Barriers to Public Acceptance of Vehicle-to-Vehicle Communications

Course No: C03-050

Credit: 3 PDH

Mark Rossow, PhD, PE, Retired

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

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

Introduction to the Study Guide

The U.S. Department of Transportation's National Highway Traffic Safety Administration has issued a Notice of Proposed Rulemaking (NPRM) that proposes to establish a new Federal Motor Vehicle Safety Standard (FMVSS), No. 150, to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions. The new standard will create an information environment in which vehicle and device manufacturers can create and implement applications to improve safety, mobility, and the environment. Without a mandate to require and standardize V2V communications, the agency believes that manufacturers will not be able to move forward in an efficient way and that a critical mass of equipped vehicles would take many years to develop, if ever. Implementation of the new standard will enable vehicle manufacturers to develop V2V safety applications that are estimated to prevent hundreds of thousands of crashes and prevent over one thousand fatalities annually.

The Study Guide for the present course consists of Section IV, "**Public Acceptance, Privacy and Security**," of the NPRM. This section has been excerpted and begins near the middle of the next page.

The entire NPRM can be downloaded by clicking on this link, but the present course is based solely on the material in Section IV.

the regulatory text of this proposal, Section XI, proposes static, dynamic, and simulated performance tests. These tests have the potential for evaluating the performance of the V2V Radios and verifying the accuracy of the Basic Safety Message (BSM) safety message, Part I.

NOTE: The performance metrics mentioned in this document are placeholders to illustrate what aspect of performance we could evaluate at each step of the test. The performance metrics themselves will be updated pursuant to any decision to propose x or y as a requirement.

Overall, we anticipate devices under test will be instrumented with independent measurement sensors, devices, and a data acquisition system (DAS) in order to collect V2V system data. The independent measurement equipment will collect Differential Global Positioning System (DGPS) information, vehicle speed, vehicle 3-axis accelerations, vehicle yaw rate, vehicle systems status information, and radio performance data.

IV. Public Acceptance, Privacy and Security

A. Importance of public acceptance to establishing the V2V system

In the Readiness Report, NHTSA extensively discussed the importance of consumer acceptance to the success of V2V, given that as a cooperative system that benefits from network effects, V2V depends on drivers' willingness to participate. V2V needs vehicles to be equipped in order to broadcast messages that other vehicles can "hear," but in order for equipped vehicles to join the roads, consumers must be willing to recognize the benefits of a V2V system and support its adoption by the U.S. vehicle fleet via the purchase of the new, equipped vehicles, or by adding V2V capability to their existing vehicles through aftermarket devices. Thus, consumers must *want* V2V in order for V2V to reach its full potential. If consumers avoid the technology for some reason, it will take longer to achieve the network effect, and safety benefits will be slower to accrue.

Additionally, the courts have determined that public acceptance of a mandated technology is necessary to ensure that the mandate fulfills the requirements of the Safety Act. As discussed further in Section V.C below, if the public rejects a technology that the agency has required for new vehicles, the courts have found that the standard may neither be practicable nor meet the need for safety in the absence of public acceptance. If vehicle manufacturers literally cannot sell V2V-equipped vehicles because consumers *en masse* refuse to buy them, then it is possible that a court would conclude that the standard was not consistent with the Safety Act.

NHTSA must therefore consider the potential elements of a V2V requirement that may affect public acceptance, and do what we can to address them, both through carefully considering how we develop the mandate, and through consumer education to improve understanding of what the technology does and does not do. Additionally, we expect, simultaneously, that vehicle manufacturers subject to the eventual mandate will likewise work to improve public understanding of the benefits of V2V, boosting consumer acceptance overall. We also seek

comment on the extent to which an if-equipped approach potentially may alleviate some consumer acceptance concerns.

B. Elements that can affect public acceptance in the V2V context

Based on our review of the research conducted so far and the responses to the ANPRM and Readiness Report, NHTSA believes that the several elements of the V2V system discussed below may affect public acceptance.

1. False positives

A "false positive" occurs when a warning is issued to a driver and the warning is unnecessary (or when the driver believes the warning is unnecessary), because there is no immediate safety risk that the driver has not already accounted for. False positives can startle and, if there are too many, annoy a driver, causing drivers to possibly lose confidence in the system's ability to warn them properly of danger and desire to have the warning disabled; reducing overall system benefits. If the driver does not notice immediately that a false positive is in fact false, the driver might carry out an unnecessary evasive maneuver, potentially increasing the risk of an accident.

In the SPMD, we initially saw fairly high numbers of false positive warnings for some V2V applications.[174] Further analysis indicated this was due largely to the fact that the safety applications under evaluation were still prototypes. Part of the goal of the SPMD was to provide vehicle manufacturers with the opportunity to gain real-world experience with V2V safety applications; providing the opportunity to improve their "tuning" to maximize safety while minimizing false positives. Driver complaints, particularly regarding IMA warnings triggered by cloverleaf highway on-ramps and elevated roads that crossed over other roadways, led manufacturers to adjust the safety applications to accommodate the these originally-unexpected "warning" conditions. The SPMD experience proved that these adjustments significantly reduced false positive warnings for this application.

At this time, NHTSA cannot account preemptively for the possibility of future false positive warnings. Given that we are only proposing today to mandate V2V transmission capability and are not yet requiring specific safety applications, we are not developing requirements for how safety applications must perform, and we recognize that doing so would be a significant undertaking. We do expect, however, that manufacturers will voluntarily develop and install safety applications once V2V communications capability is required available. As with existing advanced crash avoidance systems and as in the SPMD, we expect manufacturers

[174] See, e.g., Nodine et al., "Independent Evaluation of Light-Vehicle Safety Applications Based on Vehicle-to-Vehicle Communications Used in the 2012-2013 Safety Pilot Model Deployment," USDOT Volpe Center, DOT HS 812 222, December 2015, Section 5.1. Available at Docket NHTSA-2016-0126.

to address false positive issues that arise in use in order to improve customer satisfaction. Because false positive issues with V2V-based safety applications are typically a software issue rather than a hardware issue Manufacturers may even be able to solve by deploying solutions to such problems through over-the-air software updates, rather than requiring vehicles to be brought in for adjustment. Data from the SPMD suggests that it is possible to reduce false positives in production safety applications and thus we believe it should not pose a significant public acceptance issue for V2V. Additionally, if NHTSA determines in the future that false positives in the field create an unreasonable risk to safety, NHTSA could pursue remedies for them through its enforcement authority.

2. Privacy

If consumers fear that V2V communications will allow their movements to be "tracked," either for government or private purposes, and that such information could be used to their detriment, they may avoid buying new cars with V2V systems installed, or attempt to disable the V2V systems in their own vehicles. Concerns about privacy directly implicate consumer acceptance. For this reason, in addition to NHTSA's obligation under federal privacy law to identify the privacy impacts stemming from its regulatory activities,[175] the Agency also must consider consumer privacy carefully in our development of V2V requirements. For example, as discussed above, SAE J2735 BSM specification contains a series of optional data elements, such as vehicle identification number (VIN), intended to be broadcast as part of the V2V transmission that enables safety applications. Because the Agency has determined that transmission of VIN and other information that directly identifies a specific vehicle or its driver or owner could create significant privacy risks for private consumers, this proposal contains performance requirements that exclude from the BSM such explicitly identifying data. The Agency also is concerned that other data elements in the BSM potentially could be used to identify specific individuals when combined over time and with data sources outside of the V2V system. For this reason, we have proposed a more general exclusion of "reasonably linkable" data elements from the BSM to minimize consumer privacy risk that could result from associating BSMs with specific individuals. We discuss our privacy risk analysis in more in detail in Sections IV.C and IV.D, and in the draft PIA published concurrent with this NPRM.

NHTSA expects manufacturers to pursue a privacy positive approach to implementing the proposed V2V requirements. In furtherance of the Fair Information Practice Principles (FIPPs), especially those of transparency and notice, we have developed a draft privacy statement that we will require manufacturers to provide to consumers, included in the regulatory text below. In order to ensure effective notice, we intend for manufacturers to provide this statement to consumers in understandable, accessible formats and at multiple easily identifiable locations and times, including but not limited to the time of sale. We seek comment from the public on the most effective time and means of providing such multi-layered notice to

[175] Section 522 of the Consolidated Appropriations Act, 2005, Pub. L. 108-447

individuals purchasing new and used vehicles with V2V systems. We note that the industry has developed a set of voluntary privacy principles for vehicle technologies and services, which have been accepted by members of both the Alliance and Global Automakers, covering the significant majority of motor vehicle manufacturers.[176] We also seek comment from the public on how these principles would apply to V2V communications, as detailed in this NPRM, and the extent to which application of these voluntary minimum principles in the V2V context would provide adequate notice and transparency to consumers.

To date, vehicle technologies that have raised privacy concerns for consumers have been "opt-in," meaning that either consumers expressly agree to the use of these technologies in their vehicles (and thereby provide explicit consent) or consumer purchase vehicles containing technologies not mandated by NHTSA (and thereby, arguably, provide implicit consent). V2V presents a somewhat different situation, as we are proposing that at least 50 percent of new vehicles will be required to have V2V devices starting in model year 2021. Since this would be a mandated technology, consumer choice will be limited to the decision of whether or not to purchase a new car (all of which eventually would contain V2V technology, if mandated). From a privacy perspective, such implicit consent is not an optimal implementation of the FIPPs principle of consumer choice. However, as discussed below in Section VI.C., the agency has determined that there are no viable alternatives to a mandate of V2V technology. In the agency's view, the absence of consumer choice is required to achieve safety in the V2V context, increasing the significance of ensuring that industry deploys V2V technology in a privacy positive, transparent manner and provides consumers with effective, multi-layered privacy notice. Consumers who are privacy-sensitive tend to feel more strongly when the government is mandating something that creates potential privacy risks to individuals, as compared to when they voluntarily choose whether to purchase and use such technology. NHTSA and vehicle manufacturers will continue to work to ensure that V2V does not create the type of privacy impacts frequently raised in comments, and will need to educate consumers about the potential privacy impacts and privacy-enhancing controls designed into the V2V system. That said, NHTSA seeks comment on the extent to which an if-equipped approach potentially may provide consumers with more of a choice to "opt in" to V2V technology – or whether, if mandated, consumers should be provided an "opt out" option for privacy reasons.

3. Hacking (cybersecurity)

If consumers fear that V2V will allow wrongdoers to break into their vehicle's computerized systems and take control of vehicle operation, then, as with privacy concerns, they may avoid purchasing new vehicles equipped with V2V or attempt to remove already-installed V2V in their own vehicles. This fear is really a two-part concern: (1) that V2V equipment can be "hacked," and (2) that *if* V2V equipment can be hacked, the consumer's safety may be at risk.

