



November 2013

INTELLIGENT TRANSPORTATION SYSTEMS

Vehicle-to-Vehicle
Technologies
Expected to Offer
Safety Benefits, but a
Variety of Deployment
Challenges Exist

GAO Highlights

Highlights of [GAO-14-13](#), a report to congressional requesters

Why GAO Did This Study

In 2011, 5.3 million vehicle crashes in the United States resulted in more than 2.2 million injuries and about 32,000 fatalities. While improvements in automobile safety have reduced the number of fatalities in recent decades, DOT has worked with the automobile industry to develop V2V technologies, through which vehicles are capable of warning drivers of imminent collisions by sharing data, including information on speed and location, with nearby vehicles. GAO was asked to review the status of V2V technologies. GAO examined (1) the state of development of V2V technologies and their anticipated benefits; (2) the challenges, if any, that will affect the deployment of these technologies and what actions, if any, DOT is taking to address them; and (3) what is known about the potential costs associated with these technologies.

GAO reviewed documentation on V2V technology-related efforts by DOT and automobile manufacturers, visited a pilot study of V2V technologies in Michigan, and interviewed DOT officials, automobile manufacturers, and 21 experts identified by the National Academies of Sciences. Experts were selected based on their level of knowledge and to represent a variety of subject areas related to V2V technology development.

DOT and the Federal Communications Commission reviewed a draft of this report and provided technical comments which were incorporated as appropriate.

View [GAO-14-13](#). For more information, contact Dave Wise at (202) 512-2834 or wised@gao.gov.

November 2013

INTELLIGENT TRANSPORTATION SYSTEMS

Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist

What GAO Found

The development of vehicle-to-vehicle (V2V) technologies has progressed to the point of real world testing, and if broadly deployed, they are anticipated to offer significant safety benefits. Efforts by the U.S. Department of Transportation (DOT) and the automobile industry have focused on developing: 1) in-vehicle components such as hardware to facilitate communications among vehicles, 2) safety software applications to analyze data and identify potential collisions, 3) vehicle features that warn drivers, and 4) a national communication security system to ensure trust in the data transmitted among vehicles. According to DOT, if widely deployed, V2V technologies could provide warnings to drivers in as much as 76 percent of potential multi-vehicle collisions involving at least one light vehicle, such as a passenger car. Ultimately, however, the level of benefits realized will depend on the extent of the deployment of these technologies and the effectiveness of V2V warnings in eliciting appropriate driver responses. The continued progress of V2V technology development hinges on a decision that the National Highway Traffic Safety Administration (NHTSA) plans to make in late 2013 on how to proceed regarding these technologies. One option would be to pursue a rulemaking requiring their inclusion in new vehicles.

The deployment of V2V technologies faces a number of challenges, which DOT is working with the automobile industry to address. According to experts, DOT officials, automobile manufacturers, and other stakeholders GAO interviewed, these challenges include: 1) finalizing the technical framework and management framework of a V2V communication security system, which will be unique in its size and structure; 2) ensuring that the possible sharing with other wireless users of the radio-frequency spectrum used by V2V communications will not adversely affect V2V technology's performance; 3) ensuring that drivers respond appropriately to warnings of potential collisions; 4) addressing the uncertainty related to potential liability issues posed by V2V technologies; and 5) addressing any concerns the public may have, including those related to privacy. DOT is collaborating with automobile manufacturers and others to find potential technical and policy solutions to these challenges and plans to continue these efforts. Although V2V technologies are being tested in a real-world pilot that will end in February 2014, DOT officials stated that they cannot fully plan for deployment until NHTSA decides how to proceed later this year.

DOT and the automobile industry are currently analyzing the total costs associated with V2V technologies, which include the costs of both in-vehicle components and a communication security system. All of the automobile manufacturers GAO interviewed said that it is difficult to estimate in-vehicle V2V component costs at this time because too many factors—such as future production volumes and the time frame of deployment—remain unknown. The costs associated with a V2V communication security system also remain unknown as the specifics of the system's technical framework and management structure are not yet finalized. While the costs of in-vehicle V2V components may be modest relative to the price of a new vehicle, some experts noted that the potential costs associated with the operation of a V2V communication security system could be significant. Further, it is currently unclear who—consumers, automobile manufacturers, DOT, state and local governments, or others—would pay the costs associated with a V2V communication security system.

Contents

Letter		1
	Background	4
	DOT and Industry Have Developed and Piloted V2V Technologies, Which Offer Potentially Significant Safety Benefits If Broadly Deployed	9
	DOT Is Working with the Automobile Industry to Address a Number of V2V Technology Deployment Challenges	20
	Costs of V2V Technologies Are Being Studied and Are Likely to Be Influenced by Various Factors Including Specifics of V2V Communication Security System	33
	Agency Comments	36
Appendix I	Scope and Methodology	37
Appendix II	Structured Interview Guide for Experts Identified by the National Academies of Sciences	41
Appendix III	Expert Ratings of Potential Challenges Facing Deployment of Vehicle-to-Vehicle Technologies	51
Appendix IV	GAO Contact and Staff Acknowledgments	53
Tables		
	Table 1: Subject Matter Experts Interviewed	38
	Table 2: Expert Ratings of Potential Challenges Facing Deployment of Vehicle-to-Vehicle Technologies	51
Figures		
	Figure 1: Example of Vehicle-to-Vehicle Communications and a Warning Scenario	6
	Figure 2: Components of a Vehicle-to-Vehicle Crash Avoidance System	12

Figure 3: Examples of Crash Scenarios and Vehicle-to-Vehicle Applications

17

Abbreviations

CAMP	Crash Avoidance Metrics Partnership
CVT	connected vehicle technologies
DOT	Department of Transportation
DSRC	dedicated short-range communications
FCC	Federal Communications Commission
GHz	gigahertz
ITS	intelligent transportation systems
LiDAR	light detection and ranging
MHz	megahertz
NAS	National Academies of Sciences
NHTSA	National Highway Traffic Safety Administration
NTIA	National Telecommunications and Information Administration
RADAR	radio detection and ranging
RITA	Research and Innovative Technology Administration
VIIC	Vehicle Infrastructure Integration Consortium
VSC	Vehicle Safety Communications
V2V	vehicle-to-vehicle

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



November 1, 2013

The Honorable Lamar Smith
Chairman
The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The Honorable John J. Duncan
The Honorable Ralph Hall
The Honorable Randy Hultgren
House of Representatives

Every year, motor vehicle crashes in the United States result in numerous injuries and deaths and high economic costs. For example, according to the Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA), 5.3 million police-reported vehicle crashes occurred in the United States in 2011, resulting in about 32,000 fatalities and more than 2.2 million injuries.¹

NHTSA aims to reduce injuries, deaths, and economic losses resulting from motor vehicle crashes through a number of actions, such as establishing safety standards for motor vehicles² and conducting research that supports vehicle safety. NHTSA's safety standards cover various aspects of vehicle safety, such as brakes, headlights, seat belts, air bags, and child restraints. Improvements in automobile safety that aim to protect drivers and occupants in the event of a collision—including features such as seat belts and airbags—have reduced fatalities. Recently, however, the automobile industry has begun to introduce technologies that are intended to prevent accidents. Crash avoidance technologies, which use sensors such as cameras and radar, can observe a vehicle's visible surroundings and issue warnings to the driver

¹In addition, NHTSA has estimated that motor vehicle crashes had economic costs—including productivity losses, property damages, and medical costs—of \$230 billion in 2000 (about \$304 billion in 2013 dollars). See L. Blincoe et al, *The Economic Impact of Motor Vehicle Crashes* (Washington, D.C.: NHTSA, 2002). NHTSA has a study under way to update crash cost estimates and expects to issue results by the end of 2013.

²49 USC §§ 30101 and 30111.

when certain types of collisions with other vehicles or obstacles appear to be imminent.³

DOT and the automobile industry have been conducting research on new types of technologies to prevent crashes—called vehicle-to-vehicle (V2V) technologies—in recent years. These technologies facilitate the sharing of data, such as vehicle speed and location, among vehicles to warn drivers of potential collisions. Based on the data shared, V2V technologies are capable of warning drivers of imminent collisions, including some that sensor-based crash avoidance technologies would be unable to detect.⁴ DOT's efforts related to these technologies are being led by NHTSA and the Intelligent Transportation Systems (ITS) Joint Program Office within DOT's Research and Innovative Technology Administration (RITA). According to NHTSA, if V2V technologies are widely deployed, they have the potential to address 76 percent of multi-vehicle crashes involving at least one light vehicle by providing warnings to drivers. In late 2013, NHTSA is planning to announce further actions it will take regarding these technologies for passenger vehicles, including potentially announcing intent to pursue future regulatory action, such as a proposed rulemaking to mandate the installation of V2V technologies in newly manufactured passenger vehicles.⁵ The inclusion of V2V technologies in newly manufactured vehicles could increase vehicle costs.

You asked us to examine the development and possible future deployment of V2V technologies. We examined: (1) the state of development of V2V technologies and their anticipated benefits; (2) the challenges, if any, that will affect the deployment of these technologies, and what actions, if any, DOT is taking to address them; and (3) what is known about the potential costs associated with these technologies for automobile manufacturers and consumers.

³In some cases, certain vehicles can take action without driver input, such as emergency braking, based on such warnings. In addition, such technologies can use sensors to alert drivers when a vehicle is moving out of its lane of travel without use of a turn signal.

⁴The automobile industry has also been researching and developing autonomous vehicle technologies. These would allow for vehicle operation without direct driver input.

⁵NHTSA will complement this 2013 decision with a 2014 decision on introducing such technology for commercial vehicles, including trucks and buses. The Federal Highway Administration is developing guidance for release in 2015 to assist state departments of transportation to adapt to these new technologies.

To address these issues, we reviewed documentation relevant to the V2V technology research efforts of DOT and the automobile industry, such as DOT's *ITS Strategic Research Plan, 2010 - 2014 Progress Update 2012* and documentation related to DOT's efforts to estimate the potential benefits of V2V technologies. We interviewed NHTSA and RITA officials about these efforts. We also visited the DOT-sponsored V2V Safety Pilot Model Deployment in Ann Arbor, Michigan, and received a demonstration of V2V technologies in the Detroit area from automobile manufacturers working on the development of these technologies.⁶ We conducted structured interviews with 21 experts identified by the National Academies of Sciences as knowledgeable in the areas of V2V technology development and interoperability, technology deployment, production of light-duty passenger vehicles, data privacy and security, legal and policy issues, and human factors⁷ issues related to V2V technologies. The structured interviews included asking selected experts to rate the extent to which a series of issues—which we identified based on initial interviews with automobile manufacturers, DOT, and others—present challenges to the deployment of V2V technologies. We selected experts who represented both domestic and international automobile manufacturers, suppliers of V2V devices, a telecommunications company, and state governments, as well as automotive industry experts and academic researchers. In addition, we interviewed representatives of 10 automobile manufacturers involved in collaborative V2V technology development efforts, a V2V device supplier, and associations knowledgeable about the development of V2V technologies. We also interviewed officials with the Federal Communications Commission (FCC) about the use of radio-frequency spectrum by V2V communications. Further details about our scope and methodology can be found in appendix I. Our structured guide for interviewing experts is reproduced in appendix II.

We conducted this performance audit from October 2012 to November 2013 in accordance with generally accepted government auditing

⁶DOT collaborated with a consortium of automobile manufacturers to sponsor the Safety Pilot Model Deployment, a pilot test being conducted by the University of Michigan Transportation Research Institute that is taking place in Ann Arbor, Michigan. The pilot began in August 2012 and is scheduled to end in February 2014.

⁷The term "human factors" refers broadly to how humans' abilities, characteristics, and limitations interact with the design of the equipment they use and the environments in which they function.

standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Although there were about 32,000 motor vehicle traffic fatalities in the United States in 2011, the number has generally declined in recent years. According to NHTSA, the rate of 1.10 fatalities per 100 million vehicle miles traveled in 2011 represented an all-time low and was 28 percent lower than the rate of 1.52 in 2001.⁸ DOT has attributed reductions in fatality rates to several factors, including increased use of in-vehicle safety features such as safety belts and a reduction in fatalities related to alcohol-impaired driving.

