54%	18.48%	1.60%	1.31%
14	2033	34.74%	28.23%	25.81%	21.09%	1.81%	1.47%
15	2034	37.44%	30.41%	29.07%	23.68%	2.01%	1.63%
16	2035	39.94%	32.44%	32.25%	26.19%	2.20%	1.78%
17	2036	42.20%	34.31%	35.28%	28.59%	2.38%	1.92%
18	2037	44.19%	36.01%	38.10%	30.82%	2.55%	2.05%
19	2038	45.90%	37.52%	40.64%	32.87%	2.69%	2.17%
20	2039	47.32%	38.84%	42.88%	34.71%	2.81%	2.28%
21	2040	48.48%	39.99%	44.80%	36.33%	2.91%	2.37%
22	2041	49.43%	40.99%	46.41%	37.75%	3.00%	2.45%
23	2042	50.09%	41.93%	47.64%	39.06%	3.05%	2.52%
24	2043	50.59%	42.75%	48.62%	40.21%	3.10%	2.58%
25	2044	50.99%	43.48%	49.39%	41.23%	3.13%	2.64%
26	2045	51.26%	44.11%	49.99%	42.11%	3.16%	2.69%
27	2046	51.46%	44.68%	50.45%	42.90%	3.18%	2.73%
28	2047	51.63%	45.22%	50.83%	43.62%	3.20%	2.77%
29	2048	51.77%	45.71%	51.14%	44.29%	3.21%	2.81%
30	2049	51.89%	46.17%	51.39%	44.90%	3.22%	2.84%
31	2050	51.95%	46.57%	51.57%	45.45%	3.23%	2.87%
32	2051	51.98%	46.92%	51.69%	45.94%	3.24%	2.90%
33	2052	51.97%	47.21%	51.77%	46.39%	3.24%	2.93%
34	2053	51.95%	47.47%	51.82%	46.80%	3.24%	2.95%
35	2054	51.93%	47.70%	51.85%	47.15%	3.24%	2.97%
36	2055	51.89%	47.89%	51.86%	47.46%	3.24%	2.99%
37	2056	51.85%	48.05%	51.84%	47.73%	3.24%	3.00%
38	2057	50.40%	49.57%	51.80%	47.93%	3.24%	3.01%
39	2058	50.36%	49.64%	51.75%	48.09%	3.23%	3.02%
40	2059	50.33%	49.67%	51.70%	48.21%	3.23%	3.02%

*The communication rates are used to discern the portion of benefit that would attributed to a specific vehicle type – a process for deriving the benefit for a specific model year of vehicles in order to measure cost-effectiveness.

Table XIII-7 Preliminary Annual Benefits* Estimates of IMA and LTA

Scenario 1

	Calendar	Crash Prevented		Fatalities Eliminated		MAIS 1-5 Injuries		PDOV	
Year	**Year**	**Low**	**High**	**Low**	**High**	**Low**	**High**	**Low**	**High**
1	2020	248	355	0.47	0.65	115	162	307	437
2	2021	2,104	3,020	3.96	5.52	975	1,377	2,607	3,714
3	2022	10,148	14,569	19.11	26.64	4,704	6,642	12,574	17,913
4	2023	23,472	33,698	44.21	61.62	10,879	15,364	29,083	41,433
5	2024	45,418	65,205	85.55	119.24	21,051	29,728	56,274	80,172
6	2025	71,983	103,344	135.59	188.98	33,365	47,117	89,190	127,066
7	2026	101,478	145,689	191.14	266.42	47,036	66,423	125,735	179,131
8	2027	123,424	177,195	232.48	324.03	57,208	80,787	152,927	217,869
9	2028	146,236	209,946	275.45	383.92	67,781	95,719	181,191	258,137
10	2029	169,501	243,347	319.27	445.00	78,565	110,948	210,018	299,206
11	2030	192,932	276,986	363.40	506.52	89,425	126,284	239,050	340,567
12	2031	215,991	310,092	406.84	567.06	100,113	141,378	267,621	381,271
13	2032	238,432	342,309	449.11	625.97	110,515	156,066	295,426	420,884
14	2033	259,759	372,927	489.28	681.97	120,400	170,026	321,851	458,531
15	2034	279,931	401,887	527.27	734.92	129,750	183,229	346,845	494,138
16	2035	298,576	428,656	562.39	783.88	138,392	195,434	369,947	527,052
17	2036	315,613	453,115	594.48	828.60	146,289	206,585	391,056	557,125
18	2037	330,793	474,909	623.08	868.46	153,325	216,522	409,866	583,922
19	2038	344,118	494,038	648.17	903.44	159,501	225,243	426,375	607,442
20	2039	355,420	510,265	669.46	933.11	164,740	232,641	440,379	627,394
21	2040	364,949	523,946	687.41	958.13	169,156	238,879	452,186	644,215
22	2041	372,993	535,494	702.56	979.25	172,885	244,144	462,153	658,414
23	2042	379,552	544,911	714.92	996.47	175,925	248,437	470,280	669,992
24	2043	385,039	552,787	725.25	1010.87	178,468	252,028	477,078	679,677
25	2044	389,700	559,480	734.03	1023.11	180,629	255,079	482,853	687,905
26	2045	393,413	564,810	741.02	1032.86	182,349	257,509	487,453	694,459
27	2046	396,589	569,370	747.01	1041.20	183,822	259,589	491,389	700,066
28	2047	399,518	573,575	752.52	1048.89	185,179	261,506	495,018	705,236
29	2048	402,117	577,306	757.42	1055.71	186,384	263,207	498,238	709,823
30	2049	404,509	580,741	761.93	1061.99	187,493	264,773	501,202	714,046
31	2050	406,366	583,406	765.42	1066.86	188,353	265,988	503,502	717,323
32	2051	407,974	585,715	768.45	1071.09	189,099	267,041	505,496	720,163
33	2052	409,171	587,433	770.71	1074.23	189,653	267,824	506,978	722,275
34	2053	410,119	588,795	772.49	1076.72	190,093	268,445	508,154	723,950
35	2054	410,986	590,039	774.13	1078.99	190,495	269,012	509,227	725,479
36	2055	411,604	590,927	775.29	1080.62	190,781	269,417	509,994	726,571
37	2056	412,141	591,697	776.30	1082.03	191,030	269,768	510,658	727,518
38	2057	412,388	592,052	776.77	1082.68	191,145	269,930	510,965	727,955
39	2058	412,512	592,230	777.00	1083.00	191,202	270,011	511,118	728,173