---

[176] "PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES" available at http://www.autoalliance.org/?objectid=865F3AC0-68FD-11E4-866D000C296BA163 (last accessed dec 7, 2016).

Regarding the concern that V2V equipment can be hacked, as discussed in much more detail in Section III.E.7 above, counter measures have been identified using a risk-based approach to determine the types of threats and risks to the equipment that may occur. We are proposing to require additional hardening of the on-board V2V equipment beyond normal automotive-grade specifications to help reduce the chance of physical compromise of V2V. In addition we have included alternatives for message authentication and misbehavior reporting to solicit comment regarding to further reduction of cybersecurity risk in V2V message exchange. We seek comment on what additional requirements, if any, we might consider adding to the standard to mitigate infiltration risk yet further. If commenters believe additional steps are needed, we ask that they describe the protection mechanism and/or approach as fully as possible, and also provide cost information to accomplish them – or whether, if mandated, consumers should be provided anoption to disable V2V for cybersecurity reasons.

Regarding the concern that V2V equipment, if hacked, can create a safety risk, NHTSA expects manufacturers to ensure that vehicle systems take appropriate safe steps to the maximum extent possible, even when an attack may be successful.[177] These can include protective/preventive measures and techniques like isolation of safety-critical control systems networks or encryption and other hardware and software solutions that lower the likelihood of a successful hack and diminish the potential impact of a successful hack; real-time intrusion detection measures that continually monitor signatures of potential intrusions in the electronic system architecture; real-time response methods that mitigate the potential adverse effects of a successful hack, preserving to the extent possible the driver's ability to control the vehicle; and information sharing and analysis of successful hacks by affected parties, development of a fix, and dissemination of the fix to all relevant stakeholders. In July 2015, in response to NHTSA's challenge, the auto industry created an Information Sharing and Analysis Center ("ISAC") to help the industry proactively and uniformly address cybersecurity threats, and we would expect that such a body could be a useful forum for addressing V2V-related security risks, if any. A number of auto manufacturers are also rapidly ramping up internal teams to identity and address cybersecurity risks associated with new technologies.[178]

In March 2014, researchers from Galois, Inc. issued a white paper with specific recommendations for reducing security risk associated with V2V communications, which they

[177] Additional information about NHTSA's approach to automotive cybersecurity is available at http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity (last accessed Sept. 23, 2015).

[178] See, e.g., King, Rachel, "GM Grapples with Big Data, Cybersecurity in Vehicle Broadband Connections," Wall Street Journal, Feb. 10, 2015. Available at http://blogs.wsj.com/cio/2015/02/10/gm-grapples-with-big-data-cybersecurity-in-vehicle-broadband-connections/ (last accessed Dec 7, 2016).

stated would "automatically rule out a whole class of security vulnerabilities" at low cost with known technologies.[179] The recommendations were as follows:

- All legal inputs shall be specified precisely using a grammar. Inputs shall only represent data, not computation, and all data types shall be unambiguous (i.e., not machine-dependent). Maximum sizes shall be specified to help reduce denial-of-service and overflow attacks.
- Every input shall be checked to confirm that it conforms to the input specification. Interface messages shall be traceable to mission-critical functionality. Non-required messages should be rejected.
- Parsers and serializers shall be generated, not hand-written, to ensure they do not themselves introduce any security vulnerabilities. Evidence should be provided that
    - *parse(serialize(m)) = m*, for all messages *m*, and
    - parse(i) = REJECT, for all non-valid inputs i.
- Fuzz testing shall be used to demonstrate that implementations are resilient to malicious inputs.
- A standardized crypto solution such as AES-GCM shall be used to ensure confidentiality, integrity, and the impossibility of reply attacks.

DARPA staff, in discussing V2V cybersecurity issues with DOT researchers, recommended these techniques be included in any V2V requirements going. NHTSA seeks comment on whether these specific techniques should be incorporated into the proposed FMVSS requirements, and if so, how; alternatively, NHTSA seeks comment on whether these techniques should be incorporated prior to vehicle manufacturer certification with the FMVSS, and if so, how, and how NHTSA would verify their incorporation.

4. Health

As discussed in more detail below in Section IV.E, a number of individual citizens commented to the ANPRM and Readiness Report that they were concerned about what they believed to be potentially negative health effects that could result from a DSRC mandate. As discussed in Section IV.E below, NHTSA has considered this issue carefully, and whether there are ways to mitigate these concerns without obviating the very real safety benefits that a V2V mandate will enable. We believe that consumer education, undertaken both by the Federal government and by vehicle manufacturers, may help to alleviate some of these concerns.

---

[179] See Launchbury, John, Dylan McNamee, and Lee Pike, Galois Inc., "A Technique for Secure Vehicle-to-Vehicle Communication," Mar. 9, 2014. Available at http://galois.com/wp-content/uploads/2014/07/whitepaper_SecureInterfaces.pdf (last accessed Dec 7, 2016).

5. Research conducted on consumer acceptance issues

Working with Booz Allen Hamilton, NHTSA has conducted additional research on consumer acceptance issues since the ANPRM and Readiness Report. The objective of the research was to conduct both qualitative and quantitative research to broaden our understanding of consumers' acceptance of V2V technology and to inform future outreach and communication efforts to the public. The qualitative phase included focus groups held in Spring of 2015. Focus group participants were shown a brief video on what V2V communications are, how they work, and how they contribute to vehicle safety, and then asked to discuss a series of questions about the technology, their understanding of it and interest in it, and benefits and drawbacks. Overall, on a scale of 1 to 10, the majority of focus group participants rated their interest in V2V as a 5 or higher for the next car. However, participants also expressed concern that the technology would not be effective if it were not universally adopted, and that over-reliance on or distraction by V2V warnings could cause drivers to become less attentive and increase risk. Although most focus group participants believed that V2V would allow drivers to be tracked, few were concerned with the privacy implications of tracking.[180]

Following the conclusion of the focus groups and analysis of their findings, a survey was developed for online quantitative testing to examine these issues further. The survey was conducted by Ipsos, under contract to BAH. The survey sought to evaluate several objectives:

- What is the degree of public acceptance of V2V?
- What proportion of people are concerned about each barrier? How much importance is attached to that concern?
- What proportion of people agree with the potential benefits of V2V? How much importance is attached to that benefit?
- How does the population differ on the above viewpoints (age, gender, urbanicity, etc.)?
- What are predictors of acceptance of V2V technology (age, gender, urbanicity, etc.)?

Over 1,500 people responded to the survey, and the sample was matched to the target population on age, gender, ethnicity, income, and region. Respondents viewed a brief informational video about V2V, and then answered 35 questions. Approximately half of respondents were interested in having V2V in their next car, with "accepters" tending to be male, older, urban, and more educated. All responses had a margin of error of +/- 2.5 percent

[180] "Vehicle to Vehicle Crash Avoidance Safety Technology: Public Acceptance Final Report" December, 2015. Available at Docket No. NHTSA-2016-0126

In terms of barriers or concerns, 69 percent of respondents believed that V2V would encourage other drivers to be too reliant and less attentive to the driving task, and over 50 percent expressed concern about cybersecurity and the need for enough vehicles to be equipped for the benefits to accrue. Between 30 and 40 percent expressed concern about tracking by the government or law enforcement and about the risk that they themselves could become too reliant and inattentive to driving. Only 20 percent expressed concern about health risk from electromagnetic activity. Of those concerns, however, some were deemed more important than others (that is, simply because respondents identified a risk, did not necessarily mean that they considered it an important risk). Respondents viewed law enforcement and government tracking as less important, but cybersecurity, other drivers' inattentiveness, and health risks as more important, when they were concerned about them.

In terms of benefits of V2V, 55 percent of respondents believed that V2V would reduce the number and severity of vehicle crashes, 53 percent believed that it would make driving more convenient and efficient, and 50 percent believed that V2V could lower insurance rates. As for barriers, respondents tended to believe that benefits for others would be somewhat greater than the benefits that they themselves would experience. Importance did not vary as much for benefits as it did for barriers.

In terms of how opinions about benefits and barriers correspond to whether a respondent wanted V2V in their next car, the survey results found that, on balance, all respondents were concerned about barriers, but "accepters" of V2V rated the benefits more highly. When asked how much they would be willing to pay for V2V, 78 percent of respondents were willing to pay less than $200.

Based on the research conducted thus far and assuming that the survey respondents are, as intended, reasonably representative of the nation as a whole, it appears that while there may be work yet for the agency and manufacturers to do in order to reassure consumers of V2V's benefits, there may not be a sufficient public acceptance problem that an FMVSS requiring V2V communications in new vehicles would face clear legal risk on that issue. NHTSA intends to continue researching approaches to consumer outreach on V2V and will work with industry and other relevant stakeholders in doing so. We seek comment on what the agency should consider in developing those approaches to best ensure the success of a future V2V system.

6. User flexibilities for participation in system

In the ANPRM, we sought comment on whether there were any issues relating to consumer acceptance that the agency had *not* yet considered, and asked how the agency should consider them for the NPRM. In response, a number of individual commenters expressed concern that they experience extreme sensitivity to electromagnetic radiation, and that therefore DSRC should not be mandated, or that if it was mandated, that the agency should allow drivers to disable it. Health issues raised in comments are covered below in Section IV.E, but the question of whether the agency should require or permit an "off switch" for V2V communications arose when commenters suggested it as a way to mitigate concerns over health effects. A handful of other individual commenters stated that the agency should allow drivers to

turn off DSRC for privacy or security reasons, out of concern that DSRC transmissions could allow their movements to be tracked, or that the device could be hacked by malicious third parties to obtain personal information about the driver. A number of individual commenters raising these concerns about health or tracking suggested that they would attempt to disable V2V in their vehicles, or only purchase older vehicles without V2V.

While NHTSA had asked in the ANPRM whether commenters had thoughts regarding whether V2V-based *warnings* should be permitted to be modified or disabled,[181] in the interest of maximizing safety benefits, NHTSA had not considered allowing manufacturers to provide consumers with a mechanism to disable V2V itself, whether temporarily or permanently.

Generally, if NHTSA concludes that a vehicle system or technology provides sufficient safety benefits that it should be required as an FMVSS, NHTSA has not permitted it to be disabled. In fact, Congress expressly prohibits manufacturers, distributors, dealers, and motor vehicle repair businesses from knowingly making inoperative any part of a device or element of design installed on or in a motor vehicle in compliance with an applicable motor vehicle safety standard prescribed by NHTSA.[182] In some cases, however, NHTSA has established FMVSSs that permit system disablement or alteration when there is a clearly-defined safety need for doing so.