In recent years, automobile manufacturers have begun to equip some newly manufactured vehicles with sensor-based crash avoidance technologies intended to prevent accidents and further reduce the number of fatalities. These technologies employ sensors such as cameras, radio detection and ranging, and light detection and ranging⁹ to observe a vehicle's surroundings.¹⁰ A vehicle equipped with such technologies is capable of detecting potential collisions with other vehicles or obstacles within a range of about 150 meters (about 500 feet) and alerting drivers through applications such as forward collision

⁸However, NHTSA's preliminary data for 2012 indicate that the total number of traffic fatalities increased to approximately 34,000 and the rate of traffic fatalities per 100 million vehicle miles traveled increased to approximately 1.16.

⁹Radio detection and ranging, or RADAR, is a method of detecting objects and determining their position, velocity, or other characteristics by analysis of high frequency radio waves reflected from their surfaces. Light detection and ranging, or LiDAR, uses a narrow beam to transmit infrared light pulses to a target, which then travel back again. Measurement of the elapsed time of the light beam to reach the vehicle and return computes the vehicle's distance from the operator.

¹⁰In November 2012, the National Transportation Safety Board urged NHTSA to establish performance standards for crash-avoidance technologies and mandate that such technologies be included as standard equipment in motor vehicles. Currently, sensor-based crash avoidance technologies are not required to be installed in new vehicles. In 2010, NHTSA announced plans to mandate the installation of rear-mounted video cameras and in-vehicle displays in all new passenger vehicles by September 2014 but has not yet established rules governing the placement or minimum field of vision of such cameras.

warnings and lane departure warnings;¹¹ however, such warnings are limited to the threats within the field of view of the vehicle's sensors.

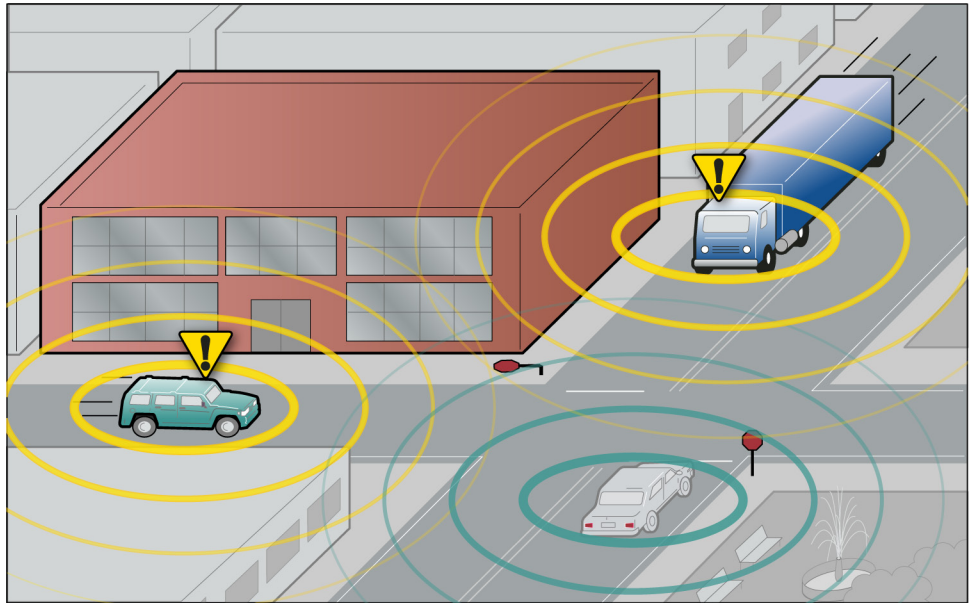
DOT has worked with the automobile industry and others to lead and fund research on connected vehicle technologies, which include V2V technologies as well as vehicle-to-infrastructure technologies. From fiscal years 2003 through 2012, the funding DOT has made available for efforts on connected vehicle technologies, part of its Intelligent Transportation Systems (ITS)¹² research program, totaled about \$445 million and ranged from a low of \$17 million in 2008 to a high of \$84 million in 2011.¹³ In a connected vehicle environment, data is shared wirelessly among vehicles (V2V communications) or between vehicles and infrastructure (vehicle-to-infrastructure communications) using dedicated short-range communications (DSRC), a technology similar to Wi-Fi that offers a link through which vehicles and infrastructure can transmit messages over a range of about 300 to 500 meters (about 1,000 to 1,600 feet). Based on analysis of internal data and data received from other vehicles, a vehicle equipped with V2V technologies is able to issue a warning to its driver when a collision with another similarly equipped vehicle could occur. The range of V2V communications is not only greater than that of existing sensor-based technologies, but due to the sharing of data between vehicles, V2V technologies are capable of alerting drivers to potential collisions that are not visible to existing sensor-based technologies, such as a stopped vehicle blocked from view or a moving vehicle at a blind intersection (see fig. 1).

¹¹A forward collision warning system can issue a warning to drivers when their vehicle is about to collide with a vehicle in front of them. Lane departure warnings can alert a driver when their vehicle begins to veer outside of a lane of travel without the driver activating a turn signal.

¹²ITS technologies consist of a range of communications, electronics, and computer technologies, such as systems that collect real-time traffic data and transmit information to the public via means such as dynamic message signs, ramp meters to improve the flow of traffic on freeways, and synchronized traffic signals that are adjusted in response to traffic conditions.

¹³DOT's early work on connected vehicle technologies focused on vehicle-to-infrastructure technologies. The department increased its focus on V2V technologies because they are projected to produce the majority of connected vehicle technology safety benefits and they do not require the same level of infrastructure investment as vehicle-to-infrastructure technologies. DOT officials indicated that the department plans to increase its focus on vehicle-to-infrastructure technologies starting in 2015.

Figure 1: Example of Vehicle-to-Vehicle Communications and a 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 not visible to the driver of the truck. Both drivers would receive warnings of a potential collision, allowing them to take actions to avoid it.

While V2V technologies send and receive data among vehicles, vehicle-to-infrastructure technologies send and receive data between vehicles and infrastructure, such as traffic signals. Vehicle-to-infrastructure technologies could offer additional safety features that V2V technologies cannot, such as providing drivers with additional warnings when traffic signals are about to change, warnings that could help reduce collisions at intersections. In addition, these technologies can offer potential mobility and environmental benefits; for example, they can collect, analyze, and provide drivers with data on upcoming roadway and traffic conditions and suggest alternate routes when roadways are congested.¹⁴

¹⁴Vehicle-to-infrastructure technologies can also provide additional safety benefits. For example, they can provide drivers with information regarding safe speeds and road conditions such as work zones and, for example, warn drivers when they may be approaching a curve at an unsafe speed.

In addition to federal efforts, automobile manufacturers have formed a number of consortia to research and develop V2V communication-based technologies and have collaborated with DOT on these efforts. Since 2002, DOT has awarded \$77 million in funding, under cost-sharing agreements to support projects related to V2V technologies, to a number of consortia established by the Crash Avoidance Metrics Partnership (CAMP). This partnership between Ford Motor Company and General Motors, L.L.C. is currently working with 6 other automobile manufacturers through the Vehicle Safety Communications (VSC) 3 Consortium to collaboratively address safety issues through advancements in vehicle communications.¹⁵ Additionally, the Vehicle Infrastructure Integration Consortium (VIIC) was created in 2005 and is currently comprised of 10 automobile manufacturers with the goal of identifying and promoting policy solutions needed to support the development and deployment of V2V and vehicle-to-infrastructure technologies.¹⁶

The automobile industry (as well as some technology companies such as Google) is also working to develop autonomous vehicle technologies, which would control steering, acceleration, and braking without a driver's input.¹⁷ Some automobile manufacturers have started to introduce semi-autonomous sensor-based technologies capable of reducing a vehicle's speed through adaptive cruise control¹⁸ or even stopping a vehicle through automatic braking when a collision is imminent. Autonomous

¹⁵The CAMP VSC 3 Consortium is currently comprised of Ford Motor Company; General Motors Holdings LLC; Honda R&D Americas, Inc.; Hyundai America Technical Center, Inc.; Mercedes-Benz Research & Development North America, Inc.; Nissan Technical Center North America; Toyota Motor Engineering & Manufacturing North America, Inc.; and Volkswagen Group of America, Inc.

¹⁶VIIC is currently comprised of BMW of North America, LLC; Chrysler Group LLC; Ford Motor Company; General Motors Holdings LLC; Honda R&D Americas, Inc.; Hyundai America Technical Center, Inc.; Mercedes-Benz Research & Development North America, Inc.; Nissan Technical Center North America; Toyota Motor Engineering & Manufacturing North America, Inc.; and Volkswagen Group of America, Inc.

¹⁷A number of states have enacted legislation permitting the operation of these vehicles under certain conditions and, according to Google, its fleet of autonomous vehicles had logged more than 300,000 miles as of August 2012. In May 2013, DOT announced plans for research on safety issues related to autonomous vehicles and offered recommendations for states related to the testing, licensing, and regulation of these vehicles.

¹⁸Vehicles with adaptive cruise control are able to adjust their own speed based on the distance between the vehicle and vehicles ahead in order to maintain a safe distance.

vehicles are being designed with the intent that a driver is needed to provide destination or navigation information, but not needed to control the vehicle.

Because V2V communications depend upon DSRC technology to transmit data among vehicles, the deployment of V2V technologies will require use of the radio-frequency spectrum. FCC has allocated spectrum for use by DSRC technologies that are part of DOT's ITS research program.¹⁹ Specifically, in 1999, FCC allocated 75 megahertz (MHz) of spectrum²⁰—the 5.850 to 5.925 gigahertz (GHz) band (5.9 GHz band)—for the primary purpose of improving transportation safety and adopted basic technical rules for DSRC operations.²¹ In 2003, FCC established licensing and service rules for the 5.9 GHz band to provide a short-range, wireless link for transferring information between vehicles and roadside systems.²² However, the President and Congress have responded to growing demand for wireless broadband services by making changes in the law to promote efficient use of spectrum, including the band previously set aside for use by DSRC-based technologies. For example, the Middle Class Tax Relief and Job Creation Act of 2012 required the National Telecommunications and Information Administration (NTIA) to

¹⁹Allocation involves segmenting spectrum, the natural resources used for wireless communication, into bands of frequencies that are designated for use by particular types of services. FCC manages spectrum use for nonfederal users, including commercial, private, and state and local government users; the Department of Commerce's National Telecommunications and Information Administration manages spectrum for federal users (47 U.S.C. §§ 303, 305). See GAO, *Commercial Spectrum: Plans and Actions to Meet Future Needs, Including Continued Use of Auctions*, [GAO-12-118](#) (Washington, D.C.: Nov. 23, 2011).

²⁰In the Matter of Amendment of Parts 2 and 90 of the Commission's Rules to Allocate the 5.850-5.925 GHz Band to the Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Services, Report and Order, 14 FCC Rcd 18221 (1999).

²¹Radio frequencies are grouped into bands and are measured in units of Hertz, or cycles per second. The term megahertz (MHz) refers to millions of Hertz and gigahertz (GHz) to billions of Hertz. The Hertz unit of measurement is used to refer to both the quantity of spectrum (such as 75 MHz of spectrum) and the frequency bands (such as the 5.850 – 5.925 GHz band).

²²Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band); Amendment of Parts 2 and 90 of the Commission's Rules to Allocate the 5.850-5.925 GHz Band to Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Services; WT Docket No. 01-90, ET Docket No. 98-95, Report and Order, 19 FCC Rcd 2458 (2004) (FCC 03-324).

conduct a study evaluating spectrum-sharing technologies and the potential risk to federal users if unlicensed devices²³ were allowed to operate in the 5.9 GHz band.²⁴

Given the potential benefits of V2V technologies, NHTSA has said it will decide by the end of 2013 how it will proceed with respect to these technologies for passenger vehicles. According to NHTSA officials, they are considering several possible actions, including announcing NHTSA's intent to pursue future regulatory action, such as a proposed rulemaking to mandate the installation of these technologies in newly manufactured passenger vehicles²⁵ and continuing to research and develop these technologies for passenger vehicles.

