REVIEW OF NHTSA PROPOSAL TO MANDATE V2V COMMUNICATION FOR SAFETY

December 20, 2016

Center for Automotive Research (CAR)
3005 Boardwalk, Suite 200
Ann Arbor, MI 48108

Review of NHTSA Proposal to Mandate V2V Communication for Safety
December 20, 2016

Author:
Eric Paul Dennis, CAR

Managing Editor:
Richard Wallace, M.S., Director, Transportation Systems Analysis, CAR

Abstract:
In December of 2016, the National Highway Traffic Safety Administration (NHTSA) of the U.S. Department of Transportation released a Notice of Proposed Rulemaking (NPRM) regarding an addition to the Federal Motor Vehicle Safety Standards (FMVSS) that would require new light vehicles to include direct short-range communication (DSRC) technology for vehicle-to-vehicle (V2V) safety applications. This report summarizes the central elements of the NPRM and highlights refinements that still need to be addressed prior to a final rulemaking. This document developed by the Center for Automotive Research (CAR) provides its affiliates, partners, the automotive industry, and the general public with a greater understanding of this potentially transformative regulation.

TABLE OF CONTENTS

1 Introduction 1
1.1 Summary of the Proposed Rule 2
2 Technology Requirements 3
2.1 Industry Standards 3
2.2 One Radio or Two? 3
2.3 Alternative Technologies 4
2.4 The Basic Safety Message 4
2.5 BSM Transmission Requirements 8
2.6 Hardware (Physical) Security 9
2.7 Aftermarket Devices 9
2.8 Congestion Mitigation 10
2.9 Over-the-Air Update Capability 10
3 Security Credential Management System 12
3.1 Public Key Infrastructure 13
3.2 Privacy Protections 13
3.3 Consumer Consent 14
3.4 Misbehavior Reporting 15
4 Request for Comments 16
5 Conclusions 19

1 INTRODUCTION

On December 13, 2016, the National Highway Traffic Safety Administration (NHTSA) of the USDOT released a Notice of Proposed Rulemaking (NPRM) focused on establishing a new Federal Motor Vehicle Safety Standard (FMVSS) to mandate vehicle-to-vehicle (V2V) communications for new light vehicles.[1, 2] After more than a decade of testing and refinement of the technologies and applications that lie at the core of V2V, NHTSA published an Advanced Notice of Proposed Rulemaking (ANPRM) in 2014. The public comments submitted in response to the ANPRM were considered and used to produce the NPRM document.

The U.S. DOT and its industry partners have been researching and developing connected vehicle technology for intelligent transportation systems (ITS) applications since the early 1990s. In 1999, the Federal Communications Commission (FCC) allocated 75 MHz of radio frequency spectrum—from 5.850 to 5.925 GHz—for use by Dedicated Short Range Communications (DSRC) to operate ITS services. In 2003, the FCC adopted service and technical rules for DSRC in this band. The FCC's actions were in response to a petition for rulemaking by ITS America and generally intended to support the USDOT's efforts to use the 5.9 GHz spectrum to deploy a nationwide connected vehicle (V2X) infrastructure.

The Transportation Systems Analysis (TSA) group at the Center for Automotive Research (CAR) in Ann Arbor has reviewed the NPRM document provided by NHTSA. CAR has produced this report to provide its Affiliates and partners, as well as the broader public, with greater understanding of this potentially transformative regulation.

[1] Herein: "NPRM."

[2] Referenced NPRM document refers to "unofficial" version posted Dec. 13, 2016 at: https://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_v2v_proposed_rule_12132016. As of December 20, publication of the official NPRM in the Federal Register remains forthcoming, as is the accompanying Preliminary Regulatory Impact Assessment (PRIA) and draft Privacy Impact Assessment (PIA).

1.1 SUMMARY OF THE PROPOSED RULE

NHTSA proposes a new Federal Motor Vehicle Safety Standard (FMVSS) (No. 150) to require that all new light vehicles (passenger cars, multipurpose passenger vehicles, trucks, and buses) with a gross vehicle weight (GVW) rating of 10,000 pounds or fewer must be capable of transmitting and receiving a basic safety message (BSM) using DSRC. Notably, this NPRM does not include proposed regulatory text that could be adopted as is. The necessary elements of a potential V2V mandate that are identified, but they are not all specified. Adoption of a final rule within FMVSS will require additional refinement.