*Benefits are defined as potential lives saved, injuries prevented and the reduction in number of property-damaged vehicles

Table XIII-8 Preliminary Annual Benefits* Estimates of IMA and LTA

Scenario 2

	Calendar	Crash Prevented		Fatalities Eliminated		MAIS 1-5 Injuries		PDOV	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2020	124	178	0.23	0.32	57	81	153	218
2	2021	1,073	1,540	2.02	2.82	497	702	1,329	1,893
3	2022	3,919	5,626	7.38	10.29	1,816	2,565	4,856	6,918
4	2023	9,075	13,029	17.09	23.83	4,206	5,940	11,245	16,020
5	2024	16,830	24,163	31.70	44.19	7,801	11,016	20,854	29,709
6	2025	27,473	39,443	51.75	72.13	12,734	17,983	34,040	48,496
7	2026	41,334	59,341	77.86	108.52	19,158	27,055	51,214	72,963
8	2027	58,535	84,037	110.26	153.68	27,132	38,315	72,528	103,328
9	2028	77,882	111,813	146.70	204.47	36,099	50,978	96,499	137,479
10	2029	98,962	142,076	186.40	259.81	45,869	64,776	122,617	174,689
11	2030	121,526	174,471	228.90	319.05	56,328	79,545	150,575	214,520
12	2031	145,080	208,287	273.27	380.89	67,246	94,963	179,760	256,098
13	2032	169,212	242,933	318.73	444.25	78,431	110,759	209,661	298,697
14	2033	193,468	277,756	364.41	507.93	89,674	126,635	239,714	341,513
15	2034	217,600	312,401	409.87	571.28	100,859	142,431	269,615	384,111
16	2035	241,072	346,099	454.08	632.91	111,738	157,794	298,697	425,544
17	2036	263,471	378,257	496.27	691.71	122,121	172,456	326,451	465,084
18	2037	284,303	408,165	535.51	746.40	131,776	186,092	352,263	501,857
19	2038	303,238	435,348	571.17	796.11	140,553	198,485	375,723	535,280
20	2039	320,068	459,511	602.87	840.30	148,354	209,502	396,576	564,989
21	2040	334,671	480,476	630.38	878.64	155,122	219,060	414,670	590,767
22	2041	347,170	498,421	653.92	911.45	160,916	227,241	430,157	612,830
23	2042	357,648	513,463	673.66	938.96	165,772	234,100	443,139	631,326
24	2043	366,434	526,078	690.21	962.03	169,845	239,851	454,026	646,836
25	2044	373,818	536,679	704.12	981.41	173,267	244,684	463,175	659,870
26	2045	379,924	545,444	715.62	997.44	176,097	248,680	470,740	670,647
27	2046	385,080	552,847	725.33	1010.98	178,487	252,055	477,129	679,750
28	2047	389,618	559,361	733.88	1022.89	180,590	255,025	482,751	687,759
29	2048	393,660	565,165	741.49	1033.51	182,464	257,672	487,760	694,895
30	2049	397,208	570,258	748.17	1042.82	184,108	259,994	492,156	701,158
31	2050	400,219	574,582	753.85	1050.73	185,504	261,965	495,887	706,473
32	2051	402,735	578,194	758.59	1057.33	186,671	263,612	499,005	710,915
33	2052	404,922	581,333	762.70	1063.07	187,684	265,043	501,713	714,775
34	2053	406,819	584,057	766.28	1068.05	188,563	266,285	504,065	718,124
35	2054	408,387	586,308	769.23	1072.17	189,290	267,311	506,007	720,891
36	2055	409,707	588,203	771.72	1075.64	189,902	268,175	507,642	723,221
37	2056	410,738	589,683	773.66	1078.34	190,380	268,850	508,920	725,042
38	2057	411,398	590,631	774.90	1080.08	190,686	269,282	509,738	726,207
39	2058	411,852	591,282	775.76	1081.27	190,896	269,579	510,300	727,008