DOT and Industry Have Developed and Piloted V2V Technologies, Which Offer Potentially Significant Safety Benefits If Broadly Deployed

Efforts by DOT and the automobile industry to develop V2V technologies have reached the point at which they have been tested in a 12-month, real world pilot that will conclude in February 2014. These efforts have focused on developing and testing needed components including hardware to send and receive data among vehicles, software applications to analyze data and identify potential collisions, vehicle features that issue warnings to drivers of these potential collisions, and a security system to ensure trust in the data that are being communicated among vehicles. According to DOT, once deployed, V2V technologies have the potential to address—by providing warnings to drivers—76 percent of all potential multi-vehicle crashes involving at least one light-duty vehicle.²⁶ However, the potential benefits of V2V technologies are dependent upon a number of factors including their deployment levels, how drivers respond to

²³Traditional unlicensed equipment consists of low powered devices that operate in a limited geographic range, such as garage door openers and devices that offer wireless access to the Internet. They include Wi-Fi-enabled local area networks and fixed outdoor broadband transceivers used by wireless Internet service providers to connect devices to broadband networks.

²⁴Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, § 6406, 126 Stat. 156, 231 (2012).

²⁵In July 2013, the National Transportation Safety Board recommended that NHTSA develop minimum performance standards for connected vehicle technologies and require their installation on all newly manufactured highway vehicles.

²⁶DOT defines light-duty vehicles as passenger cars, vans, minivans, sport utility vehicles or light pickup trucks with gross vehicle weight less than or equal to 10,000 lbs.

warning messages, and the deployment of other safety technologies that can provide similar benefits.

Development of V2V Technologies Has Evolved to Include a Real World Pilot

Recent and ongoing V2V technology development efforts have been working toward the expected late 2013 NHTSA decision as the next major milestone. DOT, for example, has focused on research and analysis that can provide input for and facilitate its upcoming decision. Most of the 21 experts and 9 automobile manufacturers we spoke with told us that they expect NHTSA's decision to help determine the progress of continued development and eventual deployment of V2V technologies.

Development of these technologies has progressed to the point of real world testing. DOT has sponsored and provided approximately 80 percent of the funding for a pilot test called the Safety Pilot Model Deployment (Safety Pilot). This project—in which DOT has partnered with the CAMP VSC 3 Consortium—has been conducted by the University of Michigan Transportation Research Institute and is taking place in Ann Arbor, Michigan, from August 2012 to February 2014. The primary goals of this pilot are to test the effectiveness of V2V technologies in real world situations and to measure their potential benefits. In total, about 2,700 passenger vehicles were equipped with these technologies in order to participate in the Safety Pilot.²⁷ NHTSA plans to release findings from the Safety Pilot in the fall of 2014. DOT is considering the data from the first 6 months of the pilot, along with other information, in working toward a decision by late 2013 on how to proceed with V2V technologies.²⁸

Efforts by DOT and the automobile industry to develop V2V technologies have focused on both in-vehicle components as well as a security system that manages V2V communications and ensures trust in the data being

²⁷The eight members of CAMP each provided eight vehicles that were fully integrated with V2V components for the Safety Pilot. The remainder of the vehicles involved were equipped with aftermarket and retrofit V2V devices. These devices were not fully integrated with the vehicle or not installed during vehicle production. In addition, 79 commercial vehicles and 88 transit vehicles were equipped with V2V devices and tested as part of the Safety Pilot.

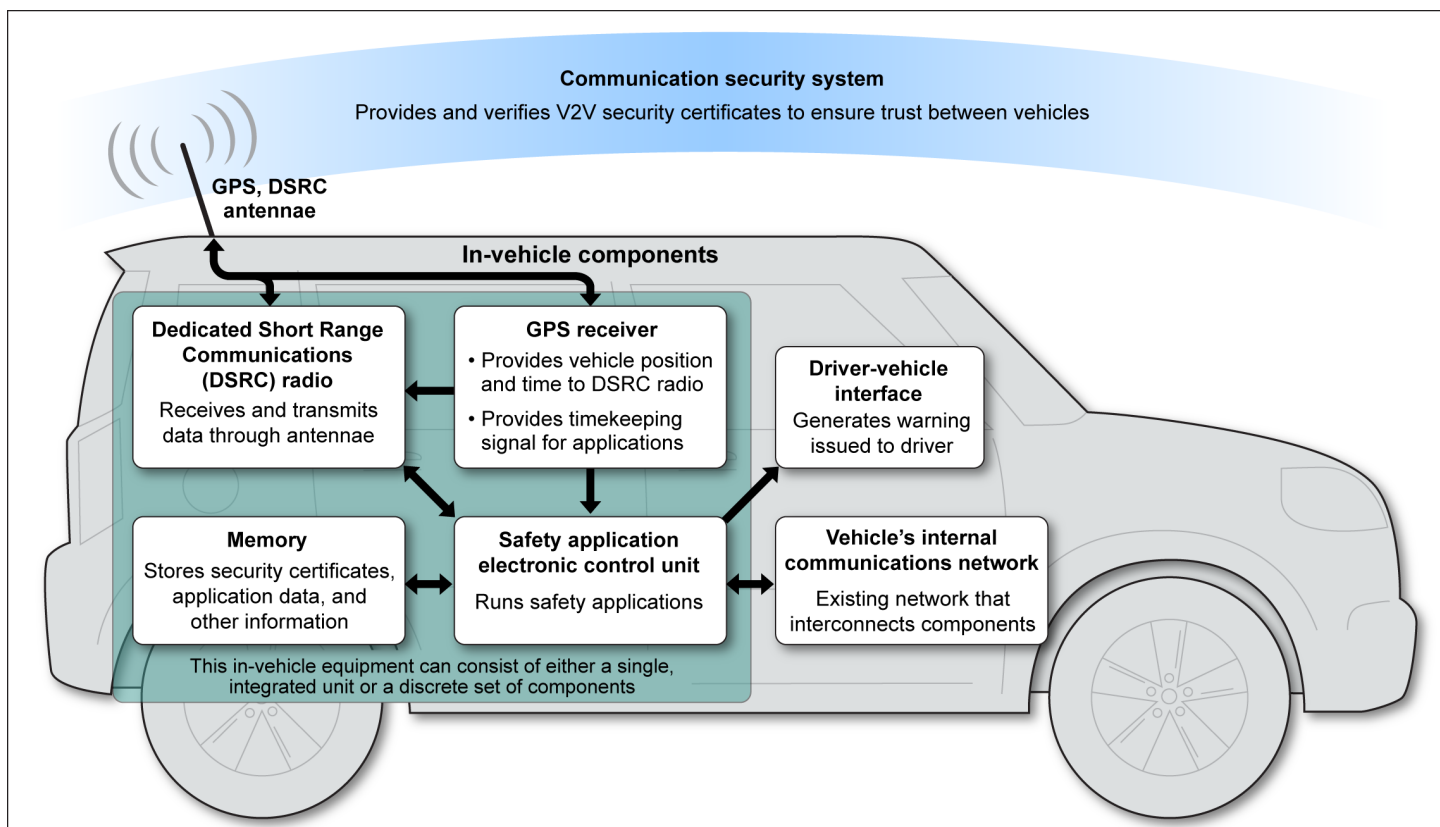
²⁸According to DOT, the department may release some information from its data analysis in relation to making this decision.

transmitted among vehicles (see fig. 2). Examples of in-vehicle components include:

- V2V hardware, including DSRC radios, cables, and antennae to send and receive data and GPS chips used to determine vehicle location.
- Software applications that analyze data such as location, speed, and brake status and, based on that analysis, predict when collisions are imminent. DOT has worked with automobile manufacturers to determine the most relevant applications based on common crash scenarios and to define, develop, and test these to inform and support NHTSA's V2V technology decision later this year.
- A driver-vehicle interface that—based on the data analysis conducted by the V2V software applications—provides a warning to the driver through vehicle features such as sounds, lights, or seat vibrations when a collision may be imminent.²⁹ Existing sensor-based crash avoidance technologies also provide warnings to drivers through similar mechanisms. DOT has been developing guidelines for automobile manufacturers in implementing driver-vehicle interfaces.

²⁹For example, for potential collisions involving vehicles in a driver's blind spot, one automobile manufacturer's vehicles provided three short low-pitched beeps repeated three times, an orange light in the side view mirror, and a vibration on the side of the driver's seat in the direction of the potential collision.

Figure 2: Components of a Vehicle-to-Vehicle Crash Avoidance System



Sources: Crash Avoidance Metrics Partnership and GAO.

In addition to in-vehicle V2V components, an external communication security system is needed to ensure that data being transmitted among vehicles are secure and trusted and have not been altered in the transmission process. Initial research and proposals by DOT and the automobile industry on the design of a communication security system have focused on a public key infrastructure system.³⁰ Such a system

³⁰Public key infrastructure describes the hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. Public key infrastructure forms the foundation of the approach to V2V communications security by employing a "public key" to authenticate a sender or encrypt data being sent in a message, thereby producing trusted and secure messages. A public key infrastructure typically involves a certificate authority that issues and verifies digital certificates, which includes the public key, a directory that holds the certificates and a certificate management and distribution system.

provides security certificates to vehicles which indicate to other vehicles that the data being transmitted are to be trusted because they are valid and have not been altered. Public key infrastructure is used to provide security for many other types of data transmissions and transactions, including online banking and Internet commerce. According to CAMP VSC 3 officials, in-vehicle V2V equipment must be able to detect and automatically report potentially misbehaving devices—such as devices that are malfunctioning, used maliciously, or hacked—to a communication security system. The communication security system must also detect and automatically revoke certificates from vehicles with such devices. Vehicles would receive certificates from a security certificate management authority. However, the technical specifications of how certificates will be provided, how often they will be validated, and who will manage this system have not yet been fully defined. According to DOT officials, a prototype V2V communication security system was developed and tested as part of the Safety Pilot, but that system’s design would need additional enhancements to be used for a full deployment.

In-vehicle V2V components could be factory built into new vehicles and fully integrated with existing internal electronics and networks. DOT and the automobile industry have also worked on developing retrofit and aftermarket V2V devices. Such devices would be installed in a vehicle post-manufacture and might not be fully integrated with the vehicle and its existing internal electronics and network. Such aftermarket devices might not have access to all of a vehicle’s data, such as brake status or steering wheel angle. As a result, they could provide a less robust set of data to other vehicles and could generate fewer or less precise warning messages to drivers. One specific type of aftermarket device that the automobile industry has worked to develop would only transmit a basic data set about a vehicle’s speed and location to other vehicles equipped with V2V technologies; this device would neither receive data from other vehicles nor provide a driver with a warning message, but would interact with the V2V communication security system. DOT is now working with the automobile industry to determine additional standards for such devices to ensure that they work on all types of vehicles and adhere to communication standards to ensure the integrity and security of their data transmission.

Because V2V communications involve the sharing of data among different devices and vehicles of various makes and models, they require technical standards to ensure interoperability. DOT and the automobile industry have worked through international standards organizations such as SAE International and the Institute of Electrical and Electronic

Engineers to develop and set standards to facilitate V2V communications. These efforts have focused on standardizing the data elements that vehicles transmit and the means through which data are transmitted.³¹

Although V2V technologies have undergone real-world testing and most experts we interviewed believed that no major technical challenges remain in the development of in-vehicle V2V components, some experts voiced concerns about two technical issues—GPS accuracy and potential channel congestion—issues that DOT and the automobile industry continue to study.

- Three experts we interviewed expressed concern that GPS used by V2V technologies may not provide sufficiently accurate vehicle position for some V2V applications. Two experts also suggested that the means through which V2V technologies use GPS to determine vehicle position (called “relative positioning”³²) may not be accurate enough, given the need for precise vehicle location data to support V2V software applications. According to DOT officials, however, the department has collected data on the performance of GPS and V2V communications over 20,000 miles in diverse geographic and environmental conditions and is confident that the automotive-grade GPS being used for V2V safety applications is sufficiently accurate. Nevertheless, DOT continues to work to address this issue through research to identify the best means to determine vehicle location through relative positioning. DOT also collected additional data during the Safety Pilot to help ensure that GPS positioning limitations do not negatively affect the performance of V2V technologies.
- Two experts noted that, given the volume of V2V data that would be transmitted in high-traffic areas such as busy highways, channel congestion on the frequency used by V2V communications could

³¹DOT has also been involved in efforts with the European Union and Japan to help set international standards for V2V technologies. For example, RITA has signed implementing arrangements with both the European Union and Japan to cooperate on research programs and support global standards to ensure interoperability of systems. For more information see U.S. Department of Transportation *International Deployment of Cooperative Intelligent Transportation Systems – Bilateral Efforts of the European Commission and the United States Department of Transportation* FHWA-JPO-12-081 (Washington, D.C.: October 2012).