BASIC SAFETY MESSAGE

DSRC-equipped vehicles would transmit and receive standardized basic safety messages (BSMs) at a rate of ten times per second, as well as include specified performance criteria for data transmitted. The BSM includes the vehicle location, speed, and heading, as well as other related data.

SAFETY APPLICATIONS

NHTSA is *not* proposing to mandate or otherwise regulate any specific V2V-enabled safety application. The agency assumes that automakers will voluntarily develop and deploy DSRC-based safety applications after DSRC communications technology is mandated.

NETWORK ADMINISTRATION AND SECURITY

NHTSA has not yet proposed a governance structure for the DSRC network or required security implementation, though considerations and alternatives are discussed at length in the NPRM. Placeholder sections are provided in the proposed regulatory language. Such details will be determined prior to adoption of a final rule.

PHASE –IN SCHEDULE

NHTSA presumes that the final rule will be adopted in 2019. A phase-in schedule will begin in 2021 with 50 percent of new light vehicles meeting the standard. In 2022, the requirement will increase to 75 percent. The phase-in is expected to be complete in 2023 with 100 percent of all new light vehicles required to comply that year and going forward.

2 TECHNOLOGY REQUIREMENTS

The proposed regulatory text would mandate that new light vehicles include interoperable V2V communication technology via DSRC-capable on-board equipment (OBE).[3] The DSRC device must transmit a basic safety message (BSM) on Channel 172 in the 5.9 GHz spectrum band as allocated by the FCC in 47 C.F.R. part 90 subpart M. Any additional, non-safety-critical communications must be transmitted in other channels within the 5.9 GHz DSRC band.[4]

2.1 INDUSTRY STANDARDS

The proposed regulatory text does not explicitly reference or require any industry standard; however, the proposed performance tests imply that full or partial adherence to several industry standards will be required to comply with the rule. These standards include:[5]

- IEEE 802.11p: Physical DSRC Network and Addressing Scheme
- IEEE 1609.0: Guide for Wireless Access in Vehicular Environments (WAVE) Architecture
- IEEE P1609.4: Multi-channel Operations
- IEEE P1609.3: Networking Services
- IEEE P1609.2: Security Services for Application and Management Messages
- IEEE 1609.12: Identifier Allocations
- SAE J2945: DSRC Minimum Performance Requirements
- SAE J2735: DSRC Message Set Dictionary

2.2 ONE RADIO OR TWO?

Once adopted, the final rule might well require two DSRC radios and antennas as described in IEEE 1609.4. One radio would be fixed to channel 172 for transmission and reception of the BSM. The other would use multi-

[3] NPRM pp. 368-387.
[4] NPRM pp. 373-374.
[5] NPRM pp. 93-98.

channel operations to set the CCH (control channel) and SCH (security channel), receive software updates, and renew security certification.[6]

2.3 ALTERNATIVE TECHNOLOGIES

NHTSA recognizes that someday other technologies might outperform DSRC as a medium for safety-related communications. Additionally, Executive Order 12866 directs agencies to use technology agnostic, performance-based standards whenever possible. The proposed regulatory text permits alternative V2V technologies to be used to comply with the mandate.[7] Any alternative technology, however, would have to be interoperable with DSRC (e.g., sending and receiving BSMs on Channel 172 of the DSRC spectrum).[8] This provision appears to imply that any addition technologies used to transmit a BSM or other safety-related communications would have to be *in addition to*, rather than an *alternative to*, DSRC technology—at least as related to exchange of the BSM.[9]

2.4 THE BASIC SAFETY MESSAGE

The exchange of the BSM over DSRC is the main focus of the proposed mandate. NHTSA believes that the mandate of V2V exchange of the BSM will allow and encourage manufacturers to develop and deploy crash-avoidance technologies and other applications to benefit safety, mobility, and efficiency of vehicle travel.