For example, FMVSS No. 126 for electronic stability control (ESC) allows manufacturers to include an "ESC Off" control that puts the system in a state where ESC does not meet the FMVSS performance requirements, as long as the system defaults to full ESC capability at the start of the next ignition cycle and illuminates a telltale in the meantime to warn the driver that ESC is not available.[183] NHTSA allowed the ESC Off control because we were aware that in certain driving situations, ESC activation could actually make driving *less* safe rather than *more* safe – if a driver is stuck in deep snow or sand and is trying to free their vehicle, quickly spinning wheels could cause ESC to activate when it should not. Additionally, the agency was concerned that drivers who did not have the option of disabling ESC when absolutely necessary might find their own, permanent way to disable ESC completely. Having an off switch that reverted to full functionality at the next ignition cycle at least allowed ESC to continue providing safety benefits the rest of the time. NHTSA concluded that allowing temporary disablement was better than risking the permanent loss of safety benefits.[184]

---

[181] *See* 79 Fed. Reg. 49270, at 49272 (Aug. 20, 2014) (Question 13 in the ANPRM asks whether commenters believe that V2V-based warnings should be permitted to be modified or disabled)
[182] *See* 49 U.S.C. 30122(b).
[183] *See* 49 CFR part 126, S5.4. We note that despite the overarching requirement to return to full functionality at the new ignition cycle, S5.4 does not require ESC to return to full functionality if the vehicle is in a mode for "low-speed, off-road driving," or if the front and rear axles are locked because the vehicle is in some sort of 4WD mode.
[184] 72 Fed. Reg. at 17279-80 (Apr. 6, 2007).

As another example, FMVSS No. 208 for occupant crash protection allowed manufacturers to include a device up until September 1, 2012, that deactivated the right front passenger seat air bag, but only in vehicles without a second row of seating, or in vehicles where the second row of seating is smaller than a specified size.[185] Like the ESC Off function, the "passenger air bag off" function also requires a telltale to illuminate to warn the driver that the air bag is disabled; unlike the ESC Off function, the passenger air bag off function, if present, remains deactivated until it is reactivated by means of the deactivation device (i.e., the driver presses the button again, rather than the air bag simply reactivating at the start of the next ignition cycle).[186] In establishing this option, the agency noted public acceptance issues with advanced air bags, and stated that allowing on-off switches for some period after all vehicles were equipped with advanced air bags would help parents feel more confident about the system's reliability based on real-world experience.[187]

Thus, in prior instances when NHTSA has allowed drivers the option of changing or disabling the functionality of a required safety system, it has been in the interest of providing *more* safety. Similarly, were V2V to impose substantial new safety risks, there could be a safety reason to disable transmission and reception of messages. To the extent that consumers may wish that the agency allow a way for them to disable V2V because of concerns about privacy or cybersecurity, we reiterate our position as discussed in Sections IV.B and IV.C on privacy and Section V on security we have worked to design requirements that reduce the possibility of such threats. To the extent that consumers wish a mechanism to disable V2V devices out of concern over potential health effects, we note simply that disabling your own V2V unit would not help you avoid V2V transmissions, because other light vehicles will also be equipped with the technology, and if you have your own vehicle it is presumably for the purpose of traveling to places where other vehicles also go. Turning V2V off for this reason would forfeit the safety benefit of being "seen" by other vehicles" and "seeing" other vehicles, without providing any other benefit.

Moreover, unlike for most of the prior technologies in which NHTSA allowed drivers the option of changing or disabling the functionality of a required safety system, allowing V2V communications to be disabled would affect the safety of more drivers than just the driver who turned off their own V2V device. A cooperative system like V2V protects you by making you more "visible" to other drivers and by letting you know when they pose imminent risks to you. A driver who disables V2V on their vehicle makes their vehicle less visible to other drivers,

---

[185] *See* 49 CFR part 208, S4.5.4.

[186] *Id*.

[187] Deactivation of the "advanced" right front passenger air bag was primarily intended to address the possibility that, in vehicles with no (or very small) back seats, a child seat might have to be placed in the front passenger seat rather than in the back. The primary mechanism to mitigate the risk of the front passenger air bag deploying when a child seat is present is a suppression system, but the agency allowed vehicle manufacturers to include an off switch for several years to improve parents' confidence that the suppression systems were working successfully in the field. *See* 65 FR at 30723 (May 12, 2000).

potentially affecting their own relative safety risk and the safety risk to those around them. The safety benefits from a cooperative system could be undermined by allowing drivers to opt out. If there is no safety benefit from opting out, and doing so would undermine safety benefits both for the driver who opts out and for drivers around them, opting out may not be justified.

However, V2V is a novel technology concept in the transportation context, which differs in some ways from other technologies covered by the FMVSS. NHTSA recognizes that, as discussed elsewhere in this notice, any technology that is required to transmit and receive information on a persistent basis creates potential privacy and cybersecurity risks. NHTSA is making every effort to reduce these risks while setting requirements that would provide life-saving benefits. That said, we acknowledge that there may be circumstances when there could be a need to deactivate the V2V device on a vehicle. These may include individuals or groups with specific privacy needs, the emergence of unanticipated cybersecurity threats, or other reasons. To address these cases, NHTSA is requesting comment on possible approaches to deactivating V2V related hardware and software as and when appropriate, as well as the costs and benefits of such approaches. These could include deactivations initiated by drivers, manufacturers, or the government; with different scopes, such as vehicle-specific or broader deactivations; with different lengths, such as for a single key start or more long-lasting; and with different levels of ease, such as an accessible consumer-friendly method or one that would require mechanical expertise.

C. Consumer Privacy

NHTSA takes consumer privacy very seriously. Although collection of data by on-board systems such as Event Data Recorders and On-Board Diagnostic systems is nothing new, the connectivity proposed by the Agency will expand the data transmitted and received by cars. V2V systems will create and transmit data about driver behavior and the surrounding environment not currently available from most on-board systems. For this reason, V2V and future vehicle to infrastructure and pedestrian (V2X) technologies raise important privacy questions.

The agency is committed to regulating V2V communications in a manner that both protects individuals and promotes this important safety technology. NHTSA has worked closely with experts and our industry research partners (CAMP and the VIIC) to design and deploy a V2V system that helps protect consumer privacy. As conceived, the system will contain multiple technical, physical, and organizational controls to reduce privacy risks – including those related to vehicle tracking by individuals and government or commercial entities. As proposed, V2V messages will not contain information directly identifying a vehicle (as through VIN, license plate or registration information) or its driver or owner (as through name, address or driver's license number), or data "linkable, as practical matter," or "reasonably linkable" to an individual. NHTSA intends for these terms to have the same meaning, specifically: capable of being used to identify a specific person on a persistent basis without unreasonable cost or effort, either in real time or retrospectively, given available data sources. Our research to date suggests that using V2V transmissions to track the path and activities of identified drivers or owners, while possible,

could be a complex undertaking and may require significant resources and effort.[188] The Agency has concluded that excluding "reasonably linkable" data elements from the BSM will help protect consumer privacy appropriately and meaningfully while still providing V2V systems in vehicles with sufficient information to enable crash-avoidance safety applications.

We request comment on the proposed mandate that the BSM exclude data elements "reasonably linkable" to an individual (as that term is defined above) and whether this appropriately balances consumer privacy with safety. Additionally, will exclusion from the BSM of "reasonably linkable" data elements undermine the need for a standard BSM data set in furtherance of interoperability or exclude data required for safety applications?

NHTSA, with the support of the DOT Privacy Officer and NHTSA's Office of the Chief Information Officer, conducted an interim privacy risk assessment of the V2V system prior to issuance of the Readiness Report and ANPRM. The interim assessment was intended to provide the structure and serve as a starting point for NHTSA's planned PIA, which is a more in-depth assessment of potential privacy impacts to consumer privacy that might stem from a V2V regulatory action, and of the system controls that mitigate those risks. On the basis of then available information and stated assumptions, NHTSA's interim privacy assessment identified the system's business needs, relevant system functions, areas of potential risks, and existing/other risk-mitigating technical and policy controls.

NHTSA received a significant number of comments on the issue of privacy in response to the ANPRM and Readiness Report. Generally, the privacy comments related to consumer acceptance and reflected consumer and industry concerns that the V2V system would be used by government and commercial entities to track the route or activities of individuals, or would be perceived by individuals to have that capability. A vast majority of the privacy comments addressed one or more of the following areas:

1. NHTSA's privacy impact assessment;
2. "privacy by design" and data privacy protections;
3. data access and privacy;
4. consumer education; and
5. Congressional or other government action related to V2V data.

Since receiving these comments, NHTSA has worked closely with privacy experts to identify and prioritize for further analysis specific areas of potential privacy impact in the V2V system. Additional privacy research, such as dynamic modeling related to location tracking and

---

[188] See Reports: FHWA-JPO-15-237 – "Final Design Analysis Report"September 18, 2015, FHWA-JPO-15-236 – "Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework (Final-Rev A)" February 24,2016, FHWA-JPO-15-235– "Final Requirements Report" September 11, 2015, and "Technical Memorandum: Modeling and simulation of Areas of Potential V2V Privacy Risk"March 8, 2016 located in Docket No. NHTSA-2016-0126

analysis of PKI best practices, is underway that will refine NHTSA's approach to mitigating potential privacy impacts stemming from the V2V system. On the basis of the PIA, comments received on the NPRM and PIA, and ongoing privacy research, agency decision-makers will be in an informed position to determine whether any residual risk (i.e., risk in the system that cannot reasonably be mitigated) is acceptable – and, in the alternative, whether functionality should be sacrificed in order to achieve an acceptable level of residual risk, and if so, what functionality.

1. NHTSA's PIA

Over a dozen organizations requested that NHTSA conduct a privacy impact assessment (PIA) of the V2V system as proposed in the NPRM. Many of these commenters noted additionally that a PIA will be critical to consumer acceptance of V2V. Several organizations requested that NHTSA take steps (in addition to conducting a PIA) to help enhance and speed consumer acceptance of V2V technologies. Comments relating to the scope of NHTSA's PIA included a request that NHTSA broaden the scope of its privacy analysis to include privacy impacts associated with vehicle to infrastructure (V2I) and vehicle to "other" (such as pedestrians) (V2X) applications, and also that NHTSA release privacy research underlying its PIA.

