



POLICY & ACTION FROM CONSUMER REPORTS

April 12, 2017

Docket Management Facility, M-30
U.S. Department of Transportation
1200 New Jersey Avenue S.E.
West Building, Ground Floor, Room W12-140
Washington, D.C. 20590

Submitted via www.regulations.gov.

**Comments of Consumers Union to the
National Highway Traffic Safety Administration on the Notice of Proposed Rulemaking:
Federal Motor Vehicle Safety Standards; V2V Communications¹
Docket No. NHTSA-2016-0126**

Consumers Union, the policy and mobilization arm of Consumer Reports,² welcomes the opportunity to comment on the notice of proposed rulemaking by the National Highway Traffic Safety Administration (NHTSA) regarding Federal Motor Vehicle Safety Standard No. 150, which would mandate vehicle-to-vehicle (V2V) communications capability on all new light vehicles. The proposed rule also would standardize the content and format of V2V transmissions, setting a common specification for basic safety messages sent to other vehicles about a car's position, speed, heading, acceleration, trajectory, and other core vehicle information.

We appreciate NHTSA's extensive work to investigate the potential traffic safety benefits of V2V-based features, and agree with the agency that V2V safety applications could significantly reduce the number and severity of motor vehicle crashes—particularly because they may address crashes that cannot be prevented by current in-vehicle camera- and sensor-based technologies. Accordingly, we support the establishment of a mandatory safety standard governing the use of wireless communications for crash prevention purposes, provided that the rule reasonably accounts for potential future developments and that manufacturers and suppliers meet baseline, enforceable standards to protect the privacy and security of communications.

¹ 82 Fed. Reg. 3854-4019 (Jan. 12, 2017).

² Consumers Union is the policy and mobilization arm of Consumer Reports, an independent, nonprofit organization that works side by side with consumers to create a fairer, safer, and healthier world. As the world's largest independent product-testing organization, Consumer Reports uses its more than 50 labs, auto test center, and survey research center to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

Public Safety Demands the Adoption of Advanced Crash Prevention Technologies

Motor vehicle crashes are the cause of an ongoing public health crisis, and it is an urgent necessity to find ways to prevent more traffic deaths and injuries. Preliminary estimates for 2016 indicate that more than 40,000 people died from motor vehicle crashes in the U.S. in 2016, a total that is 14% higher than 2014 and far outpaces the increase in vehicle miles traveled over that same time.³ Some 4.6 million people required medical attention last year because of car crashes, which, overall, had a cost to society of approximately \$432 million.⁴

While improvements to crashworthiness are far from exhausted, Consumers Union and Consumer Reports believe that the continued development and adoption of crash prevention technologies will play a major role in countering the increasing trend of deaths and injuries on our roads. We have urged manufacturers to make these technologies more readily available to consumers, including by providing emerging camera- and sensor-based safety features to consumers without the purchase of an expensive options package, and by making proven, lifesaving features like forward collision warning with automatic emergency braking (FCW/AEB) standard equipment. A car's safety makes up a major part of its overall score in our ratings, and to incentivize the rollout of front-crash prevention technologies, there are bonus points that we only award to those cars that have made FCW/AEB standard.⁵

We also have followed the research and testing of crash prevention technologies based on V2V communications, which would seek to promote motor vehicle safety by establishing a means for cars to “talk” to one another and share important safety-related information through wireless transmissions. We covered and responded to the release of NHTSA's notice of proposed rulemaking in December 2016,⁶ and also recently explored the various ways that V2V communications can improve the safety of consumers on the road.⁷ Overall, because these systems involve the use of radio signals and can transmit safety-related data without a direct line of sight, we think they have significant potential to improve traffic safety—in a manner complementary to other crash avoidance technologies—by giving drivers an early warning of yet-unseen crash hazards posed by other vehicles.

Vehicle-to-Vehicle Communications Will Likely Be an Important Part of the Solution

We welcome NHTSA's notice of proposed rulemaking on V2V communications, as safety applications based on this technology will likely be an important part of the solution in

³ National Safety Council, *NSC Motor Vehicle Fatality Estimates* (Feb. 15, 2017) (online at www.nsc.org/NewsDocuments/2017/12-month-estimates.pdf).