³²Through “relative positioning,” a vehicle’s location is determined relative to other vehicles.

result in delayed transmissions of V2V data. DOT and automobile manufacturers continue to engage in collaborative efforts and sponsor relevant studies to determine the point at which channel congestion might occur and determine potential solutions, such as limiting the frequency of V2V data transmissions in high-traffic situations without compromising safety.³³

In the longer term, V2V technology development efforts are likely to complement efforts to continue to develop and deploy other sensor-based crash avoidance technologies and autonomous vehicle technologies. NHTSA's Administrator stated in May 2013 that DOT sees these three types of technologies as being part of an evolution from vehicles with limited automatic controls to vehicles with fully autonomous self-driving capabilities. NHTSA's preliminary statement of policy on vehicle automation, issued in May 2013, recognizes the potential benefits of automation and its relationship to V2V technologies.³⁴ According to DOT officials, DOT's 2015 to 2019 ITS strategic plan, expected to be issued in early 2014, will describe DOT's planned activities in this area. Furthermore, a recent report by an automotive industry consulting firm stated that the convergence of sensor-based crash avoidance technologies and connected vehicle technologies will be needed to enable truly autonomous vehicles, given the benefits and downsides of each type of technology.³⁵ Five experts and one automobile manufacturer we interviewed said that V2V technologies are a key part of the industry's road map to vehicle automation.

V2V Technologies Have Potential to Provide Significant Safety Benefits Only after Broad Deployment

V2V technologies are expected to offer significant safety benefits by helping drivers avoid collisions in a number of collision scenarios. The automobile industry has worked with DOT to develop safety applications for rear-end, intersection, and lane-change crash scenarios. (See fig. 3 for examples of V2V safety applications and a go to <http://www.gao.gov/products/GAO-14-13> for a video that demonstrates

³³V2V technologies normally transmit data 10 times per second.

³⁴NHTSA views vehicle automation as progressing along various levels of automation from having only certain vehicle functions such as braking independently automated to the point at which the vehicle is fully automated and the driver provides no control over the vehicle during travel.

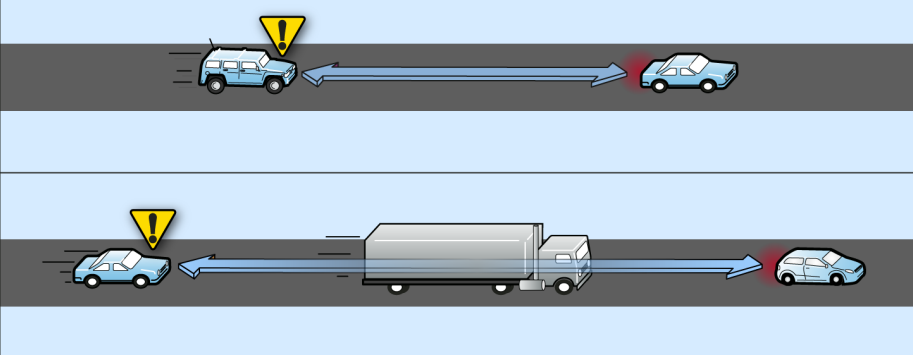
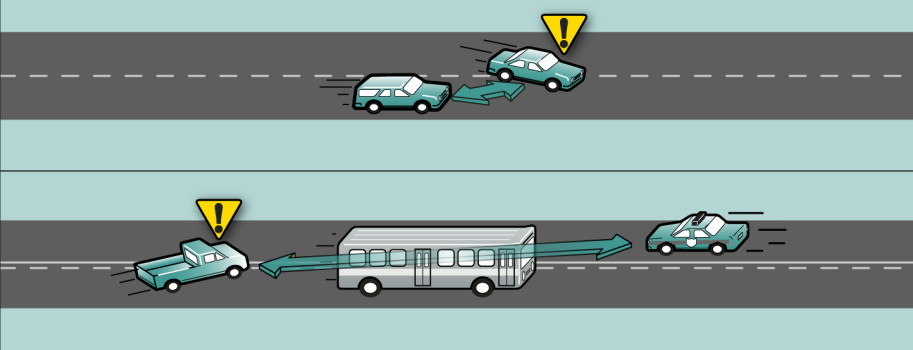
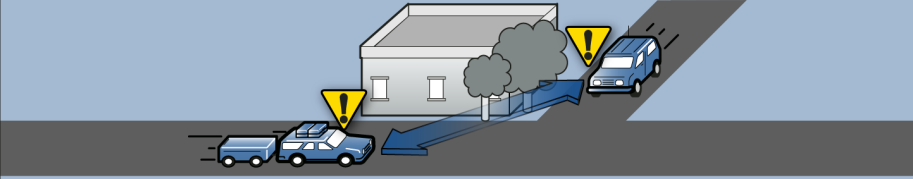

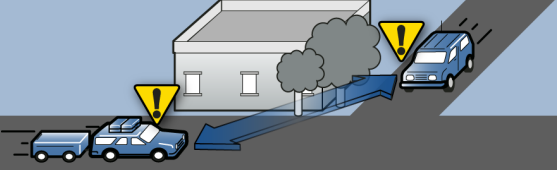
³⁵KPMG and Center for Automotive Research, *Self-Driving Cars: The Next Revolution*.


selected applications warning drivers of potential collisions.) According to NHTSA, these prevalent crash scenarios represent the majority of all vehicle crashes. Because automobiles cannot currently take autonomous actions—such as braking—based on data gathered by V2V technologies, drivers must act on V2V warnings to prevent collisions from happening. These crash scenario applications are being tested in the Safety Pilot, and DOT and the automobile industry have collected data to determine how to improve the accuracy of the applications. DOT is currently conducting a benefits assessment based in part on the first 6 months of data from the Safety Pilot to inform the decision NHTSA plans to make in late 2013.³⁶ DOT's Volpe Center³⁷ is conducting this benefits assessment, which, according to DOT, uses a methodology to determine how many vehicle collisions would be prevented through the use of V2V technologies in a number of different types of collision scenarios. The result will be an estimate of the effectiveness of V2V safety applications.

³⁶As noted previously, the Safety Pilot will end in February 2014. DOT plans to finalize its assessment and release its complete findings by fall 2014.

³⁷The John A. Volpe National Transportation Systems Center, part of RITA, is a fee-for-service organization that performs work for DOT as well as other federal, state, local, and international agencies and entities.

Figure 3: Examples of Crash Scenarios and Vehicle-to-Vehicle Applications

Scenario and warning type	Scenario example
<p>Rear end collision scenarios</p> <p>Forward collision warning Approaching a vehicle that is decelerating or stopped.</p>	
<p>Emergency electronic brake light warning Approaching a vehicle braking hard or stopped in roadway but not visible due to obstructions.</p>	
<p>Lane change scenarios</p> <p>Blind spot warning Beginning lane change that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles already in or soon to be in blind spot.</p>	
<p>Do not pass warning Encroaching onto the travel lane of another vehicle traveling in opposite direction.</p>	
<p>Intersection scenario</p> <p>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.</p>	

 To view a video demonstration of selected V2V safety applications, go to... <http://www.gao.gov/products/GAO-14-13>

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.

In May 2013, DOT reported that V2V technologies have the potential to address—by providing warnings to drivers—76 percent of all potential

multi-vehicle crashes involving at least one light vehicle.³⁸ While the majority of experts we interviewed agreed that 76 percent is plausible as a maximum level, this estimate is an upper limit of the potential safety benefits of V2V technologies which assumes their full deployment across the U.S. vehicle fleet. This estimate also assumes that V2V technologies provide warnings in all potential crash scenarios involving at least two vehicles equipped with these technologies. The actual number of crashes prevented by V2V technologies will depend on a number of factors, including the following:

- *Deployment Levels:* According to DOT, the safety benefits of V2V technologies will be maximized with near full deployment across the U.S. vehicle fleet. However, even if NHTSA pursues a rulemaking requiring installation of these technologies in new vehicles, it could take a number of years until benefits are fully realized due to the rate of turnover of the fleet. According to one automobile manufacturer we interviewed, given the rate of new vehicle sales, it can take up to 20 years for the entire U.S. vehicle fleet to turn over. It may be possible to see some benefits at lower levels of deployment, as was seen in the number of interactions among participating vehicles in the Safety Pilot, according to DOT.³⁹ Also, aftermarket devices that allow existing vehicles to be equipped with V2V devices could help speed deployment. However, three experts we interviewed expressed concern that drivers may not see value in purchasing aftermarket devices, which could limit their adoption.
- *Driver response:* The benefits of V2V technologies will also depend on how well drivers respond to warning messages. If drivers do not take appropriate action in response to warnings, then the benefits of V2V technologies could be reduced. For example, if drivers do not respond to warnings quickly enough—due to distraction, impairment, or other reasons—they may not be able to avoid a collision. Furthermore, if safety applications offer too many false warnings when no imminent threat exists, drivers could begin to ignore valid warnings or not

³⁸United States Department of Transportation, *Description of Light-Vehicle Pre-Crash Scenarios for Safety Applications Based on Vehicle-to-Vehicle Communications*, (Washington, D.C.: May 2013).

³⁹According to DOT, based on early data on vehicle interactions in the Safety Pilot, there has been a sufficient level of vehicle interactions to analyze the performance capability of the applications, examine driver response to warnings, and evaluate unintended consequences.

respond to them quickly enough. For example, the Insurance Institute for Highway Safety reported that as many as 41 percent of drivers of certain makes of vehicles with sensor-based lane departure warning systems found the systems “annoying” due to false alarms and unnecessary warnings.⁴⁰

- *Deployment of other safety technologies:* The potential benefits solely attributable to V2V technologies will also depend on the market penetration and effectiveness of sensor-based crash avoidance technologies. These existing technologies are able to address some of the same crash scenarios as V2V safety applications and their market penetration is likely to increase in the future. While there are cases where V2V technologies can provide safety benefits where sensor-based crash avoidance technologies cannot—such as around a curve or when detecting an unseen stopped car—there are some V2V technology collision scenarios that sensor-based crash avoidance technologies can also address. For example, cameras and radar can be used to provide drivers with forward collision warnings or lane change warnings when another vehicle is in a blind spot. In addition, vehicles in the future may use V2V technologies and sensor-based crash avoidance technologies to complement one another. For example, future vehicles may be able to use V2V data to validate sensor data and provide drivers with more accurate and certain warnings as well as to help execute more reliable automated control actions such as braking. The benefits attributable to V2V technologies will depend on how these technologies work together and the market penetration of these technologies. According to DOT officials, the department’s methodology for estimating the safety benefits of V2V technologies will account for the benefits of sensor-based crash avoidance technologies by estimating their penetration and effectiveness in avoiding collisions.

⁴⁰Insurance Institute for Highway Safety *Status Report*, Vol. 47, No. 5, (Arlington, VA.: July 3, 2012).

DOT Is Working with the Automobile Industry to Address a Number of V2V Technology Deployment Challenges

While V2V technologies have been tested in real world settings, a number of challenges exist to their wide-scale deployment and the realization of their potential benefits. DOT has been collaborating with automobile manufacturers and others to identify potential solutions to these challenges and is planning continued efforts to support the eventual deployment of V2V technologies. As part of these efforts, the department has been considering various policy options, such as options for managing the V2V communication security system. However, future DOT actions to address some of these issues will not be finalized until after NHTSA decides how the agency will proceed with V2V technologies later this year.