The Alliance of Automobile Manufacturers (Alliance) suggested that NHTSA hold public workshops with the Federal Trade Commission (FTC) to thoroughly investigate privacy issues related to the V2V system. It also recommended that NHTSA expand the scope of the PIA so that it "considers all possible uses of the envisioned transportation communications network including all potential internal and external abuses, and other challenges not solely those concerned with safety, mobility and the environment." The Automotive Safety Council recommended that an independent third party review the PIA. Finally, the Electronic Frontier Foundation (EFF) and Privacy Rights Clearinghouse requested that NHTSA release all initial risk assessments and research on which its initial risk assessment and PIA are based, including those related to location tracking and identification capabilities. Additionally, the Alliance took the position that PIA should analyze the privacy concerns relating to the broader V2X communications infrastructure, which includes commercial venture, law enforcement, and taxation issues. The FTC requested that NHTSA take into account the Fair Information Practice Principles (FIPPs) framework in regulating the V2V system.

NHTSA agrees with commenters emphasizing the critical importance of issuing a PIA detailing the agency's analysis of the potential privacy impacts of the V2V system as proposed in the NPRM. Not only is NHTSA required by law[189] to do so, but the FIPPs-based privacy-risk analysis documented in the PIA has informed NHTSA's proposal significantly, and helped to refine the privacy controls that NHTSA and its research partners designed into the V2V system to mitigate potential privacy impacts, including that related to vehicle tracking. NHTSA intends

[189] Section 522 of the Consolidated Appropriations Act, 2005, Pub. L. 108-447

to work closely with the FTC, which is the primary federal agency with authority over consumer privacy and data security, on consumer privacy issues related to theV2V system. Such intra-governmental collaboration is likely to include coordination on the PIA and ongoing privacy research. It may also include conducting joint public meetings or workshops with stakeholders following issuance of the NPRM and PIA, which has undergone intra-governmental review. For a variety of reasons, NHTSA did not (and could not) have it reviewed by non-governmental third parties prior to publication. However, NHTSA looks forward to receiving comments on the privacy issues discussed in the NPRM and PIA from a broad range of stakeholders and other interested entities.

With regard to the scope of NHTSA's PIA, the agency wishes to emphasize that, to the extent possible in the context of a still evolving V2V ecosystem, our PIA intentionally is scoped to take into account potential internal and external threat actors and potential abuses of the V2V system -- not solely those directly related to safety, mobility or environmental applications. As discussed in the PIA Summary section below, NHTSA's PIA focusses not on specific V2V system components or applications. Rather, it focuses on data transactions system-wide that could have privacy impacts, and the controls that mitigate those potential impacts. To the extent that specific V2V data transactions might be vulnerable to privacy impacts, our risk-analysis broadly considers potential threats posed by a wide range of internal and external actors, including foreign governments, commercial non-government entities, other non-governmental entities (such as research/academic actors and malicious individuals or groups). Additionally, our analysis takes into account potential privacy impacts posed by internal V2V system actors.

2. Privacy by Design and Data Privacy Protections

Many commenters requested that NHTSA deploy the V2V system in a way that ensures drivers' privacy and the security of the system. Some sought specific privacy protections, such as "total anonymity" if drivers cannot opt out of the V2V system, the protection of any PII associated with the system, and avoidance of using any PII at all. Commenters also sought end-to-end encryption of any PII, no local or remote V2V data storage, and limitations on V2V data collection, as well as technical and administrative safeguards on any V2V data collected.

Mercedes-Benz commented that the security entity envisioned to secure the V2V system, called the Security Credential Management Server (SCMS), must have security and privacy controls to protect against external threats and internal abuses. Fiat Chrysler Automobiles (FCA) expressed concern about the potential privacy impacts of the security system's design, called the certificate revocation list (CRL). The National Motorists Association emphasized safeguarding V2V messages sent via mandated V2V devices. Infineon Technologies pointed out that the unique cellular subscriber number would defeat the privacy and tracking requirement in the system, as proposed, to the extent that cellular is used as a V2V communications media. American Trucking Association requested that NHTSA protect the confidentiality of proprietary information, such as lane density, vehicle specifications, and trip origin and destination. The Association of Global Automakers (Global) and GM stated that V2V, as envisioned, does not pose significant risks to the privacy of individuals. By contrast, EFF stated the exact opposite,

noting its concern that the V2V system as discussed in the ANPRM and Readiness Report does not protect the privacy of drivers adequately.

Based on our exploration of privacy impacts and analysis of the V2V system design to date, we respectfully disagree with the position espoused by EFF that the V2V system fails to protect driver privacy. The system contains multiple technical and organizational controls to help mitigate unreasonable privacy risks posed by external actors including those posed by SCMS insiders. V2V transmissions would exclude data directly identifying a private motor vehicle or its driver or owner and reasonably linkable to an individual via data sources outside of the V2V system or over time. V2V devices would transmit safety information in only a limited geographical range. Neither the V2V system, nor its components (including OBEs) would collect or store the contents of messages sent or received, except for a limited time to maintain awareness of nearby vehicles for safety purposes or case of device malfunction. Additionally, the system described in our proposal would be protected by a complex PKI security infrastructure designed specifically to help mitigate privacy impacts and create a secure V2V environment in which motorists who do not know one another can participate in the system without personally identifying themselves or their vehicles.

As discussed in the PIA and demonstrated by the data flows detailed in that document, the CRL discussed in the misbehavior reporting section of our primary proposal also would be designed to mitigate privacy impacts to individuals. It would contain specific information sufficient to permit V2V devices to use certificate information to recognize safety messages that should be ignored, if received. However, the CRL would not contain identifying information about specific vehicles or specific certificate numbers – nor would the information on the CRL permit third parties or SCMS insiders to identify specific vehicles or their owners or drivers.

The Agency understands that concern about whether the V2V system can or will be used by government and commercial entities to track the route or activities of individuals is critical to consumer acceptance and the viability of NHTSA's proposal. DOT is continuing to work with privacy experts to identify additional controls that might further mitigate any privacy risks (including that of tracking) in the V2V system, no matter how remote. The planned implementation by DOT of a proof of concept (PoC) security entity (discussed in Section V.B.6.e)) and related policy research will provide an operational environment in which to continue to explore the viability of additional privacy controls applicable to the V2V system, as currently envisioned and designed.

That said, as we noted in the Readiness Report, it is important to emphasize that residual risk stemming from the V2V system will never be zero due in part to the inherent complexity of the V2V system design and the diversity/large number of interacting components/entities, both technological and human. Additionally, technology changes at a rapid pace and may adversely impact system controls designed to help protect privacy in unforeseen ways. For these reasons, as is standard practice in both the public and private sectors, NHTSA has performed a PIA to identify potential areas of residual risk and resulting privacy consequences/harms that might result from its proposal. The current status of NHTSA's PIA is summarized below. The technical framework for the V2V system has gone through many iterations and adjustments

during the conduct of the V2V research program, as the system has evolved to meet revised or additional needs and to incorporate the results of research. For this reason, while the current technical framework is sufficient for purposes of NHTSA's rulemaking proposal, DOT's assessment of the potential privacy impacts that could result from the V2V proposal necessarily will be an ongoing process that takes into account future adjustments to the technology and security system required to support the technology, as well as ongoing privacy research. After reviewing comments on the NPRM and PIA and working closely with the FTC and stakeholders to address privacy concerns, NHTSA will issue an updated PIA concurrent with its issuance of a V2V final rule.

3. Data Access, Data Use and Privacy

The issue of data ownership arose in the comments of Ford, Auto Care Association, and others. All of these commenters requested clarification of who owns the data generated by the V2V system. Many commenters asserted that vehicle owners should own V2V and other data generated by motor vehicles, generally. Systems Research Associates requested a specific regulation vesting ownership in vehicle owners, not manufacturers. Another commenter expressed concern about ownership of data inherent in the context of car sharing and rentals arrangements.

The inherently related concept of consumer consent also appeared in many privacy comments. Civil liberties organizations suggested that NHTSA mandate that consumers provide "active consent" in the form of express written consent before manufacturers may collect data containing personally identifiable information (PII). Manufacturers requested that NHTSA ensure transparency by requiring that consumers authorize collection of PII through either consent or contract, and that manufacturers inform vehicle owners of what information will be collected and how this information will be used. This approach to transparency is consistent with industry privacy principles adopted in 2014 by members of the Alliance and the Association of Global Automakers, entitled "Consumer Privacy Protection Principles for Vehicle Technologies and Services" (OEM Privacy Principles or Principles), discussed in prior sections. Several manufacturers and civil liberties organizations, including EPIC and EFF, suggested that these voluntary industry principles should serve as a baseline for data privacy protections in the V2V context. EPIC also suggested that NHTSA follow the White House's Consumer Privacy Bill of Rights.

NHTSA feels strongly that in the context a V2V system based on broadcast messages, the critical consumer privacy issue is not that of data ownership, but that of data access and use – ensuring that the consumer has clear, understandable and transparent notice of the makeup of the V2V message broadcast by mandated V2V equipment, who may access V2V messages emanating from a consumer's motor vehicle, and how the data in V2V messages may be collected and used. For this reason, NHTSA proposes that motor vehicle manufacturers, at a minimum, include the following standard V2V Privacy Statement (set forth below) in all owner's manuals (regardless of media) and on a publicly-accessible web location that current and future owners may search by make/model/year to obtain the data access and privacy policies applicable to their motor vehicle, including those specifically addressing V2V data and functions. We also

seek the public's assistance in identifying additional formats and methods for providing this privacy statement to consumers that with the goal of achieving the timely and effective notice desired – notice that has increased significance in the context of a V2V mandate that effectively (and by design to achieve safety ends) limits consumer choice and consent.

4. V2V Privacy Statement

a) V2V Messages

The National Highway Traffic Safety Administration (NHTSA) requires that your vehicle be equipped with a Vehicle-to-Vehicle (V2V) safety system. The V2V system is designed to give your vehicle a 360 degree awareness of the driving environment and warn you in the event of a pending crash, allowing you to take actions to avoid or mitigate the crash, if the manufacturer of your vehicle has installed V2V safety applications.

Your V2V system periodically broadcasts and receives from all nearby vehicles a V2V message that contains important safety information, including vehicle position, speed, and direction. V2V messages are broadcast ten times per second in only the limited geographical range (approximately 300 meters) necessary to enable V2V safety application to warn drivers of pending crash events.

To help protect driver privacy, V2V messages do not directly identify you or your vehicle (as through vehicle identification number or State motor vehicle registration), or contain data that is reasonably or, as a practical matter, linkable to you. For purposes of this statement, V2V data is "reasonably" or "as a practical matter" linkable to you if it can be used to trace V2V messages back to you personally for more than a temporary period of time (in other words, on a persistent basis) without unreasonable expense or effort, in real time or after the fact, given available data sources. Excluding reasonably linkable data from V2V messages helps protect consumer privacy, while still providing your V2V system with sufficient information to enable crash-avoidance safety applications.

b) Collection, Storage and Use of V2V Information

Your V2V system does not collect or store V2V messages except for a limited time needed to maintain awareness of nearby vehicles for safety purposes or in case of equipment malfunction. In the event of malfunction, the V2V system collects only those messages required, and keeps that information only for long enough to assess a V2V device's misbehavior and, if a product defect seems likely, to provide defect information to your vehicle's manufacturer.