⁴ *Id.*

⁵ See “Car Safety at Any Price,” Consumer Reports (Feb. 23, 2016) (online at www.consumerreports.org/car-safety/car-safety-at-any-price).

⁶ “DOT Wants Wireless Cars in 5 Years to Prevent Accidents,” Consumer Reports (Dec. 13, 2016) (online at www.consumerreports.org/car-safety/DOT-wants-wireless-cars-five-years).

⁷ “CES Preview: What to Expect in New Car Technology,” Consumer Reports (Dec. 28, 2016) (online at www.consumerreports.org/cars-ces-preview--car-technology-taking-the-spotlight); “How Cars That Talk to Roadways, Traffic Signals Can Help Drivers,” Consumer Reports (Jan. 4, 2017) (online at www.consumerreports.org/automotive-technology/taking-the-latest-in-car-technology-out-for-a-spin).

response to increasing rates of traffic injuries and deaths. The crash population identified by the agency as potentially addressable by V2V is significant, including 3.4 million light-vehicle to light-vehicle crashes every year—or 62% of the total—involving an estimated 7,000 fatalities and 1.8 million injuries annually.

We strongly agree with NHTSA that V2V-based technologies and camera- or sensor-based technologies should be viewed as complementary and not competing. This view should extend to onboard technologies that may be helping lay the groundwork for automated vehicles, as current semiautonomous driving technologies rely on the same “seeing” or “sensing” systems that vehicle-resident crash avoidance technologies do. Consumer Reports testing has found that while these systems can be useful, they are not foolproof—with some systems having trouble performing correctly due to environmental conditions involving especially sunny, rainy, snowy, or icy days.

V2V communications systems in cars would bring additional vital safety information to the table. As demonstrated in the Connected Vehicle Safety Pilot Model Deployment, the use of these systems for safety applications including Intersection Movement Assist and Left Turn Assist have proven effective in mitigating or preventing potential crashes. These two applications, in particular, rely on vehicle information that is not attainable simply by what can be seen or sensed by vehicle-resident technologies, and in the Model Deployment, it was demonstrated that they have a unique ability to address particularly deadly intersection crashes in a manner that vehicle-resident technologies currently cannot.

The Model Deployment also demonstrated the effectiveness of V2V-based FCW and Blind Spot/Lane Change Warning applications. These represent examples of applications that could use both V2V-based and vehicle-resident technologies to enhance safety. We also suggest that current rear cross-traffic warning systems could be enhanced by the use of V2V technology.

In light of the potential safety benefits, and recognizing that all consumers—not just those who purchase a luxury vehicle or a separate V2V system—deserve the added level of protection they provide, we generally support NHTSA’s intention to mandate V2V capability as a federal requirement for all new light vehicles. We support this proposal over an “if-equipped” mandate that would only set rules for the operation of V2V systems optionally included by manufacturers in new vehicles. We agree with the agency that the “if-equipped” regulatory alternative would be likely to inhibit the technology’s potential safety benefits by leading to greater uncertainty in V2V technology development, delayed deployment, and ultimately an insufficient fraction of the vehicle fleet being equipped with V2V capability.

We also generally support the performance criteria proposed by NHTSA and its applicability to V2V systems in both new cars and aftermarket products. This includes the agency’s proposals to set transmission range and reliability requirements with a specified test method, as well as generally appropriate data elements for basic safety messages, including reasonably selected event flags.⁸ In a final rule, we would urge NHTSA to follow the proposed

⁸ With regard to NHTSA’s request for comments on a possible maximum transmission range, we urge the agency to consult with other federal agencies and independent experts to confirm that the absence of a maximum transmission range would not lead to signal overload or misinterpretation by V2V devices of a signal being received. For

approach toward these performance criteria, and to require, as proposed, a strong Public Key Infrastructure approach to message authentication, specific practices and procedures for misbehavior reporting and malfunction indication,⁹ and V2V-enabled vehicles to have built-in over-the-air update capability for critical software updates.