The proposed regulatory language includes a minimum data set required to be submitted with each BSM. NHTSA's proposed BSM references industry standard, SAE J2735. Required functional elements[10] of the BSM include:[11]

- **Time:** BSMs need to include a timestamp expressed in Coordinated Universal Time (UTC) per SAE J2735. [12] Additionally, NHTSA is

---

[6] NPRM pp. 98-99, 278.
[7] NPRM pp. 93, 95, 102-105, 253-259, 388-389.
[8] Ibid.
[9] The most likely alternative technology is "5G" cellular/wireless communication. NHTSA did not directly acknowledge 5G, but this was frequently referenced in public comments submitted in response the 2014 ANPRM. At this time, 5G remains in development as a conceptual technology without a clear set of technology or performance standards.
[10] By functional elements, we mean those elements intended to support safety applications rather than assure interoperability.
[11] NPRM pp. 109-122.
[12] NPRM pp. 108-109,

proposing that the BSM will be broadcast ten times each second. The mean time between BSM broadcasts will be 100 ms (0.100 s), but NHTSA proposes that the BSM broadcast be randomly varied by +/- 5 ms to help avoid vehicles broadcasting at the same time.[13] The time stamp must be accurate within 1 ms.[14]

- **Location:** Vehicle location must be reported as the point of the center of the vehicle in longitude and latitude with reference to WGS-84.[15] Compliant vehicles must report location accuracy within 1.5 m (4.9 ft) when tested in controlled conditions.[16]
- **Elevation:** Compliant vehicles must report elevation location accurately within 3 m (~ 10 ft) when tested in controlled conditions.[17]
- **Speed:** Reported in increments of 0.02 mph, with a tolerance of 1 Kph (0.62 mph).[18]
- **Heading:** Reported as the motion of the vehicle center (regardless of which direction the vehicle is pointed). When the vehicle speed is greater than 12.5 m/s (~ 28 mph), heading must be accurate within 2 degrees. When the vehicle speed is less than 12.5 m/s, heading must be accurate within 3 degrees, unless the vehicle speed is very low (less than 1.11 m/s), in which case heading need not be reported.[19]
- **Acceleration:** Horizontal (longitude/latitude) acceleration must be reported accurately within 0.3 m/s^2. Vertical acceleration must be reported accurately within 1 m/s^2.[20]
- **Yaw Rate:** When combined with the angle of the front tires, the yaw rate of a vehicle describes the extent to which a vehicle might be "spinning," implying that the tires have lost traction.[21] NHTSA proposes that the BSM report the yaw rate accurate to 0.5 degrees per second.[22]

---

[13] Ibid.
[14] NPRM 108-109, 370.
[15] NPRM p. 111.
[16] NPRM pp. 111, 383-384.
[17] Ibid.
[18] NPRM 112-113.
[19] NPRM pp. 113-114, 371.
[20] NPRM pp. 114-115.
[21] U.S. DOT NHTSA FMVSS No. 126 Electronic Stability Control Systems.
[22] NPRM p. 115.

- **Path History:** NHTSA proposes requiring a data frame describing the path history of the vehicle's location and speed for the previous 300 m (about 1,000 ft or 0.19 miles) of travel.[23]
- **Path Prediction:** Considering that anticipation of vehicle path might be required for potential safety applications, NHTSA proposes requiring a path prediction data element, represented, "at a first order of curvature approximation, as a circle with radius, R, and an origin located at (0,R), where the x-axis is aligned to the vehicle's perspective and normal to the vehicle's vertical access."[24]
- **Exterior Lights:** NHTSA proposes that any available data regarding a vehicle's exterior lights be included in the BSM. This includes headlights (high-beam, low-beam, automatic light control), parking lights, fog lights, turn signals, and hazard lights.[25]
- **Event Flags:** NHTSA proposes adopting an "event flag" data set as described in SAE J2735. Specific event flag requirements are: ABS (Anti-lock Brake System) Activation, ESC (Electronic Stability Control) Activation, Hard Braking (more than 0.4 g.), Air Bag Deployment, Hazard Lights, Stop-line Violation, Traction Control System Activation, Flat Tire, Disabled Vehicle, Headlight Status Change, Wiper Status Change, Emergency Response Vehicle, and Hazardous Materials.[26]
- **Transmission State:** NHTSA proposes to require basic transmission state data (i.e., neutral, reverse, forward) in the BSM.[27]
- **Steering Wheel Angle:** As proposed, the steering wheel angle must be reported accurately within 5 degrees.[28]
- **Vehicle Size:** As proposed, vehicle length and width must be reported within 0.2 m (~ 8 in).[29]