NHTSA does not regulate the collection or use of V2V communications or data beyond the specific use by motor vehicles and motor vehicle equipment for safety-related applications. That means that other individuals and entities may use specialized equipment to collect and aggregate (group together) V2V transmissions and use them for any purpose including applications such as motor vehicle and highway safety, mobility, environmental, governmental and commercial purposes. For example, States and localities may deploy roadside equipment

that enables connectivity between your vehicle, roadways and non-vehicle roadway users (such as cyclists or pedestrians). These technologies may provide direct benefits such as use of V2V data to further increase your vehicle's awareness of its surroundings, work zones, first responders, accidents, cyclists and pedestrians. State and local entities (such as traffic control centers or transportation authorities) may use aggregate V2V safety messages for traffic monitoring, road maintenance, transportation research, transportation planning, truck inspection, emergency and first responder, ride-sharing, and transit maintenance purposes. Commercial entities also may use aggregate V2V messages to provide valuable services to customers, such as traffic flow management and location-based analytics, and for other purposes (some of which might impact consumer privacy in unanticipated ways). NHTSA does not regulate the collection or use of V2V data by commercial entities or other third parties.

While V2V messages do not directly identify vehicles or their drivers, or contain data reasonably linkable to you on a persistent basis, the collection, storage and use of V2V data may have residual privacy impacts on private motor vehicle owners or drivers. Consumers who want additional information about privacy in the V2V system may review NHTSA's V2V Privacy Impact Assessment, published by The U.S. Department of Transportation at http://www.transportation.gov/privacy.

If you have concerns or questions about the privacy practices of vehicle manufacturers or third party service providers or applications, please contact the Federal Trade Commission. https://www.ftc.gov.

5. Consumer Education

Many commenters emphasized the need to educate consumers about the V2V system to enhance public acceptance through a coordinated and wide-spread information campaign utilizing traditional print and television outlets and the web, including the AAA, Global, Arizona Department of Transportation, Cohda Wireless, GM, Infineon Technologies, National Motorists Association, Pennsylvania Department of Transportation, Toyota, TRW Automotive, Automotive Safety Council, and Delphi Automotive.

Comments from the Automotive Safety Council, TRW Automotive, and Delphi Automotive suggested that such education should focus on the V2V safety message, what it contains, and how any information in the BSM will be used. The National Motorists Association recommended that NHTSA educate motorists on the system's privacy protection assurances. AAA recommended educating the public on how the V2V system will benefit them, and on the privacy and security protections built into the system. Toyota suggested that NHTSA educate the public about the fact that the V2V system will not transmit or store PII. The Privacy Rights Clearinghouse suggested that NHTSA educate the public on how the V2V system works. Honda focused more on educating the public on the security designed into the V2V system.

NHTSA agrees with commenters that educating the public about this important new safety technology, and the security and privacy protections designed into the V2V system, will be critical to consumer acceptance. For this reason, as suggested by many commenters, the

agency plans to work closely with the FTC, motor vehicle manufacturers, privacy advocates and other stakeholders to design a comprehensive public education strategy on the topic of privacy in the V2V system for consumers. Any claims regarding security or privacy made as part of NHTSA's public outreach will necessarily be justified by evidence based on the best scientific knowledge regarding security and privacy. Development of a consumer education strategy will likely be among the privacy-specific topics addressed in public meetings and/or workshops held by the agency after issuance of the NPRM and PIA.

6. Congressional/Other Government Action

NHTSA received comments from civil liberties groups and manufacturers that included calls on Congress to take action to protect consumer privacy in the V2V system. EFF and Privacy Rights Clearinghouse took the position that Federal legislation is imperative to protect driver privacy. The Alliance called on Congress to coordinate the relevant Federal agencies "to articulate a framework for privacy and security before further rulemaking proceeds" because, in its view, NHTSA alone does not have the authority to address V2V privacy and security issues. Honda and EPIC emphasized the need for ensuring that data is legally protected from third party access, and that unauthorized access is legally punishable. EPIC's comment focused on legal protections from OEM access, while Honda's comment focused on legal protections from government access.

NHTSA understands why legislation making it illegal for third parties or government agencies to collect V2V messages, or limiting those parties' retention or use of V2V messages, would be attractive to stakeholders – and the Alliance is correct in its assertion that such government action is outside the scope of the agency's regulatory authority over manufacturers of motor vehicles and motor vehicle equipment. As noted above, the introduction of V2V technology creates new privacy risks that cannot be fully mitigated. That said, in the agency's view, the V2V system is protected by sufficient security and privacy measures to mitigate unreasonable privacy risks. NHTSA seeks comment on these tentative conclusions -- and on whether new legislation may be required to protect consumer privacy appropriately.

D. Summary of PIA

1. What is a PIA?

Section 522 of the Consolidated Appropriations Act, 2005 (Pub. L. 108-447) requires that Federal agencies conduct privacy impact assessments (PIAs) of proposed regulatory activities involving collections or system of information with the potential to impact individual privacy. A PIA documents the flow of information and information requirements within a system by detailing how and why information is transmitted, collected, stored and shared to: (1) ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of the proposed data transactions; and (3) examine and evaluate protections and alternative processes for handling data to mitigate potential privacy impacts. It is a practical method of providing the public with documented assurance that the agency has identified and appropriately addressed potential privacy issues resulting from its activities. A

PIA also facilitates informed regulatory policy decisions by enhancing an agency's understanding of privacy impacts, and of options available for mitigating those potential impacts.

After reviewing a PIA, members of the public should have a broad understanding of any potential privacy impacts associated with a proposed regulatory action, and the technical and policy approaches taken by an agency to mitigate the resulting privacy impacts.

2. PIA Scope

The V2V system is complex and involves many different components, entities, communications networks, and data flows (within and among system components). For this reason, NHTSA opted not to analyze the potential privacy impacts in the V2V system on a component-specific basis. Rather, NHTSA focused its PIA on discrete data flows within the system, as an organic whole. NHTSA worked with privacy experts to zero in on discrete aspects of the V2V system most relevant to individual privacy for impact assessment purposes, identify and prioritize potential privacy impacts requiring further analysis (such as dynamic modeling), and validate the privacy-related requirements in NHTSA's regulatory proposal.

The V2V NPRM PIA identifies those V2V transactions involving data most relevant to individual privacy and the multiple technical, physical and policy controls designed into the V2V system to help mitigate potential privacy impacts.

To place our discussion of potential V2V privacy issues in context, NHTSA's PIA first briefly discusses several non-V2V methods of tracking a motor vehicle that currently exist.

3. Non-V2V Methods of Tracking

For comparative purposes, it is useful to consider the potential privacy impacts of the V2V system in the context of tracking mechanisms that do not involve any aspect of the V2V system (non-V2V tracking methods). These non-V2V methods of tracking inform the Agency's risk analysis because, to the extent that they may be cheaper, easier, and require less skill or access to a motor vehicle, they are relevant to our assessment of the likelihood of an individual or entity attempting to use V2V as a method of tracking. Examples of mechanisms that currently may be used to track a motor vehicle target include physical surveillance (i.e., following a car by visual observation), placement of a specialized GPS device on a motor vehicle, physical access to Onboard GPS logs, electronic toll transactions, cell phone history, vehicle-specific cell connections (e.g., OnStar), traffic surveillance cameras, electronic toll transponder tracking, and databases fed by automated license plate scanners. As compared to the potential approaches to V2V tracking discussed below, many of these non-V2V tracking methods appear may be cheaper, easier, require less (and/or no skill) under certain scenarios.

4. V2V Data Flows/Transactions with Privacy Relevance

As a starting point for the analysis that underlies this PIA, NHTSA identified and examined all data flows within the V2V system to determine which included data fields that may

have privacy impacts, either alone or in combination. We identified three data flows relevant for privacy impact purposes:

- Broadcast and receipt of V2V messages (also called Basic Safety Messages (BSMs)
- Broadcast and receipt of Misbehavior Reports
- Distribution of Certificate Revocation List (CRL)

Below, we describe these three data flows and detail the technical, policy and physical controls designed into the system to mitigate potential privacy impacts in connection with each flow. We then discuss the potential privacy impacts that remain, notwithstanding existing privacy controls. These constitute potential areas of residual risk for consideration by decision-makers.

a) Broadcast and Receipt of the Basic Safety Message (BSM)

BSMs are one of the primary building blocks for V2V communications. They provide situational awareness information to individual vehicles regarding traffic and safety. BSMs are broadcast ten times per second by a vehicle to all neighboring vehicles and are designed to warn the drivers of those vehicles of crash imminent situations.

Under NHTSA's proposal and any future adaptation of the technology, BSMs would contain information regarding a vehicle's GPS position, speed, path history, path trajectory, breaking status and other data, as detailed above in Section III.E. As discussed below, some data transactions necessitated by the security system may result in additional potential privacy impacts, some of which may be residual.

b) Broadcast and Receipt of Misbehavior Messages

Under NHTSA's proposal, when a vehicle receives a BSM from a neighboring vehicle, its V2V system validates the received message and then performs a cross check to evaluate the accuracy of data in the message. For example, it might compare the message content with other received messages or with equivalent information from onboard vehicle sensors. As a result of that cross check, the vehicle's V2V system may identify certain messages as faulty or "misbehaving." NHTSA's primary proposal for misbehavior reporting proposes that the V2V system then prepares a misbehavior report and sends it to the V2V security entity. The security entity evaluates the misbehavior report and may identify a defective V2V device. If it does, the V2V security entity will update the Certificate Revocation List (CRL) with information about the certificates assigned to the defective V2V device. The CRL is accessed by all V2V system components and vehicles on a periodic basis and contains information that warns V2V system participants not to rely on messages that come from the defective device. The security entity also might blacklist the device, in which case it will be unable to obtain additional security credentials from the security entity.

Also under our proposal, organizational and/or legal separation of information and functions within the security entity are important privacy impact-mitigating controls that are designed to prevent a single component or insider from having sufficient information to identify certificates assigned to a specific vehicle or owner. NHTSA plans to work closely with stakeholders to develop policies and procedures to institutionalize appropriate separation of data and functions within the National SCMS.