For software updates, NHTSA should consider setting a requirement under which the default setting is for security updates to be accepted, but under which manufacturers also are required to provide consumers meaningful options in choosing how updates are applied and how much they want the updates to occur automatically versus being asked to consent. One such option could be a “timeout” feature, in which critical updates occur automatically after the consumer has been given a certain amount of time to affirmatively consent but has taken no action. Another option could be a triage of sorts, under which an update would occur automatically or require affirmative consent depending on its importance to performance, operation, and security as well as its relevance to the driver.¹⁰ Regardless of an update’s importance, we suggest that consumer messages regarding updates should be particularly clear about changes if they in any way alter the signals, alerts, or other information with which the driver directly interfaces. We note that by the time of implementation, new vehicles are expected to include the video screens necessary for the agency’s rear visibility standard, and that these screens also could be used for clear alerts and disclosure to consumers related to software updates.

Regarding cybersecurity more broadly, NHTSA properly recognizes that the protection of data security is a critical element of motor vehicle safety, particularly as cars come to rely more heavily on electronics and software-based systems. While we have urged and continue to urge NHTSA to develop a mandatory safety standard for cybersecurity based on sufficient public research and consultation with other federal agencies, and to require full reporting of cybersecurity considerations and vulnerabilities, we appreciate that the agency refers in the proposed V2V rule to the importance of covered entities following the October 2016 Cybersecurity Best Practices. We agreed with most of NHTSA’s recommendations to industry in our November 28, 2016, comments on the Best Practices, and suggested certain enhancements in the interest of bolstering the document.¹¹

More specifically, we appreciate that NHTSA has considered several security risks associated with V2V devices themselves. The agency is on the right track—in particular, by recognizing that security requirements should be included in regulatory text, that V2V systems

example, if multiple major intersections are close together, and there is no maximum transmission range, we would urge NHTSA to ensure that a V2V device could decipher useful information among all the signals it may receive from other devices in other vehicles.

⁹ These warnings to drivers should involve a combination of both audible and visual messages. It is particularly important to include specific text to the effect that the system is misbehaving or is not operable, rather than utilizing just audible or illuminated symbols, which may be confused with other warnings.

¹⁰ Elimination of “false positive” warnings through software updates could be one example of an over-the-air update that would be invisible to the user, but key to the performance of the system, so it could be a candidate for the type of update that consumers might want updated without requiring consent.

¹¹ See Comments of Consumer Reports and Consumers Union to the National Highway Traffic Safety Administration on the Request for Comment on Cybersecurity Best Practices for Modern Vehicles (Nov. 28, 2016) (online at www.regulations.gov/document?D=NHTSA-2016-0104-0995).

should employ a security level of at least 128-bit encryption, and that additional work is needed on the security of message authentication. However, we urge NHTSA to propose full data security-related regulatory text for public comment. So as not to delay a final rule, it should do so during the period when it is evaluating comments on the current notice of proposed rulemaking.

Any Mandatory Standard Should Reasonably Account for Potential Future Developments

We generally support NHTSA's intention to move forward with the rulemaking to set a new federal safety standard for V2V communications, including to mandate V2V capability in new cars and set performance criteria for both new cars and aftermarket products. As it does so, however, we urge the agency to keep in mind that any mandatory standard should reasonably account for potential future developments. In other words, while NHTSA prioritizes interoperability, the agency also should carefully assess the various directions that technological innovation could take the market for wireless, vehicle-to-vehicle safety communication devices. Such an approach would yield the strongest possible standard and the one that is likeliest to be useful well into the future.

This topic is one that NHTSA clearly considered as it developed the notice of proposed rulemaking. For instance, we appreciate the appropriate balance struck by the agency to specify requirements for V2V devices' range, reliability, and test methods, while also choosing not to specify requirements with regard to certain elements of a V2V device or a V2V-equipped vehicle, such as antenna configuration and placement. Throughout the proposed rule, NHTSA makes clear that its conclusions and proposals rely on the best currently available scientific data, and that it must make reasoned judgments based on the information that it has. The agency also is clear that it will review relevant new evidence in the future, and in order to ensure an effective regulation, may propose revisions to a subsequent proposed or final rule as necessary and appropriate to reflect changes in the overall state of the evidence.