V2V Technology Deployment Challenges and Efforts to Address Them

According to experts we interviewed, DOT officials, automobile manufacturers, and other stakeholders, the deployment of V2V technologies faces a number of challenges, including: (1) finalizing the technical framework and management structure of a V2V communication security system to ensure trust among vehicles, (2) ensuring that the possible sharing of the band of radio-frequency spectrum used by V2V communications will not adversely affect their performance, (3) considering human factors to ensure that drivers respond appropriately to V2V warnings, (4) addressing the uncertainty related to potential liability issues posed by V2V technologies, and (5) addressing any concerns the public may have about V2V technologies, including those related to privacy.⁴¹

Framework of V2V Communication Security System

As discussed earlier, a security system capable of detecting, reporting, and revoking the credentials of vehicles found to be sharing inaccurate information will be needed to ensure trust in the V2V data transmitted among vehicles. Final plans and policies for the V2V communication security system—including its technical framework and management

⁴¹After identifying a series of potential challenges facing the development and deployment of V2V technologies through preliminary interviews with DOT officials, two automobile industry groups, two automobile manufacturers, representatives of CAMP and the VIIC, and others, we asked experts identified by the National Academies of Sciences to discuss the extent to which each may pose a challenge. After interviewing 21 experts, in addition to automobile manufacturers and DOT officials, we counted the experts' ratings of potential challenges facing the development and deployment of V2V technologies and conducted a content analysis of their relevant responses. See appendix I for further details on our methodology and appendix III for a summary of the ratings provided by experts for each of the potential challenges discussed.

structure—have not yet been developed and will need to be finalized prior to V2V technology deployment.

- *Technical framework:* Of the 21 experts we interviewed, 12 cited the technical development of a V2V communication security system as a great or very great challenge to the deployment of V2V technologies. One expert told us that it is challenging to establish technical specifications for a system that attempts to maintain users' privacy while providing security for over-the-air transmission of data. Another expert noted that a public key infrastructure system the size of the one needed to support the nationwide deployment of V2V technologies has never been developed before; the sheer magnitude of the system will pose challenges to its development. Both the manner through which V2V communication security certificates will be provided to vehicles and how often they will be provided need to be determined. Some proposals call for using DSRC-equipped roadside infrastructure to provide security certificates, while other proposals call for using non-DSRC communications technologies such as cellular.
- *Management structure:* How a V2V communication security system will be managed has not yet been determined and the delineation of relevant roles and responsibilities could be difficult. Twelve of the experts we interviewed cited the establishment of a management framework for a security system as a great or very great challenge to V2V technology deployment. Because no similar institutions exist, many questions remain about how such a system should be structured and who should manage it. One expert suggested that deciding which approach is most appropriate involves weighing competing philosophies. The expert added that developing the management structure could prove more difficult than developing the technical aspects of the security system.

DOT has researched options to address the technical framework of a V2V communication security system and officials noted that additional technical and policy analyses are under way that will determine the specifics by early 2014. DOT officials stated that a framework that meets the technical requirements of CAMP will be finalized and subsequently prototyped and tested. As mentioned earlier, a prototype technical framework for issuing and managing security certificates has been tested as part of the Safety Pilot. DOT officials told us that there were no significant technical challenges identified during the development of this framework but noted that additional analysis related to the detection and revocation of credentials from vehicles found to be sharing inaccurate

information is needed. In preparation for the testing of the Safety Pilot's prototype technical framework, DOT conducted research on the risks associated with such a system and identified potential approaches to address those risks.⁴² In addition, the department held public workshops in April 2012 to bring together various stakeholders to discuss issues related to a V2V communication security system.⁴³ DOT officials explained that NHTSA is currently engaging a firm with expertise in information security systems to perform a review that will help inform the eventual technical specifications of a V2V communication security system. Although various technical frameworks are being considered, limits to DOT's authority could limit the viability of some options. For example, according to DOT officials, the department does not have the legal authority to require the installation of roadside infrastructure to support a V2V communication security system because, aside from roads on federal lands, the federal government does not own or operate U.S. roadways.

In addition, DOT has worked with automobile manufacturers through the VIIC to examine potential management structures for a V2V communication security system. However, officials told us that it would be premature to comment on what the management structure will look like without knowing whether the agency will pursue a rulemaking related to V2V technologies. As part of its research on the technical framework of a V2V communication security system, DOT also sought stakeholder input on the potential management structure and identified three potential options:

- *Federal model:* DOT officials explained that, if the federal government were to provide the security management services required to support V2V technologies, it most likely would do so through a service contract that would include specific provisions to ensure adequate market access, privacy and security controls, and reporting and continuity of services. According to DOT, the department has

⁴²U.S. Department of Transportation, *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-JPO-11-130 (Washington, D.C.: November 2011).

⁴³U.S. Department of Transportation, *Enabling a Secure Environment for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Transactions: April 2012 Public Workshop Proceedings*, FHWA-JPO-12-072 (Washington, D.C.: June 2012).

appropriate legal authority to pursue this model but does not have sufficient resources to introduce such a structure at this time.

- *Public-Private model:* Under a public-private partnership, the security system would be jointly owned and managed by the federal government and private entities. DOT officials stated that statutory authority would be needed to create a public-private management structure that is vested with the authority that Congress deems necessary and appropriate to finance and operate a V2V communication security system. DOT officials added that the required legal authority would likely need to include authorization to establish and collect fees on behalf of the entity and possibly provisions addressing liability, privacy, data ownership, and security requirements applicable to such a system.
- *Private model:* DOT officials stated that its current legal authority and resources have led NHTSA to focus primarily on working with stakeholders to develop a viable private model. DOT officials suggested that, through an agreement with a privately owned and operated security management provider, a private model could be used to support a V2V communication security system. Aside from any aspects specifically detailed in the agreement, DOT suggested that the governance and financing of a private management structure would depend on what entity constitutes and owns the entity.

Potential Spectrum Sharing

In response to requirements in the Middle Class Tax Relief and Job Creation Act of 2012,⁴⁴ FCC issued a Notice of Proposed Rulemaking in February 2013 that requested comments on allowing unlicensed devices to share the 5.9 GHz band of the radio-frequency spectrum that had been previously set aside for the use of DSRC-based ITS applications such as V2V technologies.⁴⁵ The proposed modifications would provide access to additional spectrum with consistent technical requirements, resulting in faster data speeds by allowing unlicensed devices to use wider bandwidth channels. Existing FCC regulations⁴⁶ are designed to ensure that unlicensed devices do not cause interference with licensed users and

⁴⁴Sec. 6406 of Act. Pub. L. No. 112-96, 126 Stat. 156, 231.

⁴⁵In the Matter of *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, Notice of Proposed Rulemaking*, 28 FCC Rcd 1769 (2013).

⁴⁶47 C.F.R. § 15.5.

require operators of unlicensed devices to immediately correct the problem or cease operation if interference occurs.⁴⁷ NTIA completed an evaluation in January 2013 in response to requirements in the act that it study spectrum-sharing technologies and the risks to federal users associated with allowing unlicensed devices to share the 5.9 GHz band. NTIA concluded that further work was needed to determine whether and how the risks identified can be mitigated and is currently collaborating with federal and industry stakeholders, as well as FCC, to conduct a quantitative analysis of potential mitigation strategies.⁴⁸ FCC officials told us that they are unlikely to act further on a rulemaking in this area until NTIA's analysis is complete.⁴⁹

Although existing FCC regulations are designed to ensure that unlicensed devices do not cause interference, four automobile manufacturers and 16 experts we interviewed expressed concern or uncertainty about the potential effects of allowing unlicensed devices to share the 5.9 GHz band. One automobile industry group said that its members are not opposed to opening the 5.9 GHz band for sharing but emphasized the importance of understanding the implications of doing so to ensure that it will not hinder critical V2V safety applications. As part of the federal rulemaking process, FCC sought public comments on potential approaches to help minimize any potential harmful interference.⁵⁰ In response, one automobile manufacturer wrote that it is very concerned that V2V technologies and unlicensed devices will not be able to coexist on the 5.9 GHz band. This automobile manufacturer recommended that FCC proceed with extreme caution when allowing sharing of the 5.9 GHz

⁴⁷In its February 2013 Notice of Proposed Rulemaking, FCC stated that unlicensed devices typically operate at very low power over relatively short distances and often employ various techniques, such as dynamic spectrum access or listen-before-talk protocols, to reduce the interference risk to others as well as themselves. The primary operating condition for unlicensed devices is that the operator must accept whatever interference is received and must correct whatever interference is caused.

⁴⁸See Department of Commerce, *Evaluation of the 5350-5470 MHz and 5850-5925 MHz Bands Pursuant to Section 6406(b) of the Middle Class Tax Relief and Job Creation Act of 2012* (Washington, D.C.: January 2013).

⁴⁹FCC officials told us that they expect NTIA to finalize its recommendations for FCC by December 2014 and that, while FCC has generally stated that it would wait for the outcome of NTIA's studies before acting, FCC reserves the right, based on the record developed in the proceeding or changed circumstances, to act prior to that time.

⁵⁰78 Fed. Reg. 21320, April 10, 2013.

band, stating that V2V technologies cannot tolerate harmful interference and suggesting that every potential signal loss could render V2V communications ineffective at a moment in which they could protect drivers' lives. Members of the VIIC also noted that the development and testing of V2V technologies has always assumed use of the 5.9 GHz band. Because of this, one expert we interviewed suggested that opening the 5.9 GHz band for sharing would create an added burden for both automobile manufacturers and suppliers, which would have to consider technical steps to make coexistence with unlicensed devices feasible and conduct additional testing to maintain confidence that V2V technologies will work as envisioned. In addition, DOT coordinated with NTIA to submit its concern through comments to FCC that sharing the allocation could degrade the performance of V2V safety applications.

As NTIA continues its analysis of potential risk mitigation strategies, DOT officials told us that the department is working cooperatively with the agency to examine spectrum-sharing arrangements that have been proposed for the 5 GHz band and expects results of this analysis to be available in spring 2014. According to DOT officials, the automobile and Wi-Fi industries are discussing other possible spectrum sharing techniques but specific approaches have not yet been defined.

Human Factors

Because V2V technologies require drivers to take actions based on warning messages,⁵¹ the ultimate effectiveness and safety benefits of V2V technologies depend upon how well drivers respond to the warnings. Addressing the human factors that affect how drivers will respond includes minimizing the risk that drivers could become too familiar with or overly reliant upon warnings over time and fail to exercise due diligence in responding to them, assessing the risk that V2V warnings could distract drivers and present new safety issues, and determining what types of V2V warnings will maximize driver response.

The challenges posed by human factors are in many ways similar to those posed by sensor-based crash avoidance technologies and some other vehicle technologies. However, human factors issues may present even greater challenges to V2V technologies. One automobile manufacturer explained that, since not all vehicles in the United States

⁵¹As discussed earlier, warnings messages can be provided in a number of forms, including beeps or other audio warnings, bright lights, and seat vibrations.

will be equipped with V2V technologies in the early years of their deployment, it is unknown how drivers will adjust their behavior to account for the fact that not all of the vehicles on the road are capable of providing data. By contrast, with sensor-based technologies, drivers know that their vehicle's warning system is not dependent on the presence of similar technologies in nearby vehicles. Further, the potential introduction of aftermarket V2V devices with a lower level of integration with a vehicle's existing internal network could create additional human factors challenges if aftermarket device warning messages and data are less robust than fully integrated systems. For these reasons, one automobile manufacturer said that it is unrealistic to expect aftermarket devices to perform in all situations.

Automobile manufacturers have already developed different approaches to issuing warnings to drivers for existing sensor-based crash avoidance technologies. Three experts we interviewed suggested that the manner in which V2V warnings are issued to drivers should be allowed to vary among automobile manufacturers once basic standards are put in place. However, two experts suggested that the manner in which V2V warnings are issued to drivers should be similar across vehicles to avoid the confusion that might arise from receiving different types of warnings in similar situations when driving a different vehicle (e.g., a rental car).