[23] NPRM pp. 116-117, 371.
[24] NPRM pp. 117-118, 372.
[25] NPRM pp. 119, 372.
[26] NPRM pp. 119-120, 373.
[27] NPRM pp. 120, 373.
[28] NPRM pp. 121, 373.
[29] NPRM pp. 121-122, 373.

OPTIONAL DATA ELEMENTS

NHTSA proposes allowing manufacturers the option of including the following additional data elements in the BSM:

- Brake Applied Status
- Traction Control State
- Stability Control Status
- Auxiliary Brake Status
- Antilock Brake Status
- Brake Boost Applied
- Location Accuracy

If a manufacturer chooses to include optional elements in the BSM, the data should be provided as described in SAE J2735. The fields will be specified "unavailable" if the vehicle does not report optional data.

PROHIBITED DATA ELEMENTS

NHTSA proposes to prohibit the BSM from including "any data linked or reasonably linkable to a specific private vehicle, or its driver or owner, including but not limited to VIN, VIN string, vehicle license plate, vehicle registration information, or owner code."[30] NHTSA defines *reasonably linkable* to mean "capable of being used to identify a specific individual on a persistent basis without unreasonable cost or effort, in real time or retrospectively."[31]

The NPRM provides confirmation at several points that NHTSA does not consider location information (linked to a temporary key) to be reasonably linkable data.[32] Presumably, the forthcoming draft Privacy Impact Assessment (PIA) will discuss this conclusion in detail.

MESSAGE PACKAGING

The BSM vehicle data must be "packaged" with specific data elements that allow a receiving device to understand and decode the BSM. As per SAE J2735, each BSM will include a *message ID* ("2"), *message count* (repeating

[30] NPRM pp. 122-123, 373.
[31] NPRM pp. 123, 369.
[32] E.g., NPRM p. 41.

sequence from "0" to "127"), and *temporary ID* (4-byte randomly-generated string array).[33]

The proposed regulatory language alternatively defines the *temporary ID* as a "randomly generated 4-*digit* number."[34] This appears to be a mistake and most likely will be revised to require a four-*byte* string as defined in SAE J2735 and discussed in the NPRM, pp. 107-108.

2.5 BSM TRANSMISSION REQUIREMENTS

In the BSM context, *transmission requirements* generally refer to the physical attributes of the electromagnetic waves carrying the BSM signal. As already discussed, the BSM must be transmitted ten times per second on Channel 172 of the 5.9 GHz DSRC spectrum.[35] Additional performance-based requirements are proposed as follows:

RANGE

NHTSA proposes a minimum transmission range of 300 m (984 ft) in a radial plane at the same elevation as the device and within a vertical displacement of at least ten degrees above the vehicle and six degrees below the vehicle.[36] Packet error rate (PER) must not exceed 10 percent within this range.[37]

Compliance to range requirements is determined by a controlled test. Test procedures need not account for variable performance in complex, real-world environments.[38] Because compliant vehicles will need to meet performance objectives, NHTSA does not propose to address underlying factors such as antenna location, antenna polarization, or transmission power.[39] NHTSA does, however, intend to specify a data rate of 6 Mbps.[40]

DATA EXPIRATION

In the preamble to the NPRM document, NHTSA proposes that no data older than 150 ms (0.15 s) should be included in the BSM.[41] NHTSA

[33] NPRM pp. 107-108.
[34] NPRM p. 370, emphasis added.
[35] NPRM pp 81-82, 373-374.
[36] NPRM pp. 74-78, 373, 382-383.
[37] Ibid.
[38] NPRM 381-384.
[39] NPRM pp. 79-80.
[40] NPRM pp. 84-89, 374.
[41] NPRM p. 90.

acknowledges, however, that because some elements of the BSM do not include a timestamp, "it is not clear how this is done in practice."[42] The proposed regulatory text does not include a data expiration provision or test procedure.