At the same time, regarding other portions of the rule, we urge NHTSA to ensure that it chooses its words carefully in the final standard so that it is as performance-oriented as possible, and as neutral as possible toward which specific technologies are used for V2V communications. While we understand the agency's conclusion that the radio transmission technology known as dedicated short-range communication (DSRC) is the only currently viable medium for V2V communications, we also recognize that there may be other viable options in the future. Therefore, it is important for NHTSA to maintain a pathway for vehicles to comply with the standard using non-DSRC technologies that meet certain performance and interoperability standards, as is currently outlined in section 9 of the proposed rule. The agency should not foreclose the use of another communications medium that meets necessary performance and interoperability requirements.

NHTSA also should remain open to the possibility that the spectrum allocation for intelligent transportation services may be excessive. As we recommended in an August 2016 statement filed with the Federal Communications Commission (FCC),¹² there should be

¹² "Consumer and Auto Safety Groups Call for Non-Commercial Use of the Auto-Safety Spectrum and Strong Privacy and Security Protections," Consumer Federation of America, Consumers Union, Advocates for Highway

dedicated and adequate spectrum available exclusively for safety purposes, but the current allocation of 75 MHz may be more than is necessary, and an impartial determination should be made as to what amount is needed solely for safety. We also called for the commercial use of this dedicated safety spectrum to be prohibited, including because it would be anti-competitive and run counter to public ownership principles and the efficiency and flexibility of the spectrum.

Additionally, as it seeks interoperability, we urge NHTSA to maintain all appropriate flexibility in the standard for the FCC to make future decisions that align with the public interest. For example, NHTSA's proposed rule specifies that all transmissions of basic safety messages should occur on wireless channel 172, via a dedicated radio at a data rate of 6 Mbps. We suggest that instead of referring specifically to channel 172, it may be more appropriate and may better promote spectrum flexibility for NHTSA to refer in the standard to the FCC's rule at 47 C.F.R. § 90.377, footnote 2, or more generally to "the appropriate channel designated by the Federal Communications Commission for public safety applications involving safety of life and property." Similarly, while we understand the technical rationale for specifying the data rate of basic safety messages, we suggest that NHTSA should take care that a final rule does not foreclose the emergence of technologies using other data rates as long as they are interoperable.

Privacy, Security, and Other Serious Challenges to Deployment Should Be Fully Addressed

As NHTSA moves forward with the proposed standard, we strongly urge the agency to fully address the serious challenges to V2V deployment that exist, so that the safety potential of the technology might be realized. The agency should start with consumer privacy and data security matters. Consumers deserve to know what their car is transmitting, and who has access to this information.

It is our view that the most appropriate and straightforward way to address consumers' concerns about the privacy and security of their data is to require vehicle and equipment manufacturers to meet baseline, enforceable standards. Consumers should be able to trust that companies are legally obligated to protect the privacy and security of V2V communications as they deploy them. At a minimum, manufacturers must adhere to the Fair Information Practice Principles (FIPPs), which NHTSA expects but does not require manufacturers to follow. We urge NHTSA to work with Congress and other federal agencies to ensure consumers have transparency, meaningful choice, control, and security for the personal data of theirs that is associated with a motor vehicle. We strongly prefer this approach over alternative approaches that would rely primarily on opt-out provisions that could undermine important safety technology.

With regard to the proposals in NHTSA's notice of proposed rulemaking, we strongly agree with the agency on the central role of privacy and security in public acceptance of V2V communications technology. In addition to the cybersecurity measures addressed previously in these comments, we appreciate that the agency recognizes that transmission of the Vehicle Identification Number and other information that directly identifies a specific vehicle or its

and Auto Safety, and Center for Auto Safety (Aug. 24, 2016) (online at consumersunion.org/news/consumer-and-auto-safety-groups-call-for-non-commercial-use-of-the-auto-safety-spectrum-and-strong-privacy-and-security-protections).

driver or owner could create significant privacy risks for private consumers, and that therefore the agency proposes excluding such explicitly identifying data in basic safety messages. We also appreciate that NHTSA has proposed a more general exclusion of “reasonably linkable” data elements from basic safety messages to further minimize consumer privacy risks. We support these approaches, and urge NHTSA to maintain them as the agency moves forward with the rulemaking.