NHTSA has a research program in place to develop human factors principles that may be used by automobile manufacturers and suppliers as they design and deploy V2V technology and other safety technology driver-vehicle interfaces that provide warnings to drivers. This program is evaluating alternative approaches to issuing warnings relative to effectiveness and potential driver distraction. In addition, DOT has surveyed drivers participating in the Safety Pilot about driver distraction, in addition to other topics, and collected data on driver responses to various V2V warnings. NHTSA has also sponsored other research on driver warnings—including initial research on the potential standardization of warnings across automobile manufacturers—and is planning to complete a compendium of research findings in late 2013. Based on research in this area, NHTSA has worked with stakeholders to develop design principles for V2V driver-vehicle interfaces, which NHTSA plans to

publish in April 2014.⁵² DOT continues to determine next steps in this area.⁵³

Liability Issues

Six automobile manufacturers and 17 experts we interviewed expressed concern about the challenge posed by uncertainties related to potential liability in the event of a collision involving vehicles equipped with V2V technologies. This challenge is manifested in a number of potential liability issues and questions that are unanswered at this time:

- One automobile manufacturer said that because V2V technologies offer warnings that are based in part on data transmitted by other vehicles—as opposed to sensor-based systems that collect data solely from a vehicle’s surroundings—it could be harder to determine whether fault for a collision between vehicles equipped with V2V technologies lies with one of the drivers, an automobile manufacturer, the manufacturer of a V2V device, or another party.
- One expert suggested that, because V2V data may be needed to determine fault in the event of a collision, there could be challenges in determining who owns the data transmitted between vehicles. This expert suggested that establishing rules regarding V2V data ownership would, in the event of a collision, help to answer questions about which parties have access to the data.
- There may be challenges in determining liability if V2V technologies do not work appropriately—for example, if data transmission is delayed due to channel congestion, hacking into the system, or inaccurate GPS readings.
- Four automobile manufacturers shared their concern that the introduction of aftermarket V2V devices into vehicles already on the road would create additional liability issues. One automobile manufacturer explained that this is because it is difficult to integrate aftermarket devices into a vehicle’s existing internal network,

⁵²According to DOT officials, these principles address how to minimize the potential for driver distraction. They include a conceptual framework that will address, among other things, how to time the presentation of warning messages to drivers and how to prioritize multiple messages.

⁵³For example, DOT plans to develop a driver-vehicle interface software-evaluation tool that will allow the automobile industry to evaluate the distraction potential of possible types of driver-vehicle interfaces. According to DOT officials, this tool will be finalized in 2015.

potentially making it more difficult to gather and transmit the same degree of information as a fully integrated device and, therefore, making it more difficult to determine the cause of a collision.

Automobile manufacturers may be reluctant to move forward with plans to install V2V technologies in their newly manufactured vehicles because of the uncertainty that accompanies these liability issues. Citing some automobile manufacturers' concerns about the liability risks posed by V2V technologies, members of the VIIC have suggested that additional work needs to be done to estimate the potential liability and risks associated with the deployment of V2V technologies and determine ways to mitigate that risk. One automobile manufacturer and two experts suggested that congressional action could be needed to limit the liability levels of automobile manufacturers in the event of a V2V device malfunction. One of these experts suggested that legislation setting forth liability limits for V2V devices that are shown to meet certification tests and function according to regulations and standards may be appropriate. However, one expert suggested that all vehicle technologies involve liability issues and that if the automobile industry ensures that V2V technologies work properly before deployment, V2V technologies should not pose any greater liability risks than existing sensor-based crash avoidance technologies.

DOT officials told us that they do not believe that V2V technologies pose any greater liability issues for automobile manufacturers than existing sensor-based crash avoidance technologies and therefore do not believe that related legislation is necessary. One expert we interviewed suggested that DOT should help guide the process of determining who or what entity owns the data transmitted between vehicles by V2V technologies as that knowledge would make it easier to determine liability in the event of a crash. Another expert suggested that DOT will have a role to play in helping to address liability issues once the specifics of the future deployment of these technologies become clearer.

Public Acceptance

DOT and the CAMP VSC 3 Consortium conducted Driver Acceptance Clinics in 2011 and 2012 to obtain volunteer drivers' feedback on V2V technologies, among other purposes, and participants rated the

desirability and usefulness of these technologies highly.⁵⁴ However, according to stakeholders and experts we interviewed, obtaining broad public acceptance could present a challenge to deployment, as concerns related to driver privacy and the limited potential benefits of V2V technologies in the early years of their deployment could impede overall public acceptance of these technologies.

- *Privacy concerns:* Public interest groups we interviewed said that overcoming concerns about privacy under a system that involves the sharing of data among vehicles will pose a challenge. One group suggested that the possibility that V2V data could be obtained by third parties such as law enforcement agencies could harm the deployment of these technologies. Similarly, one expert suggested that public acceptance of V2V technologies might be limited without rules prohibiting the use of vehicles' speed and location data to issue tickets or track drivers' movements. Three experts we interviewed suggested that legislation may be needed to limit the potential use of V2V data. Representatives of automobile manufacturers that are members of the VIIC stated that, although the security system under development is being designed to ensure data privacy through a structure that prevents the association of a vehicle's V2V communication security certificates with any unique identifier of drivers of their vehicles, the potential perception of a lack of privacy is a challenge. Further, one automobile manufacturer that is part of the VIIC said that it could be difficult to explain how V2V technologies work to the public without raising concerns related to privacy.⁵⁵
- *Perception of functionality:* Public acceptance of V2V technologies could also be negatively affected by drivers' perception of the technologies' limited functionality, especially when few vehicles are

⁵⁴Six clinics were conducted across the country between August 2011 and January 2012. The goals of the clinics were to promote V2V technologies, to assess their performance and reliability, and to obtain drivers' feedback. Over 90 percent of participants said that they would like to have V2V technology features in their vehicles and almost 80 percent reported having a high level of understanding of how these technologies work.

⁵⁵We have previously reported on the challenges faced in protecting the privacy of consumer data collected by private companies, noting that entities have not consistently implemented recommended practices, such as notifying users about the collection of their data and placing limits on the retention of data, or consistently disclosed which third parties are given access to such information. See GAO, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*, [GAO-12-903](#) (Washington, D.C.: Sept. 11, 2012).

equipped with V2V devices in early years. As mentioned earlier, when there are few equipped vehicles on the roads, drivers may see limited benefits of V2V technologies as they may not frequently encounter similarly equipped vehicles and infrequently receive warning messages in potential collision scenarios. Some experts said that limited benefits in the early years of deployment might pose challenges to consumer acceptance of V2V technologies. For this reason, six experts we interviewed suggested that the simultaneous introduction of applications with mobility applications would help provide benefits to drivers when deployment is low. For example, one expert suggested that mobility applications capable of helping drivers avoid congested roads or notifying them of a broken-down car ahead in the roadway would provide more apparent benefits to drivers, even with a low rate of deployment of V2V technologies.⁵⁶ In addition, seven experts we interviewed suggested that it would be helpful for either DOT or automobile manufacturers to reach out to customers to communicate the potential safety benefits of V2V technologies in advance of deployment in order to increase public acceptance of these technologies.

DOT officials told us that the department recognizes that public acceptance needs to be considered for the deployment of V2V technologies and noted that they have worked closely with automobile manufacturers and other stakeholders to develop a technical approach that limits risks to individual privacy. DOT officials have emphasized the need to distinguish between the ability to identify bad actors through a V2V communication security system and the ability to monitor the movements of individual vehicles. DOT stated that as currently conceived, a V2V communication security system would contain multiple technical, physical, and organizational controls to minimize privacy risks—including the risk of vehicle tracking by individuals and government or commercial entities. According to DOT officials, after NHTSA decides whether to proceed with a rulemaking and it is known what entity will provide the security for V2V technologies, the department will perform a

⁵⁶However, such mobility applications may require the deployment of vehicle-to-infrastructure technologies.

comprehensive Privacy Impact Assessment, as required by law,⁵⁷ to determine how to balance individual privacy, data security, and safety. DOT officials have emphasized that, to ensure transparency, it will be important to communicate what V2V data is generated by a vehicle, the extent to which it can be linked to drivers, and who or what entities—both legally and technologically—will be able to collect, use, and share the data. DOT officials told us that the department will continue to assess any risks to privacy posed by the introduction of V2V technologies and identify mitigation measures to minimize those risks as more aspects of a system of V2V communications are defined. DOT officials also said that, since its current authority to regulate the interception and use of V2V data is limited, the department might express a strong policy preference or make recommendations to Congress for limitations on the use of V2V data by entities over which the department lacks regulatory authority.

DOT officials told us that the department does not currently have a specific plan about how to proceed with public outreach efforts because NHTSA has not yet decided whether a rulemaking is appropriate at this time. Additional DOT efforts to address other challenges facing the deployment of V2V technologies could help increase their public acceptance. For example, DOT is collecting data from the Safety Pilot regarding the acceptance of V2V technologies by participating drivers. Furthermore, DOT's ongoing development of guidelines for the implementation of driver-vehicle interfaces to address human factors challenges could help increase overall acceptance of these technologies. In addition, DOT has plans for further research on vehicle-to-infrastructure technologies, which could provide additional safety benefits and enable the types of mobility applications that some experts suggested could help increase public acceptance of V2V technologies. Further, DOT is working with industry stakeholders to develop clear certification standards for aftermarket devices, along with all other V2V devices, and is considering incentives to encourage drivers to purchase these devices.

⁵⁷Consolidated Appropriations Act for 2005, Pub. L. No. 108-447, Div. H, §522, 118 Stat. 2809, 3268. The objective of a Privacy Impact Assessment is to determine if collected personal information data is necessary and relevant. These assessments are used to identify and address information privacy when planning, developing, implementing, and operating individual agency information management systems and integrated information systems. They assess security and privacy risks associated with operating information systems that collect, access, use, or disseminate personal information.

Status of DOT Planning for
V2V Technology
Deployment

DOT has indicated that its 2015 to 2019 ITS strategic plan—currently under development and expected to be issued in early 2014—will focus on the challenges facing the deployment of V2V technologies. As noted earlier, DOT officials told us that they do not want to take certain actions, such as determining the structure of a V2V communication security system, until after NHTSA’s late 2013 decision on how to proceed regarding V2V technologies. DOT has stated that the department’s forthcoming plan will include details of near term efforts to further develop the technical framework and management structure of a V2V communication security system and consideration of incentives needed to support the eventual deployment of V2V technologies to the U.S. vehicle fleet. In addition, DOT plans to develop an understanding of how the public views connected vehicle technologies and their benefits in order to develop effective methods for describing the value of V2V technologies to users in the context of partial deployment.

According to DOT, the strategic vision for the 2015 to 2019 ITS strategic plan is to improve safety, mobility, and environmental mitigation through connected vehicles and to enable a transportation system that builds upon the capabilities of V2V technologies and vehicle-to-infrastructure technologies. In line with this goal, as noted earlier, DOT is planning for additional research, including research conducted with the automobile industry, into vehicle-to-infrastructure technologies. In addition, by defining how an automated vehicle fleet can be introduced with limited impact to current infrastructure and researching how increases in the degree of automation of the U.S. vehicle fleet could have liability implications for stakeholders, DOT has stated that it plans to prepare for the introduction of autonomous vehicles to a connected vehicle environment featuring both V2V and vehicle-to-infrastructure technologies.

Costs of V2V Technologies Are Being Studied and Are Likely to Be Influenced by Various Factors Including Specifics of V2V Communication Security System

DOT and the automobile industry, through the CAMP VSC 3 Consortium, are currently analyzing the total costs of deploying V2V technologies, which include the costs of in-vehicle components and the costs associated with a V2V communication security system. DOT is currently obtaining estimates of the costs of in-vehicle V2V components from automobile manufacturers and industry suppliers and has engaged a contractor to study the potential costs of providing V2V communications security through a number of possible technical and management options. NHTSA will use these cost estimates to inform its decision on how to proceed with V2V technologies later this year. In addition, the CAMP VSC 3 Consortium is now conducting an independent analysis of potential security system costs. According to an official with that organization, this study should be completed in late 2013 and the consortium will provide input and comments on the key assumptions of DOT's cost study as well. Despite these efforts, all of the automobile manufacturers we interviewed told us that they had not yet completed any formal studies estimating V2V technology costs. We also conducted a literature search for published studies discussing potential V2V technology costs and were unable to identify any such studies. Finally, we asked the experts we interviewed to identify studies on the potential costs of deploying V2V technologies; none of the 21 experts were able to identify any studies beyond those now being conducted by DOT or the CAMP VSC 3 Consortium.