INITIALIZATION TIME

NHTSA proposes that vehicles must begin transmitting the BSM "within 2 seconds after V2V device power is initiated."[43] By contrast, the preamble of the NPRM discusses initialization times "within 2 seconds after a vehicle key on event," as well as "within 2 seconds after the driver puts the vehicle into forward or reverse gear."[44] This discrepancy appears to be an unintentional result of evolving discussions. It is not clear which initialization event NHTSA intends for a final rule.

2.6 HARDWARE (PHYSICAL) SECURITY

NHTSA mentions in the preamble that the V2V equipment should be "hardened" against intrusion as per Federal Information Processing Standards (FIPS)-140 Level 3.[45] Nonetheless, the proposed regulatory text does not include such a provision.[46] Also, FIPS 140-3 has not yet been published (as of December 20, 2016).[47]

2.7 AFTERMARKET DEVICES

NHTSA acknowledges that certain data elements require access to other vehicle networks (e.g., transmission state, light status, steering wheel angle). In the preamble, NHTSA discusses the potential for aftermarket devices that omit these data.[48] The NPRM document does not resolve the issue of whether or not NHTSA intends to regulate aftermarket V2V devices.

[42] Ibid.
[43] NPRM p. 373.
[44] NPRM pp. 124-125.
[45] NPRM p. 15, 154-158.
[46] The preamble does include *potential* regulatory text, p. 157.
[47] https://www.nist.gov/itl/current-fips, accessed Dec 20, 2016.
[48] NPRM pp. 68-70.

2.8 CONGESTION MITIGATION

A digital network, whether wireline or wireless, has physical limitations on the amount of data that can be simultaneously transmitted. For V2V communications, if enough V2V-equipped vehicles were within communication range, the volume of BSM transmissions possibly could overload the network, reducing the fidelity of data received and negatively affecting the ability of V2V-based applications to function. Considering this, NHTSA proposes that DSRC units be capable of detecting high-traffic environments and respond appropriately to avoid network congestion.[49]

NHTSA and partners continue to refine congestion mitigation approaches.[50] Generally, any approach to congestion mitigation requires a vehicle to determine the local density of transmitting vehicles.[51] NHTSA *does* include a relatively detailed procedure for congestion mitigation in the proposed regulatory text.[52] When a congested message environment is detected, NHTSA proposes reducing transmission power (range).[53] Other options include increasing the transmission bitrate[54] and transmitting certain elements of the BSM at reduced frequency.[55]

2.9 OVER-THE-AIR UPDATE CAPABILITY

NHTSA has determined that a functional V2V network will require "periodic updates to address functionality, potential security, or potential privacy issues as the arise." Consequentially, NHTSA intends to propose over-the-air (OTA) update capability. [56] OTA provisions are not included in the proposed regulatory text, but multiple placeholders have been set-aside for OTA updates and communication with a Security Credential Management System (SCMS).

[49] NPRM pp. 374-379.
[50] NPRM pp. 85, 255.
[51] NPRM p. 91.
[52] NPRM pp. 374-379, 384-385.
[53] NPRM p. 379.
[54] NPRM p. 85.
[55] NPRM p. 135.
[56] NPRM p. 151

NETWORK LINK TO THE SCMS

NHTSA has not yet determined how vehicles would communicate with the SCMS authority. The NPRM discusses an approach by which a second DSRC radio would be included for non-BSM communications, as well as an alternative approach whereby some combination of cellular, Wi-Fi, and satellite communication would be used for non-BSM messages.[57] The proposed regulatory text suggests that all communications would utilize DSRC.[58]

[57] NPRM pp. 287-288.
[58] NPRM pp. 373-374.