Another potential source of deployment challenges for V2V communications involves aftermarket products, which could present a wide variety of different types of technologies and installation procedures once the marketplace develops. In a manner similar to other aftermarket products, we suggest that manufacturers of aftermarket V2V devices self-certify that they meet the performance and interoperability requirements in the standard—in this case, the same requirements that new car manufacturers would have to meet. NHTSA could audit compliance as it does for child seats. We suggest that a program of voluntary certification for installers could help drive proper installation, and help minimize the risk raised by the agency of “an improperly installed aftermarket device [putting] all other V2V-equipped vehicles it encounters at risk,” a scenario that we think should not be possible with adequate on-device technology to determine whether another vehicle’s device, or the original device itself, is properly installed.

In addition, to address any challenges related to driver behavior, it is important that V2V technology be carefully integrated into the driving experience, so that potential for driver distraction, annoyance, or inattention is minimized. The technology should effectively communicate warnings so the driver understands precisely why the vehicle’s safety system is reacting to a perceived risk and can take timely action if necessary to avoid a crash. We encourage NHTSA to continue its research to determine the most effective and least distracting ways for V2V devices to communicate this information to a driver. More broadly, we urge the agency to undertake significant additional research into human-machine interface—and continue seeking any funding from Congress necessary to do so—as well as to seek useful human-machine interface data from companies that may possess it.

Of course, the best way to get public acceptance for any new safety feature is to be able to show real-world results demonstrating the safety benefits. Consumer Reports’ survey results already show that consumers rank safety in the top three overall—along with cost and reliability—among the factors most important to them when buying a new car. NHTSA’s survey results also suggest a fairly high acceptance by consumers of the safety benefits from V2V communications. As a follow-up—and to assess the views of consumers at the outset of V2V implementation—we suggest an additional round of focus groups and survey research within the first year of implementation to gauge consumer acceptance in terms of each of its major components, including understanding of the technology, its performance, and their views related to privacy and security. We recommend that this type of assessment be included as an official part of the final rule.

To the extent possible, we also urge NHTSA to make provisions in any final rule for annual manufacturer reporting of real-world safety benefits. The data reported to the agency could be aggregated and used to create formal assessments of V2V’s safety benefits. We recommend that NHTSA specify in its final rule a description of the contents and timing of the

assessments and any other information that might be necessary to adequately evaluate the real-world performance of V2V-equipped vehicles. We also suggest that the agency partner with independent third-party organizations for evaluations of the reported data.

Implementation Should Occur Faster Than Planned If Outstanding Issues Are Resolved

NHTSA has proposed an implementation time frame for V2V capability that includes a minimum of two years of lead time after the issuance of a final rule, followed by a three year phase-in period before 100% of new cars must be equipped with V2V communications devices. We recommend a more expeditious implementation process, and one that incorporates effective V2V-based safety applications into the rule as soon as possible.

Given the safety potential of V2V technologies, we urge NHTSA to set a lead time of no longer than 18 months, which the market study commissioned by NHTSA and undertaken by the Intelligent Transportation Society of America indicated may be an adequate amount of time for the mass production of V2V devices. At that point, the appropriately aggressive phase-in plan would begin.

We note that the proposed rule does not include performance standards for any V2V safety applications, though NHTSA indicates that Intersection Movement Assist and Left Turn Assist are priority applications because they have a demonstrated effectiveness, would address crashes that are disproportionately severe, and cannot currently be deployed using camera- or sensor-based technologies. We agree that it is appropriate for these V2V applications to be prioritized. However, we also think that if a V2V-based safety application is effective—if NHTSA reasonably determines it would protect the public against unreasonable risk of death or injury in a crash—the agency should set performance standards and test methods for it as early as possible. If the agency possesses the necessary data showing the benefit to safety, there is no reason to wait until an arbitrary time after a V2V final rule is issued before protecting the public through these applications.

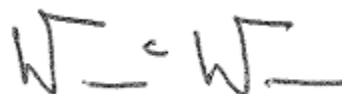
Conclusion

Thank you for your consideration of our comments. We look forward to continuing to work with NHTSA and all stakeholders to bring about safer roads for consumers, including through the finalization and deployment of new safety features based on V2V communications.

Respectfully submitted,



Jennifer Stockburger
Director of Operations
Consumer Reports
Auto Test Center



William C. Wallace
Policy Analyst
Consumers Union
Washington, D.C.