*Benefits are defined as potential lives saved, injuries prevented and the reduction in number of property-damaged vehicles

Table XIII-9 Preliminary Annual Benefits* Estimates of IMA and LTA

Scenario 3

	Calendar	Crash Prevented		Fatalities Eliminated		MAIS 1-5 Injuries		PDOV	
Year	Year	Low	High	Low	High	Low	High	Low	High
1	2020	0	0	0.00	0.00	0	0	0	0
2	2021	83	118	0.16	0.22	38	54	102	146
3	2022	371	533	0.70	0.97	172	243	460	655
4	2023	908	1,303	1.71	2.38	421	594	1,124	1,602
5	2024	1,609	2,310	3.03	4.22	746	1,053	1,993	2,840
6	2025	2,516	3,613	4.74	6.61	1,166	1,647	3,118	4,442
7	2026	3,548	5,093	6.68	9.31	1,644	2,322	4,396	6,262
8	2027	4,744	6,811	8.94	12.45	2,199	3,105	5,878	8,374
9	2028	6,023	8,647	11.34	15.81	2,792	3,942	7,462	10,631
10	2029	7,466	10,719	14.06	19.60	3,461	4,887	9,251	13,180
11	2030	8,952	12,851	16.86	23.50	4,149	5,859	11,091	15,801
12	2031	10,437	14,983	19.66	27.40	4,837	6,831	12,931	18,423
13	2032	12,004	17,234	22.61	31.52	5,564	7,857	14,874	21,190
14	2033	13,530	19,425	25.49	35.52	6,271	8,856	16,765	23,884
15	2034	15,015	21,557	28.28	39.42	6,960	9,828	18,605	26,506
16	2035	16,418	23,571	30.92	43.10	7,610	10,746	20,343	28,981
17	2036	17,738	25,466	33.41	46.57	8,222	11,610	21,978	31,311
18	2037	18,976	27,243	35.74	49.82	8,795	12,421	23,511	33,496
19	2038	20,048	28,782	37.76	52.63	9,292	13,123	24,840	35,389
20	2039	20,997	30,145	39.55	55.12	9,732	13,744	26,016	37,064
21	2040	21,781	31,270	41.03	57.18	10,095	14,257	26,987	38,448
22	2041	22,482	32,277	42.35	59.02	10,421	14,716	27,856	39,685
23	2042	22,977	32,987	43.28	60.32	10,650	15,040	28,469	40,559
24	2043	23,431	33,639	44.13	61.51	10,860	15,337	29,032	41,360
25	2044	23,802	34,172	44.83	62.49	11,032	15,580	29,492	42,016
26	2045	24,132	34,645	45.45	63.36	11,185	15,796	29,900	42,598
27	2046	24,379	35,001	45.92	64.01	11,300	15,958	30,207	43,035
28	2047	24,627	35,356	46.39	64.66	11,415	16,120	30,514	43,472
29	2048	24,833	35,652	46.78	65.20	11,510	16,255	30,769	43,836
30	2049	24,998	35,889	47.09	65.63	11,587	16,363	30,974	44,127
31	2050	25,163	36,126	47.40	66.06	11,663	16,471	31,178	44,419
32	2051	25,328	36,363	47.71	66.50	11,740	16,579	31,383	44,710
33	2052	25,452	36,541	47.94	66.82	11,797	16,660	31,536	44,928
34	2053	25,534	36,659	48.10	67.04	11,835	16,714	31,638	45,074
35	2054	25,617	36,777	48.25	67.25	11,874	16,768	31,740	45,220
36	2055	25,700	36,896	48.41	67.47	11,912	16,822	31,843	45,365
37	2056	25,741	36,955	48.48	67.58	11,931	16,849	31,894	45,438
38	2057	25,782	37,014	48.56	67.69	11,950	16,876	31,945	45,511
39	2058	25,782	37,014	48.56	67.69	11,950	16,876	31,945	45,511

*Benefits are defined as potential lives saved, injuries prevented and the reduction in number of property-damaged vehicles

XIV. Appendix B: List of Policy, Standards and Research Needs

A. Policy needs

B. Standards needs

C. Research needs

XV. Appendix C: List of Tables, Figures and Equations

A. Tables

B. Figures

C. Equations

DOT HS 812 014
August 2014

U.S. Department
of Transportation

National Highway
Traffic Safety
Administration

NHTSA
www.nhtsa.gov

10690-081514-v2c