3 SECURITY CREDENTIAL MANAGEMENT SYSTEM

For effective V2V-facilitated safety applications, V2V devices must be confident that the data received via BSMs are legitimate and accurate. Theoretically, connected vehicles could form ad-hoc wireless networks without any central network administration component; however, "as designed, V2V technology cannot operate without a sufficient security system."[59]

NHTSA elaborates:

> Even in a warning system, it is important for safety applications to have accurate information available to make their decisions. Incorrect warnings can (at worst) directly increase safety risks and (at minimum) affect the driver's acceptance of the warning system. If the driver of a V2V-equipped vehicle receives a large number of warnings when there is no crash imminent (i.e., false warnings), then the driver may lose confidence and not respond appropriately when there is a true crash–imminent situation.[60]

DSRC achieves message authentication through a public key infrastructure (PKI). In the NPRM document, NHTSA also introduces two alternative approaches, including *performance-based authentication* and *no requirement for message authentication*.[61] Where relevant, the NPRM generally assumes that connected vehicles will be required to communicate with an SCMS for multiple functions relating to message authentication, as well as privacy and security. This approach seems reasonable, because the majority of stakeholders believe it is necessary that a national V2V network use PKI authentication coordinated through an SCMS or similar administrative structure.[62]

The proposed regulatory text does not include any specific provision for communication between DSRC devices and an SCMS, but it does contain several placeholder sections for such requirements. Additionally, the preamble of the NPRM discusses the role of an SCMS at considerable length, including "potential regulatory text."[63]

---

[59] NPRM pp. 268-269.
[60] NPRM pp. 128-129.
[61] NPRM pp. 14-15, 140-144.
[62] NPRM p. 231.
[63] NPRM pp. 237-241.

3.1 PUBLIC KEY INFRASTRUCTURE

Within a PKI authentication framework, each BSM would be digitally signed with a security certificate. The requirement to obscure the link between BSMs and individual drivers requires a PKI system that uses both a public and private key.[64] An SCMS organization would certify legitimate DSRC devices and relay information regarding the legitimacy of public keys between equipped vehicles so that each device can confirm BSMs as signed by a certified and approved sender.[65]

NHTSA is considering requiring only a fraction of BSMs to include the full public key. Evidence exists that full certification of every fifth BSM is sufficient to ensure the validity of messages.[66] Each BSM would include a temporary ID to allow the receiving vehicles to establish continuity between sending vehicles.[67]

3.2 PRIVACY PROTECTIONS

Location data (as included in the BSM) is one of the most sensitive types of personally identifiable information (PII).[68] As pointed out in the NPRM, "the introduction of V2V technology creates new privacy risks that cannot be fully mitigated."[69]

NHTSA and DSRC developers are fully aware of the privacy issue and have subsequently designed an SCMS and PKI such that individual vehicles, drivers, and owners are not directly linked to BSMs. NHTSA and DSRC industry stakeholders have invested extensive effort into designing a network that is appropriately situated on the "spectrum between the competing interests of maximizing privacy protections and technological practicability."[70]

Reflecting the compromise between privacy and practicality, NHTSA suggests that a final V2V mandate would require that V2V-equipped vehicles receive a weekly set of 20 public key pseudonym certificates.[71] These 20

---

[64] NPRM pp. 129-131.
[65] Ibid.
[66] NPRM p. 135.
[67] NPRM pp. 107-108, 370.
[68] Dennis, Cregger, and Hong. *ITS Data Ethics in the Public Sector*. CAR and MDOT. June 2016.
[69] NPRM p. 183. Also discussed p. 188.
[70] NPRM p. 137.
[71] NPRM pp. 135-139

certificates validate BSMs for five-minute intervals on a rotating basis for a seven-day period.