All of the automobile manufacturers we interviewed said that it is difficult to estimate the costs of in-vehicle V2V components at this time because too many factors remain unknown. According to both automobile manufacturers and experts we interviewed, a number of factors will influence the costs of in-vehicle V2V components:

- *Volume:* Five experts and two automobile manufacturers we interviewed pointed out that as the volume of V2V components produced increases, the per-unit costs are likely to decrease due to the economies of scale in manufacturing. Thus, a federal requirement that automobile manufacturers install V2V technologies in newly manufactured vehicles would likely result in lower per-vehicle costs of in-vehicle V2V components than would otherwise be the case.
- *Time frames:* The costs of in-vehicle components of V2V technologies may decline over time due to technological advances. Two automobile manufacturers we interviewed said that both the automobile and consumer electronics industries have been successful at driving down

the costs of other technologies over time and suggested that this also may occur with the cost of in-vehicle V2V components.

- *Degree of integration with existing vehicle technologies:* Automobile manufacturers already install sensor-based crash avoidance technologies in some vehicle models. The extent to which V2V technologies are integrated with the existing components of these and other technologies that use similar components will influence the costs of V2V technologies. For example, vehicles that already have GPS chips installed for navigation purposes may not need an additional GPS chip specifically for V2V technologies purposes. One expert and one automobile manufacturer we interviewed explained that automobile companies have been successful in integrating different technologies in their vehicles in recent years, resulting in reduced costs.
- *Federal requirements:* The specifics of any federal regulation regarding V2V technologies, including any possible regulation mandating their installation in new vehicles, would likely influence costs. For example, the introduction of requirements related to V2V technological specifications and standards, the use of hardware for V2V components, and the use of V2V safety applications would influence the ultimate costs of V2V technologies.

Although the costs of in-vehicle V2V components are difficult to estimate at this time, they may be modest compared to the price of a new vehicle. According to CAMP VSC 3 Consortium representatives, in-vehicle V2V components—including the DSRC components and GPS receiver—are already commercially available at a relatively low cost. A CAMP VSC 3 representative noted that although members of the partnership are unable to discuss potential V2V technology costs with one another due to antitrust concerns, they have agreed to focus their V2V technology development efforts on limiting their costs as much as possible. As a result, compared to the average sale price of a new vehicle—about \$31,000 in 2012, according to the National Automobile Dealers Association—the potential costs of these physical components may not add significantly to a vehicle's price. One expert we interviewed estimated that the costs of V2V components would add less than one percent to the price of a new vehicle. These costs may be less than the costs of sensor-based crash avoidance technologies, according to one industry association we interviewed, because sensors are more expensive.

At this time, the potential costs associated with a V2V communication security system are unknown as specifics of a security system remain undetermined. One expert we interviewed explained that since it is not yet known how the security system will look or how it will be organized or managed, no one has a good handle on those costs. According to DOT officials, how often vehicles must communicate with the security system and requirements of how security certificates will be provided will influence the ultimate cost of a V2V communication security system. Furthermore, it is currently not only difficult to estimate the potential costs, but unclear who or what entity—consumers, automobile manufacturers, DOT, state and local governments, or others—would pay the costs. Determining who or what entity will fund the system will likely prove challenging.

Although the potential costs of a V2V communication security system are unknown at this time, eight experts we interviewed noted that either these costs, or the costs of roadside equipment that may be needed, could be significant. One expert said that, given the need for continuous operation of a security system, the costs are likely to be much greater than the costs of in-vehicle V2V components. Potential sources of funding may also face challenges in providing it. For example, if roadside equipment is needed to support a security system, it could be costly in a nationwide deployment. Participants in a 2012 DOT-hosted workshop focused on connected vehicle security⁵⁸ noted that the costs of roadside equipment could range between \$25,000 and \$30,000 per installation, a cost that many state and local governments would find prohibitive if they were responsible for its financing.⁵⁹ In addition, three experts whom we interviewed said that the costs of ongoing maintenance and operation of such installations could also prove prohibitive. According to DOT officials, however, the potential costs of roadside equipment could be much lower if its installation were to be integrated into already planned construction work at selected sites. They also noted that these costs should decline

⁵⁸DOT Research and Innovative Technology Administration, *Enabling a Secure Environment for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Transactions: April 2012 Public Workshop*, (Washington, D.C.: June 2012).

⁵⁹As we have reported in the past, funding constraints have posed a significant challenge to the deployment of intelligent transportation systems technologies by state and local governments. See GAO, *Intelligent Transportation Systems: Improved DOT Collaboration and Communication Could Enhance the Use of Technology to Manage Congestion*, [GAO-12-308](#) (Washington, D.C.: Mar. 19, 2012).

over time due to declining costs of technologies and increased volumes of production.

Agency Comments

We provided a draft of this report to the Secretary of Transportation and the Chairman of the Federal Communications Commission for review and comment. DOT and FCC both provided comments via email that were technical in nature. We incorporated these comments as appropriate.

We are sending copies of this report to interested congressional committees, the Secretary of Transportation, and the Chairman of the FCC. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-2834 or wised@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff that made significant contributions to this report are listed in appendix IV.



David J. Wise
Director, Physical Infrastructure Issues

Appendix I: Scope and Methodology

To address all of our objectives, we reviewed documentation of the efforts of the U.S. Department of Transportation (DOT) and automobile manufacturers related to vehicle-to-vehicle (V2V) technologies, such as the department's ITS Strategic Research Plan, 2010 - 2014 Progress Update 2012 and documentation on completed and ongoing research. We also interviewed officials from DOT's National Highway Traffic Safety Administration (NHTSA) and the Research and Innovative Technology Administration (RITA) about these efforts. We also interviewed officials with the Crash Avoidance Metrics Partnership (CAMP) Vehicle Safety Communications (VSC) 3 Consortium as well as, both collectively and individually, representatives from all of the following automobile manufacturers that currently comprise the Vehicle Infrastructure Integration Consortium: BMW, Chrysler, Ford,¹ General Motors, Honda, Hyundai-Kia, Mercedes-Benz, Nissan, Toyota, and Volkswagen. We also interviewed a V2V device supplier and representatives of industry and public interest groups knowledgeable on the topic of V2V technologies, such as the Alliance of Automobile Manufacturers and the American Automobile Association.

In addition, we collaborated with the National Academies of Sciences (NAS) to identify and recruit experts in vehicle-to-vehicle technologies. We provided NAS with criteria for selecting experts, which included: (1) type and depth of experience, including recognition in the professional community and relevance of any published work; (2) employment history and professional affiliations, including any potential conflicts of interest; and (3) other relevant experts' recommendations. NAS initially identified 35 experts knowledgeable in the areas of V2V technology development and interoperability, technology deployment, production of light-duty passenger vehicles, data privacy and security, legal and policy issues, and human factors issues related to V2V technologies. From that list, we selected and conducted structured interviews with 21 experts who represented domestic and international automobile manufacturers, suppliers of V2V devices, a telecommunications company, and state governments, as well as automotive industry experts and academic researchers (see table 1 for list of experts interviewed). In conducting our structured interviews, we used a standardized interview guide (see

¹While we interviewed Ford as part of group meetings with the Vehicle Infrastructure Integration Consortium and the CAMP VSC3 Consortium and interviewed a Ford official as an expert identified by the National Academies of Sciences, we did not otherwise individually interview Ford.

appendix II) to obtain consistent answers. During these interviews we asked, among other things, for expert views on the state of development of V2V technologies, the potential benefits of V2V technologies, their potential costs, and DOT’s role in developing V2V technologies. We also asked for each expert’s views on a number of already defined potential challenges facing the deployment of V2V technologies. We determined this initial list of potential challenges after initial interviews with DOT, industry associations, select automobile manufacturers, and other interest groups knowledgeable about V2V technologies. Prior to conducting the interviews, we pretested the structured interview guide with two of the selected experts to ensure our questions were worded appropriately and could be administered consistently. After conducting these interviews, we conducted a content analysis of expert responses relevant to each objective and counted the rating of each potential challenge discussed. See appendix III for a count of the ratings provided by experts on potential challenges facing deployment of V2V technologies.

Table 1: Subject Matter Experts Interviewed

Name	Affiliation^a
Roger Berg	DENSO
Chris Body	Kapsch TrafficCom
John Campbell	Battelle
Susan Chrysler	University of Iowa
Richard Deering	Richard Deering Associates
Thomas Dingus	Virginia Tech
Dorothy Glancy	Santa Clara University School of Law
John Kenney	Toyota
Bob Koeberlein	Idaho Transportation Department
Greg Krueger	Science Applications International Corporation (SAIC)
Mike Manser	University of Minnesota
Jim Misener	Independent consultant
Ravi Puvvala	Savari
Bob Rausch	Transcore
Russell Shields	Ygomi
Steve Shladover	California Partners for Advanced Transportation Technology (PATH)
Mike Shulman	Ford Motor Company
Kirk Steudle	Michigan Department of Transportation
Mitch Tseng	Tseng Infoserv

Name	Affiliation ^a
Bryant Walker Smith	Stanford Law School
William Whyte	Security Innovation

Source: GAO.

^aWe interviewed experts as individuals, not as representatives of any institution. We provide information on institutions to help readers identify experts.

We completed a literature search to obtain documentation, studies, and articles related to our objectives. Although this report focuses upon V2V technologies, our literature search was broadened to include any relevant work published in the past 10 years that was related to terms including “vehicle-to-vehicle communications,” “vehicle-to-infrastructure communications,” “vehicle-to-roadside communications,” or “intelligent vehicle highway systems.”

To specifically address the state of development of V2V technologies and their anticipated benefits, we conducted a site visit to Ann Arbor, Michigan, where we interviewed researchers from the University of Michigan Transportation Research Institute who are managing the Safety Pilot Model Deployment and toured areas of the city in which related infrastructure was installed. We also interviewed automobile manufacturers’ CAMP VSC 3 Consortium representatives in Farmington Hills, Michigan, and received a demonstration of V2V safety warnings in multiple potential crash scenarios. We also reviewed DOT’s May 2013 Description of Light-Vehicle Pre-Crash Scenarios for Safety Applications Based on Vehicle-to-Vehicle Communications report that estimates potential benefits of V2V technologies.

In addition, to specifically address the challenges facing the deployment of V2V technologies, we interviewed officials from the Federal Communications Commission and a privacy group to obtain their views on the potential challenges of spectrum allocation and data privacy, respectively, related to deployment of V2V technologies.

To specifically address the potential costs associated with V2V technologies, we discussed efforts to estimate costs with DOT and representatives of the CAMP VSC 3 Consortium and reviewed relevant documentation, such as the April 2012 public workshop entitled Enabling a Secure Environment for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Transactions, which DOT organized to facilitate discussion of communications security structures under development among public and private stakeholders. In addition, we asked all

automobile manufacturers we interviewed about the potential costs of V2V technologies.

We conducted this performance audit from October 2012 through November 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Structured Interview Guide for Experts Identified by the National Academies of Sciences

Questions for Connected Vehicle Technology Experts

(Experts identified by the Transportation Research Board of the National Academies)

Overview of GAO Review of Connected Vehicle Technologies

The United States Government Accountability Office (GAO) is undertaking work looking at the use of connected vehicle technologies (CVT) involving vehicle-to-vehicle (V2V) communications. These technologies allow vehicles to wirelessly communicate with one another through Dedicated Short Range Communications (DSRC); share data, such as data on vehicle location and speed; and provide drivers with warnings of potential collisions. GAO is examining these technologies at the request of the House Committee on Science, Space, and Technology and Committee on Transportation and Infrastructure, Subcommittee on Highways and Transit. Specifically, we are examining:

- (1) the progress of development of connected vehicle technologies that involve vehicle-to-vehicle communications and their anticipated benefits;
- (2) the challenges that affect the development and deployment of these technologies and their potential costs; and
- (3) how the U.S. Department of Transportation is leading efforts to address these challenges.

Our work is limited to CVTs involving V2V communications and we are not including vehicle-to-infrastructure (V2I) communications beyond the extent to which infrastructure may be needed to support V2V communications. We are reviewing efforts in the United States and not in other countries. In addition, our work is limited to passenger vehicles and we are not including commercial and transit uses.