Under the second alternative for misbehavior reporting, the no misbehavior reporting proposal would not involve any additional broadcast or transmission of reports to V2V security entities. This means that no additional privacy risk would be imposed under the no misbehavior reporting alternative.

c) Misbehavior Reports

As described above, NHTSA's primary proposal for misbehavior reporting proposes that the V2V equipment in vehicles send misbehavior reports to the V2V security entity. Such reports will include the received BSM (which appears to be faulty) and other information, such as:

- Reporter's pseudonym certificate
- Reporter's signature
- Time at which misbehavior was identified
- 3D GPS coordinates at which misbehavior was identified
- List of vehicles (device/pseudonym certificate IDs) within range at the time
- Average speed of vehicles within range at the time
- Suspicion type (warning reports, proximity plausibility, motion validation, content and message verification, denial of service)
- Supporting evidence
    - Triggering BSM(s)
    - Host vehicle BSM(s)
    - Neighboring vehicle BSM(s)
    - Warnings
    - Neighboring devices
    - Suspected attacker

d) Distribution of Certificate Revocation List

As explained above, by evaluating misbehavior reports, the security entity envisioned may identify misbehaving V2V devices in vehicles and place information about those devices on the CRL. The security entity then would make updated CRLs available to V2V system participants and other system parts on a periodic basis to alert OBEs to ignore BSMs coming from the defective V2V equipment. There is only one type of CRL. Current system design

plans do not include placing individual security certificates on the CRL. Rather, each CRL would contain information (specifically, linkseed1, linkseed2, time period index, and LA Identifiers 1 and 2) that OBEs could use to calculate the values of the certificates in messages that should be ignored.

5. Privacy-Mitigating Controls

From the inception of the research program that would result in V2V technology over a decade ago, NHTSA has worked with its research partners, CAMP and the VIIC, to purse an integrated, privacy positive approach to the V2V system. For this reason, the V2V system described in our proposal would contain multiple layers of technical, policy and physical controls to help mitigate potential privacy impacts system-wide. Below, we discuss the privacy impact-mitigating controls that would apply to each of the three privacy-relevant data flows discussed above. In the course of this discussion, we detail some of the key privacy controls that we expect to see in a National SCMS (based on the current SCMS technical design, see Section V.B.2).

a) Privacy Controls Applicable to the Broadcast and Receipt of the Basic Safety Message (BSM)

(1) No directly identifying or "reasonably linkable" data in V2V transmissions

Under our proposals, the BSM would not contain information that directly identifies a private motor vehicle (as through VIN, license plate or registration information) or its owner or driver. BSM transmissions also would exclude data "reasonably linkable" or "as a practical matter" linkable to a specific individual.

(2) Rotating Security Credentials

Another critical control would help mitigate privacy risks created by signing messages. At the time of manufacture, a vehicle's V2V equipment would receive 3 years' worth of security certificates. Once the device is initialized into the V2V security system, the security system would send to the device keys on a weekly basis that will unlock 20 certificates at a time. During the course of the week, a vehicle's V2V equipment would use the certificates on a random basis, shuffling certificates at five minute intervals. These certificates would enable a vehicle's V2V system to verify the authenticity and integrity of a received BSM or, in the alternative, identify V2V messages that should be ignored (i.e., those that the security entity has identified as coming from misbehaving V2V equipment and placed on the CRL). The shuffling and random use of certificates every five minutes also will help minimize the risk of vehicle tracking by preventing a security certificate from becoming a de facto vehicle identifier (also referred to as a "quasi-identifier").

(3) Limited Transmission Radius

V2V equipment in vehicles would transmit safety information in a very limited geographical range, typically only to motor vehicles within a 300 meter radius of a V2V device. This limited broadcast is sufficient to enable V2V crash avoidance applications in neighboring vehicles, while limiting access by more geographically distant vehicles that cannot benefit from the safety information.

(4) No BSM Data Collection or Storage within the V2V system

Neither V2V devices in motor vehicles, nor the V2V system as a whole would collect or store the contents of V2V messages sent or received, except for the short time period necessary for a vehicle to use messages for safety applications or in the limited case of device malfunction. These technical controls would help prevent in-vehicle V2V equipment or the V2V system, as a whole, from after-the-fact tracking of a vehicle's location by accessing and analyzing a vehicle's BSMs. Although specialized roadside and mobile equipment would be able to access and collect BSMs, the V2V data collected would contain no information directly identifying or reasonably linkable to a specific private vehicle or its driver or owner, because the transmission of such information would not be allowed by the V2V rule. Research is ongoing on the methods, cost and effort required to use collected BSMs in combination with other available information or over time to track a specific, targeted vehicle or driver. The Agency believes that such linkage between collected BSMs and a specific vehicle or driver is plausible, but has not yet determined whether it is practical or reasonable, given the resources or effort required. This additional research will help to ensure that our proposed V2V FMVSS incorporates all available, appropriate controls to mitigate unreasonable privacy risk related to collection of BSM transmissions by roadside or mobile sensors. We acknowledge that introduction of this technology will result in residual privacy risk that cannot be mitigated. We seek comment on these tentative conclusions.

(5) FIPS-140 Level 3 HSM

NHTSA has proposed performance requirements that include use of FIPS-140 Level 3 hardware security module (HSM) in all V2V equipment in motor vehicles. This physical computing device would safeguard and manage a vehicle's security certificates and guard against equipment tampering and bus probing. This type of secure hardware provides evidence of tampering, such as logging and alerting of tampering, and tamper resistance such as deleting keys upon tamper detection.

(6) Consumer Notice

NHTSA would require that motor vehicle manufacturers, at a minimum, include a standard V2V Privacy Statement in all owner's manuals (regardless of media) and on a publicly accessible web location that current and future owners may search by make/model/year to obtain

the data access and privacy policies applicable to their motor vehicle, including those specifically addressing V2V data and functions, asdetailed in Section IV.C. As discussed above, NHTSA also considering the possibility of requiring additional methods for communicating the V2V Privacy Statement to consumers and seeks comment on the most effective methods for providing such notice.

b) Privacy Controls Applicable to Broadcast and Receipt of Misbehavior Messages

When a V2V device in a motor vehicle appears to malfunction, the V2V system would collect and store only BSMs relevant to assessing the device's performance, consistent with the need to address the root cause of the malfunction if it is, or appears to be, widespread.

(1) Encryption of Misbehavior Report

Like all security materials exchanged between V2V equipment in vehicles and a security authority, misbehavior reports would be encrypted. This would help limit but not prevent potential privacy risks that could stem from unintended or unauthorized access to data in misbehavior messages. Specifically, this would reduce the possibility that BSMs contained in misbehavior reports may provide information about the past location of a reporting vehicle (and thereby of the vehicle owner's activities and relationship between the two vehicles), or of vehicles located nearby the reporting vehicle.

(2) Functional/data separation across SCMS components

A key privacy-mitigating control applicable to this data stream is the technical design for the security entity proposed by NHTSA, which provides for functional and data separation across different organizationally and/or legally separate SCMS components. This technical control is designed to prevent individual SCMS entities or insiders from using information, including from misbehavior messages, for unauthorized purposes. The technical separation of information and functions within the security entity could be overcome only by a specific entity within the security organization (called the Misbehavior Authority or MA) after determining, based on misbehavior messages, that a vehicle's V2V equipment is malfunctioning and needs to be blacklisted (i.e., prevented from obtaining any additional security certificates). In order to do so, the MA would need to gather information from the various independent, separate parts of the security entity to identify the device to be blacklisted.

(3) Misbehavior Reports Are Stripped of Geographic Location Information

An example of information separation serving as a privacy control is evident in one particular component of the security organization – the Location Obscurer Proxy (LOP). Misbehavior messages (like other communications between a vehicle's V2V equipment and the security entity) travel through the LOP entity to get to other parts of the security organization.

The LOP would strip out information from the misbehavior message that otherwise would permit other parts of the security organization (like the MA) to associate a vehicle's V2V messages with its geographic location. This technical separation of geographic information from messages transmitted between vehicle's V2V systems and the security entity is designed to prevent individual security entities or V2V security organization insiders from colluding to use BSM information inappropriately or to track individual vehicles.

(4) Separation of Security Organization Governance

The design for the V2V security entity (or SCMS) calls for the separation of some critical functions into legally distinct and independent entities that, together, make up the SCMS. This legal separation of security entity governance is designed to prevent individual entities or V2V security organization insiders from colluding to use information for unauthorized purposes such as tracking individual vehicles.

c) Privacy Controls Applicable to Distribution of the CRL List

(1) Misbehaving V2V equipment in a vehicle stops broadcasting

It is possible that information regarding a vehicle's revoked security certificates could enable all revoked certificates to be associated with the same vehicle. This might be used to persistently identify a vehicle during the vehicles' activities. In order to mitigate this potential privacy risk, once a vehicle's V2V system determines that information about it is on the CRL and that the security organization has revoked its security certificates, it would stop broadcasting the BSM.

6. Potential Privacy Issues by Transaction Type

Based on our analysis of the privacy relevant data flows and controls discussed above, we identified five potential privacy scenarios for further research and/or consideration by the Agency. Table IV-1 below summarizes the scenarios and corresponding system transactions identified for further analysis.

Table IV-1 Transactions Identified for Further Analysis

Transaction Type	Description
BSM Broadcast Transaction	1. Can data elements, such as location, in the BSM be combined to form a temporary or persistent vehicle identifier
BSM Broadcast Transaction	2. Can data elements in the BSM be combined to identify vehicles temporarily so that different security certificates can be associated with the same vehicle during the vehicle's activities
BSM Broadcast Transaction	3. Do the physical characteristics of the carrier wave (i.e., the wave's fingerprint) associated with a vehicle's BSM serve as a vehicle identifier

Broadcast and Receipt of a Misbehavior Message	4. Do BSMs in misbehavior reporting provide sufficient information about the past location of the reporting or other vehicles to retrospectively track the vehicle's path?
Certificate Revocation List (CRL) Distribution Transaction	5. Does information regarding blacklisted vehicles' security certificates enable all vehicle security certificates to be associated with one another and thus, with the same specific vehicle?

As noted above, based on our exploration of privacy impacts and analysis of the V2V system design to date, it is NHTSA's expectation that the multiple technical, policy and physical controls incorporated into the design of the V2V system detailed will help to mitigate privacy risks to consumers. Methods of tracking vehicles, such as surveillance and use of specialized GPS devices already exist and may be easier, less expensive, and require less skill and access than would vehicle tracking using V2V messages or other information in the V2V system in certain conditions. Nevertheless, DOT is continuing to work with privacy experts to perform dynamic modeling and explore the viability of additional controls that might further mitigate any potential impacts demonstrated in the privacy-relevant transactions identified above for further analysis. The planned implementation by DOT of a PoC security entity (SCMS) and related PKI policy research will provide an operational environment in which to continue to explore the viability of additional privacy-mitigating controls applicable to the V2V System, as currently envisioned and designed. We seek comment on whether there are other potential privacy risks stemming from the V2V systems proposed that the agency should investigate and, if so, what specific risks.