To track an individual vehicle with confidence, an adversary would need to know each of the 20 pseudonym certificates. Discovering all 20 certificates would require monitoring the vehicle's BSMs for a sequential 100-minute period. Even then, tracking that vehicle would only be possible for seven days. At the end of the week, the vehicle would receive a refreshed set of 20 public certificates from the SCMS.[72] NHTSA has tentatively concluded that such "residual risk" is acceptable.[73]

3.3 CONSUMER CONSENT

NHTSA has determined that its authority is sufficient to mandate the installation of V2V devices in new light vehicles; however, NHTSA is not claiming authority to regulate an ongoing "relationship between the vehicle manufacturers and their customers."[74] In fact, NHTSA has determined that "V2V device users will need to consent to both software and security certificate updates."[75] This creates a complication given the assumption that an effective V2V network will require vehicles to communicate with an SCMS manager and/or manufacturers for refreshment of pseudonym certificates and other software updates. At this time, "NHTSA is not requiring that certificate and software updates be pushed to vehicles without consumers' consent."[76]

NHTSA proposes that BSMs must be validated through the PKI, including the temporary pseudonym certificates, with a one-week expiration date. To preserve privacy, NHTSA proposes that the DSRC device must "completely discard used certificates at the end of a one-week period.[77] This implies that, if a consumer refuses a necessary update, "V2V will not work."[78]

This confluence of necessity and uncertainty of authority imposes a complication for a potential FMVSS. NHTSA is open to allowing drivers to disable safety applications, but it does not intend to allow drivers to

[72] Ibid.
[73] NPRM pp. 176-177.
[74] NPRM p. 250.
[75] NPRM p. 151.
[76] Ibid.
[77] NPRM pp. 139-140.
[78] Ibid.

temporarily disable V2V communications.[79] Yet, drivers apparently could disable V2V communications by declining to approve software updates and weekly certificate renewals.

3.4 MISBEHAVIOR REPORTING

NHTSA envisions that a sub-component of an SCMS would be a misbehavior authority to collect and redistribute a list of devices that have been identified as "untrusted."[80] DSRC units must be capable both of internal self-diagnosis and detection of aberrant behavior from received BSMs.[81]

[79] NPRM pp. 172-175.
[80] NPRM pp. 141-142.
[81] NPRM pp. 141-150, 379-381.

4 REQUEST FOR COMMENTS

Public comments will be accepted on the NPRM for a 90-day period following forthcoming publication of it in the Federal Register. NHTSA has specifically asked for comments on the following topics:[82]

- Potential for data fusion of V2V and vehicle-resident technologies (p. 33)
- If an "if-equipped" V2V FMVSS would be preferable to a mandate (pp. 33, 68)
- The relationship between V2V and automated driving technologies (p. 35)
- Potential for market forces to achieve V2V benefits without a mandate (p. 67)
- Potential certification requirements for aftermarket V2V device installation (p. 70)
- Development, efficacy, and validation of Intersection Movement Assist (IMA), Left Turn Assist (LTA), and other V2V safety applications (pp. 71, 267, 315)
- Alternative interoperable technologies (p. 71)
- Appropriateness of performance-based BSM transmission requirements (pp. 73, 74, 79, 80)
- Potential need for upper limit on transmission range of BSM (p. 75)
- Appropriateness of minimum transmission range and elevation requirements (pp. 75, 82)
- How to test transmission performance (p. 78)
- If packet error rate (PER) maximum threshold of 10 percent is appropriate (pp. 78, 82)
- Choice of Channel 172 for BSM (pp. 81, 82)
- Appropriateness of 6 Mbps data transmission rate (pp. 81, 82, 85, 86)
- Costs and benefits of spectrum sharing with unlicensed devices (p. 84)
- Other needed BSM performance parameters (pp. 90, 134)
- Omission of certain BSM reception performance requirements (p. 92)
- Overlooked requirements for interoperability (pp. 93, 105, 140, 259)
- Appropriateness of speed data provision in BSM (p. 113)

[82] Each listed topic includes a citation to the page of the NPRM where NHTSA has requested comment.