Please keep the following in mind as you consider your responses to the questions:

- We use the term “stakeholders” to indicate organizations that have been or are expected to be involved in the development or deployment of CVTs involving V2V communications including, but not limited to, automobile manufacturers, parts suppliers, government agencies, and telecommunications companies.
- We use the term “CVTs involving V2V communications” to include devices that send and receive data, safety applications (such as Forward Collision Warning and Emergency Electronic Brake Lights Warning) that analyze data and provide warnings through driver-vehicle interfaces, and any security system(s) that may be needed to help establish trust between vehicles sharing data.
- We use the term “V2V devices” to represent the devices now being tested in the Safety Pilot Model Deployment in Ann Arbor, Michigan:¹
 - (1) Fully-integrated devices: these devices would be installed during vehicle production and send, receive and analyze vehicle data to generate driver warnings of potential collisions. Because they are fully integrated into vehicles, they can analyze additional vehicle data—such as steering wheel angle, acceleration rate, brake status and turn signal status—to provide more robust warnings to drivers and provide more complete data to other vehicles.

¹These devices are wireless and include components such as a GPS chip to determine vehicle location and an antenna for data transmission at 5.9 GHz using DSRC. Vehicles with these devices transmit data on vehicle location and speed (called “basic safety messages”).

-
- (2) Aftermarket safety devices: these devices, installed after vehicle production, send, receive, and analyze vehicle data to generate warnings of potential collisions. However, because they are not integrated with vehicles' electronics architecture and are thus unable to consider additional data, these devices may be limited in their warnings and driver-vehicle interface.
 - (3) Vehicle awareness devices: these devices are installed after vehicle production and are not connected to any vehicle systems. They send data on a vehicle's location and speed which may be received by other vehicles, but these devices do not generate driver warnings.

Status and Benefits of Vehicle-to-Vehicle Connected Vehicle Technologies

- 1) Please discuss your views on the status of development of CVTs that involve V2V communications in the United States, including progress made and successes to date.
- 2) In your opinion, what are some of the greatest potential benefits of CVTs that involve V2V communications?
 - a. Which potential V2V applications are likely to offer the greatest benefits and why?
- 3) What work, in your opinion, needs to be completed before such technologies are commercially feasible and available in the U.S.?
 - a. In your opinion, what is a realistic timeframe in which automobile manufacturers might begin to install these technologies in new vehicles being manufactured for the U.S. vehicle fleet?
- 4) According to a 2007 report by the U.S. DOT, CVTs involving V2V communications have the potential to address up to 76 percent of unimpaired roadway crashes, which could have the potential to greatly reduce the number of roadway fatalities that occur each year.
 - a. What views, if any, do you have on DOT's projection of these technologies' potential benefits?
 - b. Other than this study and DOT's Safety Pilot Driver Clinics and Model Deployment, are you aware of any other studies that estimate the potential benefits of V2V technologies?

Costs of Vehicle-to-Vehicle Connected Vehicle Technologies

- 5) To your knowledge, are there any studies that estimate the potential future costs associated with the deployment of CVTs involving V2V communications?
 - a. Specifically, are you aware of any work that has been done to estimate the costs associated with the deployment of (1) fully-integrated devices, (2) aftermarket safety devices, and (3) vehicle awareness devices?
- 6) To your knowledge, are there any studies that estimate the potential costs of the type(s) of security system(s) needed to support CVTs involving V2V communications, including any infrastructure that such a security system may require?
- 7) What factors may affect the costs associated with the deployment of CVTs involving V2V communications?

Challenges Associated with Vehicle-to-Vehicle Connected Vehicle Technologies

8) In your opinion, to what extent does each of the following issues present a challenge to the development and eventual deployment of CVTs that involve V2V communications? *(Place only one 'x' in each row below to indicate your response.)*

	Very great challenge ▼	Great challenge ▼	Moderate challenge ▼	Slight challenge ▼	No challenge ▼	Don't know ▼
a. Technical challenges in the development of each of the following V2V technologies:						
- V2V devices.....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- V2V safety applications.....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Driver-vehicle interface.....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- i. Please discuss the technical challenges being faced in the development of CVTs involving V2V communications.
- ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iii. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

	Very great challenge ▼	Great challenge ▼	Moderate challenge ▼	Slight challenge ▼	No challenge ▼	Don't know ▼
b. Technical development of a data security system to help establish trust between vehicles sharing information.....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- i. Please discuss any challenges posed by issues of technical development of a data security system to the development and deployment of CVTs involving V2V communications.
- ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iii. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
▼	▼	▼	▼	▼	▼

c. Standardization to ensure interoperability among different types of devices and vehicles.....

- i. Please describe the challenge that ensuring the interoperability of CVTs involving V2V communications presents to development and deployment of these technologies.
- ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iii. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
▼	▼	▼	▼	▼	▼

d. Deployment of V2V devices and applications into a great enough percentage of the U.S. vehicle fleet to realize significant benefits

- i. Please discuss the challenge(s) associated with the process of deploying V2V technologies across the U.S. vehicle fleet.
 - a. Please discuss any challenges presented by the potential need for less-than fully integrated aftermarket V2V devices.
- ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iii. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
▼	▼	▼	▼	▼	▼

e. Costs of deploying CVTs involving V2V communications (including V2V devices, safety applications, driver-vehicle interface, and security system).....

- i. Please discuss any challenge(s) posed by the costs associated with specific aspects of the deployment of CVTs involving V2V communications.
- ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iii. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
▼	▼	▼	▼	▼	▼

f. Potential need for roadside equipment required to support security system.....

- i. Please discuss the extent to which the potential need for roadside equipment to support V2V technologies may or may not present a challenge(s).
- ii. Please discuss the extent to which financing any roadside equipment needed for a system of V2V technologies may or may not present a challenge(s).
- iii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iv. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

**Appendix II: Structured Interview Guide for
Experts Identified by the National Academies
of Sciences**

Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
▼	▼	▼	▼	▼	▼

g. Establishment of a framework, including determination of roles and responsibilities, for management of a security system to support a V2V environment.....

- i. Please discuss the challenge(s) associated with the establishment of a governance structure for the management of a security system to support CVTs involving V2V communications.
- ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iii. Please discuss how U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
▼	▼	▼	▼	▼	▼

h. Establishing acceptable end user privacy

- i. Please discuss any challenges posed by issues of end user privacy to the development and/or deployment of V2V technologies.
- ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iii. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

	Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
	▼	▼	▼	▼	▼	▼
i. Public acceptance.....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
i. Please discuss the challenge of public acceptance to the development and deployment of V2V technologies.						
ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.						
iii. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.						

	Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
	▼	▼	▼	▼	▼	▼
j. Use of DSRC technology at 5.9 GHz frequency band.....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
i. Please discuss any challenge(s) presented by the decision to use DSRC technology to establish V2V communications to date and in the future.						
ii. The Federal Communications Commission allocated 75 MHz of spectrum in the 5.9 GHz band for vehicle safety and mobility applications. Please discuss any implications of the possibility of making the bandwidth set aside for CVTs for other uses.						
iii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.						
iv. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.						

Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
▼	▼	▼	▼	▼	▼

k. Human factors for V2V

communications (e.g. how warning messages affect driver performance)

□	□	□	□	□	□
---	---	---	---	---	---

- i. Please discuss the challenges that human factors pose to the development and eventual deployment of CVTs that involve V2V communications.
- ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iii. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
▼	▼	▼	▼	▼	▼

l. Liability issues (i.e. uncertainty related to legal responsibility for vehicle crashes after broad deployment of V2V devices)

□	□	□	□	□	□
---	---	---	---	---	---

- i. Please discuss the extent to which the broad introduction of V2V technologies to the U.S. vehicle fleet may pose potential challenges related to liability.
- ii. Does this issue present different challenges for different relevant stakeholders? If so, please discuss.
- iii. Please discuss how well U.S. DOT and other stakeholders are addressing this challenge and any additional steps they should take.

**Appendix II: Structured Interview Guide for
Experts Identified by the National Academies
of Sciences**

9) What additional challenges, if any, exist in the ongoing development and eventual deployment of CVTs that involve V2V communications? For each additional challenge, please discuss its extent, how it presents different challenges for different relevant stakeholders, and how well DOT and other stakeholders are addressing it and additional steps that they should take.

	Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
	▼	▼	▼	▼	▼	▼
a. _____	□	□	□	□	□	□

	Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
	▼	▼	▼	▼	▼	▼
b. _____	□	□	□	□	□	□

	Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
	▼	▼	▼	▼	▼	▼
c. _____	□	□	□	□	□	□

U.S. DOT's Role in Connected Vehicle Technologies

- 10) In your view, how well is U.S. DOT carrying out the following efforts related to the development and deployment of CVTs involving V2V communications?
- a. Evaluating the potential safety benefits of CVTs involving V2V communications
 - b. Considering the potential costs of deploying CVTs involving V2V communications
 - c. Supporting the development of V2V safety applications.
 - d. Conducting development and testing of V2V devices and promoting the development of technical standards.
 - e. Communicating and collaborating with key stakeholders, including automobile manufacturers and suppliers and other interested parties.
 - f. Identifying policies to help lead to deployment of CVTs involving V2V communications.
- 11) Please discuss how, in your opinion, each of the following possible actions regarding CVTs involving V2V communications would affect automobile manufacturer costs, new vehicle costs, vehicle production, and deployment of CVTs involving V2V communications:
- a. A federal mandate for automobile manufacturers to install equipment necessary to support V2V safety applications?
 - b. The inclusion of V2V safety applications in NHTSA's New Car Assessment Program?²
 - c. Continued research and development?
- 12) Do you have any views not already discussed on the development and deployment of CVTs involving V2V communications, including any additional actions U.S. DOT should take?

²Doing so would enable automobile manufacturers to earn higher government safety ratings for vehicles that support V2V safety applications. For more information on the New Car Assessment Program, please see www.safercar.gov.

Appendix III: Expert Ratings of Potential Challenges Facing Deployment of Vehicle-to-Vehicle Technologies

As part of our review, we conducted 21 structured interviews with individuals identified by the National Academies of Sciences to be experts on vehicle-to-vehicle (V2V) technologies (see table 1 in appendix I for list of experts interviewed). In conducting these structured interviews, we used a standardized interview guide (see Appendix II) to obtain consistent answers. During these interviews we asked, among other things, for each expert's views on a number of already defined potential challenges facing the deployment of V2V technologies. The ratings provided by the experts for each of the potential challenges discussed are shown in table 2 below. To inform our discussion of the challenges facing the deployment of V2V technologies, we considered these ratings as well as experts' responses to open-ended questions.

Table 2: Expert Ratings of Potential Challenges Facing Deployment of Vehicle-to-Vehicle Technologies

Potential Challenge	Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
Technical challenges in the development of each of the following V2V technologies:						
V2V devices	0	2	9	7	2	1
V2V safety applications	0	3	12	4	1	1
Driver-vehicle interface	4	1	9	5	1	1
Technical development of a data security system to help establish trust between vehicles sharing information	6	6	4	3	0	2
Standardization to ensure interoperability among different types of devices and vehicles	1	6	6	6	2	0
Deployment of V2V devices and applications into a great enough percentage of the U.S. vehicle fleet to realize significant benefits	4	4	8	2	0	3
Costs of deploying connected vehicle technologies involving V2V communications (including V2V devices, safety applications, driver-vehicle interface, and security system)	2	4	4	7	3	1
Potential need for roadside equipment required to support security system	1	8	6	3	0	3
Establishment of a framework, including determination of roles and responsibilities, for management of a security system to support a V2V environment	4	8	6	1	1	1
Establishing acceptable end user privacy	6	1	7	4	1	2
Public acceptance	2	7	7	3	1	1
Use of DSRC technology at 5.9 GHz frequency band	6	4	5	1	0	5
Human factors for V2V communications (e.g. how warning messages affect driver performance)	4	3	6	5	0	3

Appendix III: Expert Ratings of Potential Challenges Facing Deployment of Vehicle-to-Vehicle Technologies

Potential Challenge	Very great challenge	Great challenge	Moderate challenge	Slight challenge	No challenge	Don't know
Liability issues (i.e. uncertainty related to legal responsibility for vehicle crashes after broad deployment of V2V devices)	4	4	5	3	0	5

Source: GAO analysis of structured interviews with experts identified by the National Academies of Sciences.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

David Wise, (202) 512-2834, or wised@gao.gov

Staff Acknowledgments

In addition to the individual above, Judy Guilliams-Tapia, Assistant Director; Melissa Bodeau; Leia Dickerson; David Hooper; Terence Lam; Maren McAvoy; Josh Ormond; Madhav Panwar; Matthew Rosenberg; Chad Williams; and Elizabeth Wood made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