E. Health effects

NHTSA received numerous comments from individuals in response to the ANPRM concerning the potential for V2V technology to contribute to electromagnetic hypersensitivity ("EHS"). Overall, the comments focused on how a national V2V deployment could potentially disadvantage persons that may be electro-sensitive.[190] In response, NHTSA engaged the DOT Volpe Center to review available literature and government agency actions regarding EHS in support of this NPRM. More specifically, NHTSA needed to learn more about the potential conditions causing EHS, actions taken by other federal agencies that have been involved in similar technology deployments or whose mission is primarily human health-focused, and any qualifying actions granted by the Americans with Disabilities Act (ADA) related to EHS among other potential externalities that may affect a potential V2V technology deployment.

[190] "Electromagnetic Hypersensitivity Comment Review and Analysis", NHTSA V2V Support – Task 3, dated March 13, 2015, Noblis.

1. Overview

According to the World Health Organization (WHO), EHS is characterized by a variety of non-specific symptoms that are attributed to exposure to electro-magnetic frequencies ("EMF") by those reporting symptoms. The symptoms most commonly experienced include dermatological symptoms (redness, tingling, and burning sensations) as well as neurasthenic and vegetative symptoms (fatigue, tiredness, difficulty concentrating, dizziness, nausea, heart palpitation, and digestive disturbances). The collection of symptoms is not part of any recognized syndrome. Reports have indicated that EHS can be a disabling problem for the affected individual; however, EHS has no clear diagnostic criteria and it appears there is no scientific basis to link EHS symptoms to EMF exposure. Further, EHS is not a medical diagnosis, nor is it clear that it represents a single medical problem.[191]

2. Wireless Devices and Health and Safety Concerns

The Federal Communications Commission (FCC), federal health and safety agencies such as the Environmental Protection Agency (EPA), the Food and Drug Administration (FDA), the National Institute for Occupational Safety and Health (NIOSH) and the Occupational Safety and Health Administration (OSHA) have been actively involved in monitoring and investigating issues related to radio frequency ("RF") exposure. Federal, state, and local government agencies and other organizations have generally relied on RF exposure standards developed by expert, non-government organizations such as the Institute of Electrical and Electronics Engineers (IEEE) and the National Council on Radiation Protection and Measurements (NCRP).

Several U.S. government agencies and international organizations are working cooperatively to monitor research on the health effects of RF exposure. The World Health Organization's (WHO) International Electromagnetic Fields Project (IEFP) provides information on health risks, establishes research needs, and supports efforts to harmonize RF exposure standards. Some health and safety interest groups have interpreted certain reports to suggest that wireless device use may be linked to cancer and other illnesses, posing potentially greater risks for children than adults. While these assertions have gained increased public attention, currently no scientific evidence establishes a causal link between wireless device use and cancer or other illnesses.[192]

---

[191] "Electromagnetic fields and public health: Backgrounder", The World Health Organization (WHO), December 2005. Available at http://www.who.int/peh-emf/publications/facts/fs296/en/ (last accessed Sept. 28, 2015).

[192] "Wireless Devices and Health Concerns", Federal Communications Commission (FCC), Consumer and Governmental Affairs Bureau, updated March 12, 2014. Available at http://www.fcc.gov/guides/wireless-devices-and-health-concerns (last accessed Dec 12, 2016).

3. Exposure Limits

In the U.S, IEEE has developed limits for human exposure to RF energy, and these limits have been widely influential around the world and require periodic updates. Internationally, the exposure limits for RF energy vary widely in different countries. A few countries have chosen lower limits, in part due to differences in philosophy in setting limits. IEEE and most other Western exposure limits are designed on the basis of identified thresholds for hazards of RF and thus are science-based. Switzerland, Italy, and a few other countries have adopted "precautionary" exposure limits for RF energy. These are not based on identified hazards, but reflect the desire to set exposure limits as low as economically and technically practical, to guard against the possibility of an as-yet unidentified hazard of RF exposure at low levels.[193]

4. U.S. Department of Energy (DOE) Smart Grid Implementation

Many comments to the ANPRM were related to the implementation and expansion of "smart grid" or "smart meter" technology being deployed in the United States. The "smart grid" generally refers to a class of technology used to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. These systems are made possible by two-way communication technology and computer processing that has been used for decades in other industries.[194]

Federal legislation was enacted in both 2005 (Energy Policy Act, or "EPAct") and 2007 (Energy Independence and Security Act, or "EISA") that contained major provisions on demand response, smart metering, and smart grids.[195] The primary purpose of using smart meters and grids is to improve energy efficiency – very precise electricity usage information can be transmitted back to the utility in real-time, enabling the utility to better direct how much electricity is transmitted, and when, which in turn can improve power generation efficiency by not producing more power than necessary at a given time. According to a report prepared by the Federal Energy Regulatory Commission (FERC) in December 2014, approximately 15.3 million advanced meters were installed and operational through the Department of Energy (DOE) Smart Grid Investment Grant (SGIG) program. Ultimately, 15.5 million advanced meters are expected

---

[193] "COMAR Technical Information Statement the IEEE exposure limits for radiofrequency and microwave energy", Marvin C. Ziskin, IEEE Engineering in Medicine and Biology Magazine, March/April, 2005. Available at http://ewh.ieee.org/soc/embs/comar/standardsTIS.pdf (last accessed Dec. 12, 2016).

[194] Department of Energy "Smart Grid" website. Available at http://energy.gov/oe/services/technology-development/smart-grid (last accessed Dec 12, 2016).

[195] "Demand Response & Smart Metering Policy Actions Since the Energy Policy Act of 2005 – A Summary for State Officials", Prepared by U.S. Demand Response Coordinating Committee for The National Council on Electricity Policy, 2008. http://energy.gov/oe/downloads/demand-response-and-smart-metering-policy-actions-energy-policy-act-2005-summary-state (last accessed: Dec 12, 2016)

to be installed and operational under SGIG. All SGIG projects are expected to reach completion in 2014, with continued reporting requirements through 2016.[196]

In the last several years, some consumers have objected to deployment of the "smart" utility meters needed for DOE's Smart Grid implementation. Smart meters transmit information via wireless technology using electromagnetic frequencies (EMF). Smart utility meters operate in the 902-928 MHz frequency band and the 2.4 GHz range, which is where the human body absorbs energy less efficiently and the Maximum Permissible Exposure (MPE) limits for RF exposure are less restrictive.[197]

Smart utility meters in households or businesses will generally transmit data to an access point (usually on utility poles) once every four hours for about 50 milliseconds at a time. Once the smart grid is fully active, it is expected that smart utility meters will transmit more frequently than once every four hours, resulting in a higher duty cycle.[198] A 2011 report from the California Council on Science and Technology (CCST) showed minimum and maximum exposure levels for various sources, including a smart meter that is always on at two distances from the body. The CCST concluded that RF exposure levels for smart meters in either scenario would be less than microwave ovens and considerably less than cell phones, but more than Wi-Fi routers or FM radio/TV broadcasts.[199] It should also be noted that a 2011 report from the Electric Power Research Institute (EPRI) assessed exposures in front of and behind smart utility meters. It determined that the average exposure levels from smart utility meters, measured from a single meter and from an array of meters, were at levels similar to those from other devices that produce RF in the home and surrounding environment.[200]

A typical "smart" utility meter device uses a low power one watt wireless radio to send customer energy-usage information wirelessly.[201] The V2V DSRC devices used for NHTSA

---

[196] "Assessment of Demand Response and Advanced Metering", Federal Energy Regulatory Commission (FERC) Report, December 2014. Available at https://www.ferc.gov/industries/electric/indus-act/demand-response/dem-res-adv-metering.asp (last accessed Dec 12, 2016).
[197] Federal Communications Commission, (FCC), 2011. Radio frequency safety, available at https://www.fcc.gov/encyclopedia/radio-frequency-safety (last accessed Dec 12, 2016).
[198] "Review of Health Issues Related to Smart Meters", Monterey County Health Department, Public Health Bureau, Epidemiology and Evaluation, March, 2011. Available at https://www.nema.org/Technical/Documents/Smart%20Meter%20Safety%20-%20Marin%20Co%20CA%20whitepaper.pdf (last accessed Dec 12, 2016).
[199] "Health Impacts of RF Exposure from Smart Meters", California Council on Science and Technology, April 2011. Available at https://ccst.us/publications/2011/2011smart-final.pdf (last accessed Dec 12, 2016).
[200] "RF Exposure Levels from Smart Meters: A Case Study of One Model", Electric Power Research Institute (EPRI), February 2011. Available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001022270 (last accessed Dec 12, 2016).
[201] Radio Frequency FAQ, http://www.pge.com/en/safety/systemworks/rf/faq/index.page (last accessed Jun. 5, 2015).

research in the Safety Pilot activities are allowed to transmit at up to 33 dBm[202] (approximately 2.0 watts of power output)., as defined by FCC specifications.[203] The "normal" operating transmission output range for these devices is 20 dBm (or approximately 100mW) for devices operating in the allocated DSRC frequency range. For additional comparison purposes, the typical cellular phone operates at higher power output levels of 27 dBm (approximately 500 mW). Cellular phones are capped at the same maximum transmission power output of 33 dBm.