- Appropriateness of chosen event flags in BSM (p. 120)
- Options for defining vehicle size in BSM (p. 122)
- Privacy implications of V2V (pp. 123, 176, 178, 188, 191)
- When a vehicle should begin transmitting a BSM (p. 126)
- Alternatives to Public Key Infrastructure (p. 129)
- How to test for compliant message authentication capability (p. 134)
- Frequency of transmission of pseudonym certificate and/or certificate digest (p. 135)
- Appropriateness of proposed scheme of pseudonym certificate rotation (p. 137)
- How to test to determine that a DSRC device will not send BSMs without a valid security certificate, and if that needs to be tested for certification (p. 138)
- How to specify and test for misbehavior detection (pp. 142, 143, 144, 149)
- How to specify and test for malfunction detection and indication (p. 150)
- How to encourage users to consent to software and security updates (pp. 152, 251)
- How to include hardware security requirements in an FMVSS (p. 156)
- How to handle DSRC device end-of-life security (p. 157)
- General cybersecurity implications of V2V and the SCMS (pp. 158, 159, 210)
- Should GNSS (GPS) jamming be considered, and if so, how? (p. 159)
- Whether or not a compromised (hacked) V2V device should be considered a safety-critical issue (p. 161)
- If it is desirable and necessary to require over-the-air (OTA) update capability (p. 162)
- Should owners be given the option to decline critical security updates? (p. 163)
- What can be done to improve public acceptance (pp. 166, 172)?
- How to communicate V2V privacy policies with consumers (pp. 167-168, 189)
- Should there be opt-in or opt-out provisions? (p. 168)
- How to prevent hacking and manage cybersecurity risks (pp. 169, 170)
- Costs and benefits of allowing users to deactivate V2V devices (p. 175)

- Would the privacy-related risks of V2V necessitate new legislation to protect consumer privacy? (p. 183)
- Governance structure of a security credentials management system (SCMS) (p. 241)
- Viability of a vehicle-based security system (VBSS) alternative to an SCMS (p. 243)
- If requiring devices to be pre-loaded with a lifetime of security certificates would be preferable to the proposed weekly update scheme (p. 251)
- If NHTSA should assert authority over roadside equipment to ensure that devices do not collect data that could affect consumer privacy (p. 252)
- If the proposed mandate is sufficiently "performance oriented" (pp. 256, 263)
- How to mandate safety applications (p. 266)
- Any information on the likely deployment timeline for V2V-enabled safety applications following a mandate (pp. 277, 315, 323)
- Cost assumptions in PRIA (pp. 289, 307, 310, 340, 355).
- SCMS costs and funding (pp. 295, 307)
- Opportunity-costs of RF spectrum usage for V2V (pp. 309, 310, 312, 313, 314)
- Phase-in schedule (pp. 357, 359)

5 CONCLUSIONS

NHTSA's V2V NPRM is the latest confirmation that the agency is committed to facilitating the nationwide deployment of a DSRC V2V safety network. For those familiar with the UDOT's Connected Vehicle Program and related efforts, the discussions included in the NPRM preamble likely will be familiar. The agency remains mostly consistent with the approaches discussed in the 2014 Advanced Noticed of Proposed Rulemaking (ANPRM) and supporting documents.

The agency intends to adopt a Federal Motor Vehicle Safety Standard that will mandate that all new light vehicles come equipped with standardized DSRC-based V2V communication. Currently, NHTSA does not plan to require and specific V2V-based safety applications, but it anticipates that manufacturers will voluntarily deploy such applications when they can be confident that a national V2V network will be expansive and supported appropriately.

The recent NPRM includes additional details that previously were not broadly publicized—most importantly the proposed specifications for the Basic Safety Message (BSM) and testing requirements; however, the NPRM currently includes placeholders for regulatory language that will likely need to be developed before a final rule can be adopted. Most critically, the agency has not proposed regulatory text describing the provision of network administration and security (i.e., the SCMS).

The public will be provided a 90-day comment period when the NPRM is officially published in the Federal Register.[83] The public is welcome to comment on any aspect of the NPRM and any other supporting documents. Additionally, NHTSA has specifically requested public comment on a variety of details listed above in section 4. Considering that regulatory text remains under development, stakeholder feedback via public comment and otherwise will be critical in the development of the final rule.

NHTSA anticipates adopting a final rule with publication of a new FMVSS in 2019. The preliminary phase-in schedule is projected to begin in 2021 at 50 percent of new light vehicles and step up to 100 percent compliance (all new light vehicles) by 2023.

[83] As of Dec. 20, 2016, publication in the Federal Register of the NPRM, as well as supporting Preliminary Regulatory Impact Assessment (PRIA), and draft Privacy Impact Assessment (PIA), remains forthcoming.