The public objections to these deployments have been based on concerns over potential health effects. Specifically, some consumers are concerned about exposure to wireless RF emissions emanating from smart meters in their homes, which has led to legal challenges for smart meter programs. Due to these objections, several state commissions authorized an "opt-out" provision for individual consumers who do not wish to have smart meters installed in their homes. In response to public perception of the technology, the Department of Energy pursued development of outreach materials citing current scientific and industry evidence that radio frequency from smart grid devices in the home is not detrimental to health. The materials are being provided to state commissions, utilities in the DOE Smart Grid Program, and other community-based organizations in effort to convey these messages to the end-user community.[204]

5. Federal Agency Oversight & Responsibilities

Many consumer and industrial products use or produce some form of electromagnetic energy. Various agencies within the Federal Government have been involved in monitoring, researching, or regulating issues related to human exposure to radio frequency radiation. A summary of the federal Government's role is provided below:[205]

- **Federal Communications Commission (FCC):** The FCC authorizes and licenses most RF telecommunications services, facilities, and devices used by the public, industry, and state and local governmental agencies. The FCC's exposure guidelines that V2V devices

---

[202] dBm or decibel-milliwatt is an electrical power unit in decibels (dB), referenced to 1 milliwatt (mW). The power in decibel-milliwatts (P(dBm)) is equal to 10 times base 10 logarithm of the power in milliwatts (P(mW)).
[203] "Table I.5a—Maximum STA transmit power classification for the 5.85–5.925 GHz band in the United States", IEEE specification 802.11P -2010, Page 31. Available at https://www.ietf.org/mail-archive/web/its/current/pdfqf992dHy9x.pdf (last accessed Dec 12, 2016).
[204] Recommendations on Consumer Acceptance of Smart Grid, Electricity Advisory Committee, Richard Cowart, Chair to Honorable Patricia Hoffman, Assistant Secretary for Electricity Delivery and Energy Reliability, U. S. Department of Energy, June 6, 2013. http://energy.gov/sites/prod/files/2013/06/f1/EAC_SGConsumerRecs.pdf (last accessed Dec 12, 2016).
[205] "Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields", OET Bulletin 56, Fourth Edition, August 1999, Federal Communications Commission, Office of Engineering and Technology. Available at https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet56/oet56e4.pdf (last accessed Dec 12, 2016).

are anticipated to follow, and the ANSI/IEEE and NCRP guidelines upon which they are based, specify limits for human exposure to RF emission from hand-held RF devices in terms of specific absorption rate (SAR). Additionally, under the National Environmental Policy Act of 1969 (NEPA), the FCC has certain responsibilities to consider whether its actions will "significantly affect the quality of the human environment." To meet its NEPA obligations, the Commission has adopted requirements for evaluating the impact of its actions (47 CFR 1.1301, et. seq.). One of several environmental factors addressed by these requirements is human exposure to RF energy emitted by FCC-regulated transmitters and facilities. The FCC's rules provide a list of various Commission actions that may have a significant effect on the environment. If FCC approval to construct or operate a facility would likely result in a significant environmental effect, the applicant must submit an Environmental Assessment (EA). The EA is reviewed by FCC staff to determine whether an Environmental Impact Statement (EIS) is necessary.[206]

- **National Telecommunications and Information Administration:** NTIA is an agency of the U.S. Department of Commerce and is responsible for authorizing Federal Government use of the RF electromagnetic spectrum. Like the FCC, NTIA also has NEPA responsibilities and has enacted similar guidelines and processes to those of FCC to ensure compliance.
- **Food and Drug Administration (FDA):** by authority of the Radiation Control for Health and Safety Act of 1968, the FDA's Center for Devices and Radiological Health (CDRH) develops performance standards for the emission of radiation from electronic products including: X-ray equipment, other medical devices, television sets and microwave ovens, laser products, and sunlamps. The CDRH has not adopted performance standards for other RF-emitting products. The FDA is the leading federal health agency in monitoring the latest research developments and advising other agencies with respect to the safety of RF-emitting products used by the public, such as cellular and mobile devices.
- **Environmental Protection Agency (EPA):** EPA activities pertaining to RF safety and health are presently limited to advisory functions. EPA has chaired an Interagency Radiofrequency Working Group, which coordinates RF health-related activities among federal agencies who have regulatory responsibilities in this area.
- **Occupational Safety and Health Administration (OSHA):** OSHA is responsible for protecting workers from exposure to hazardous chemical and physical agents. In 1971, OSHA issued a protection guide, which V2V devices are anticipated to operate within, for exposure of workers to radiation (29 CFR 1910.97). The guide covers frequencies

[206] "Evaluating Compliance with FCC Guidelines for Human Exposure to Radio frequency Electromagnetic Fields", Federal Communications Commission, Office of Engineering & Technology, OET Bulletin 65 (Edition 97-01), August 1997. Available at https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet65/oet65b.pdf (last accessed Dec 12, 2016).

from 10 MHz to 100GHz. The guide was later ruled to be only advisory and not mandatory.[207]

- **National Institute for Occupational Safety and Health (NIOSH):** NIOSH is part of the U.S. Department of Health and Human Services, Centers for Disease Control and Prevention (CDC) and conducts research and investigations into issues related to occupational exposure to chemical and physical agents. NIOSH research is focused on radio frequencies, extremely low frequencies (ELF) and static magnetic fields. CDC/NIOSH provides various guidance documents related to the focused research areas.[208]
- **The Architectural and Transportation Barriers Compliance Board (Access Board):** The Access Board is the federal agency devoted to the accessibility for people with disabilities. In November 1999, the Access Board issued a proposed rule to revise and update their accessibility guidelines. During the public comment period on the proposed rule, the Access Board received approximately 600 comments from individuals with multiple chemical and electromagnetic sensitivities. The Board issued a statement recognizing that people with these sensitivities may be considered disabled under the ADA if conditions perceived to be caused by these sensitivities "so severely impair the neurological, respiratory, or other functions of an individual that it substantially limits one or more of the individual's major life activities." The Board contracted with the National Institute of Building Sciences (NIBS) to establish the Indoor Environmental Quality (IEQ) Project. The overall objectives of the IEQ project were to establish a collaborative process among a range of stakeholders to recommend practical, implementable actions to both improve access to buildings for people with EMS while also improving indoor environmental quality to create healthier buildings for the entire population. The NIBS IEQ Final Report was issued in July 2005 and provides recommendations for accommodations for people with chemical and/or electromagnetic sensitivities. The agency is unaware of any further actions by the Access Board on this issue.[209]
- **Department of Defense (DOD):** The DOD conducts research on the biological effects of RF energy.

---

[207] OET Bulletin #56, Federal Communications Commission, FCC, available at https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet56/oet56e3.pdf (last accessed Dec 12, 2016).

[208] "EMF (ELECTRIC AND MAGNETIC FIELDS)," available at http://www.cdc.gov/niosh/topics/emf/ (last accessed Dec 12, 2016).

[209] "IEQ Indoor Quality Final Report, National Institute for Building Services, July 14, 2005. http://apps.fcc.gov/ecfs/document/view?id=7520945309 (last accessed: Dec 12, 2016)

6. EHS in the US and abroad

a) Americans with Disabilities Act

The Americans with Disabilities Act ("ADA") does not contain a lengthy list of medical conditions that constitute disabilities. Instead, the ADA provides a general definition for "disability", which requires a showing of a having a physical or mental impairment that substantially limits one or more major life activities, a history or record of such an impairment, or being perceived by others as having such an impairment. Several states have enacted even more liberal policies on disability rights that afford greater potential protections than the ADA as it relates to EHS.

To date, the agency is unaware of any finding that EHS constitutes a disability. As mentioned above, the NIBS IEQ provided some recommendations, but did not conclude the EHS was in fact a disability. The agency is unaware of any further actions, either by the Access Board or some other entity, which recognized EHS as a disability or any science that would prove this.

b) Global recognition

Globally, some nations have heightened awareness of EHS by requiring provisions to accommodate those claiming its effects. In Sweden, for example, these provisions could include unique lighting fixtures and/or computer monitors for places of employment. The Canadian Government, The Canadian Human Rights Commission (CHRC) has also recognized EMS, describing environmental sensitivities as follows: "The term "environmental sensitivities" describes a variety of reactions to chemicals, electromagnetic radiation, and other environmental factors at exposure levels commonly tolerated by many people."[210] The CHRC published a series of recommendations for building environments in effort to reduce potential EMS conditions.[211] In 2009, the European Parliament urged member states to follow Sweden's example to provide people with ES protection and equal opportunities.

7. Conclusion

The agency appreciates the ANPRM comments bringing attention to V2V technology and a potential relationship to EHS. The agency takes these concerns very seriously. The literature review conducted by the agency highlighted long, and still ongoing, activities to better understand the relationship to electromagnetic radiation and the symptoms of individuals

---

[210] "What You Should Know About Electromagnetic Sensitivity (EMS)", Christiane Tourtet. B.A, International MCS/EMS Awareness, available at http://www.nettally.com/prusty/CTEMS.pdf (last accessed Dec. 8, 2016).

[211] Sears, Margaret E., "The Medical Perspective on Environmental Sensitivities," May 2007. Available at http://www.chrc-ccdp.ca/sites/default/files/envsensitivity_en_1.pdf. (last accessed Dec. 8, 2016).

reporting electromagnetic hypersensitivity. As a Federal government agency focused on automotive safety, NHTSA acknowledges the expertise of our sister agencies such as the Federal Communications Commission and the Food and Drug Administration, among others, which have been involved with electromagnetic fields, in parallel with the pervasiveness of cellular phone deployment in the United States and globally.

The FDA currently states in response to the question, "Is there a connection between certain health problems and exposure to radiofrequency fields via cell phone use?" that "The results of most studies conducted to date indicate that there is not. In addition, attempts to replicate and confirm the few studies that did show a connection have failed."[212] However, NHTSA acknowledges that research is still ongoing and, as technology evolves; wireless communications will most likely continue to increase. The agency believes the continued efforts of the Radiofrequency Interagency Work Group (RFIAWG)[213] may yield any potential future guidance for wireless device deployment and usage.

V2V devices are currently certified for use in the 5.9 GHz frequency allocation by the FCC, and the agency additionally anticipates any future certifications by the FCC will ensure that V2V devices will comply with all criteria related to RF emissions.

Currently, the FCC publishes a very helpful guide on "Wireless Devices and Health Concerns,"[214] in which the Commission states, "While there is no federally developed national standard for safe levels of exposure to radiofrequency (RF) energy, many federal agencies have addressed this important issue." The Commission acknowledges the efforts the interagency working group, its members, and their ongoing monitoring and investigating issues related to RF exposure.

V2V devices would operate at distances to humans significantly further that the distance relationship of a portable cellular phone to its operator, where the device is generally carried on a person or pressed directly to the ear. V2V devices used in the Safety Pilot operated at similar power levels to handheld cellular phones and the agency expects power levels for production deployment to remain consistent with the levels used in the Safety Pilot activities. Based on these two conditions, we believe it is reasonable to anticipate that any new guidance issued by the RFIAWG and its participating federal agencies on future cellular phone or wireless device usage could potentially be relevant to V2V devices, albeit in a somewhat diminished magnitude based on the distances the devices will operate in relation to persons.

---

[212] Radiation-Emitting Products, "Current Research Results," available at http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/HomeBusinessandEntertainment/CellPhones/ucm116335.htm (last accessed Dec. 8, 2016).
[213] Group members can be found at http://www.emrpolicy.org/litigation/case_law/docs/workgroupmemberslist.pdf (last accessed: Dec 8, 2016)
[214] See "Wireless Devices and Health Concerns" https://www.fcc.gov/guides/wireless-devices-and-health-concerns (last accessed Dec. 8, 2016).