



This document is scheduled to be published in the Federal Register on 04/01/2016 and available online at <http://federalregister.gov/a/2016-07353>, and on FDsys.gov

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

[Docket No. NHTSA-2016-0040]

Request for Public Comments on NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Emerging Automotive Technologies

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation.

ACTION: Request for public comments.

SUMMARY: Automotive technology is at a moment of rapid change and may evolve farther in the next decade than in the previous 45-plus year history of the Agency. As the world moves toward autonomous vehicles and innovative mobility solutions, NHTSA is interested in facilitating the rapid advance of technologies that will promote safety.

NHTSA is commanded by Congress to protect the safety of the driving public against unreasonable risks of harm that may occur because of the design, construction, or performance of a motor vehicle or motor vehicle equipment, and mitigate risks of harm, including risks that may be emerging or contingent. As NHTSA always has done when evaluating new technologies and solutions, we will be guided by our statutory mission, the laws we are obligated to enforce, and the benefits of the emerging technologies appearing on America's roadways.

NHTSA has broad enforcement authority, under existing statutes and regulations, to address existing and emerging automotive technologies. This proposed Enforcement Guidance Bulletin sets forth NHTSA's current views on emerging automotive technologies – including its view that when vulnerabilities of such technology or

equipment pose an unreasonable risk to safety, those vulnerabilities constitute a safety-related defect – and suggests guiding principles and best practices for motor vehicle and equipment manufacturers in this context. This notice solicits comments from the public, motor vehicle and equipment manufacturers, and other interested parties concerning the proposed guidance for motor vehicle and equipment manufacturers in developing and implementing new and emerging automotive technologies, safety compliance programs, and other business practices in connection with such technologies.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments by any of the following methods:

- Internet: Go to *http://www.regulations.gov* and follow the online instructions for submitting comments.
- Mail: Docket Management Facility, M-30, U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building, Room W12-140, Washington, DC 20590.
- Hand Delivery or Courier: U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building, Room W12-140, Washington, DC 20590 between 9 a.m. and 5 p.m. Eastern Time, Monday through Friday, except Federal holidays.
- Facsimile: (202) 493-2251.

Regardless of how you submit your comments, please mention the docket number of this document.

You may also call the Docket at (202) 366-9322.

Instructions: All comments received must include the Agency name and docket ID.

Please submit your comments by only one means. Regardless of the method used for

submitting comments, all submissions will be posted without change to <http://www.regulations.gov>, including any personal information provided. Thus, submitting such information makes it public. You may wish to read the Privacy Act notice, which can be viewed by clicking on the “Privacy and Security Notice” link in the footer of <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: Justine Casselle, Office of the Chief Counsel, National Highway Traffic Safety Administration, or Elizabeth Mykytiuk, Office of the Chief Counsel, National Highway Traffic Safety Administration, at (202) 366-2992.

SUPPLEMENTARY INFORMATION:

- I. Executive Summary
- II. Legal and Policy Background
 - A. NHTSA’s Enforcement Authority Under the Safety Act
 - B. Determining the Existence of a Defect
 - C. Determining an Unreasonable Risk to Safety
- III. Guidance and Recommended Best Practices: Safety-Related Defects, Unreasonable Risk, and Emerging Technologies

I. Executive Summary

Recent and continuing advances in automotive technology have great potential to generate significant safety benefits. Today’s motor vehicles are increasingly equipped with electronics, sensors, and computing power that enable the deployment of safety technologies and functions, such as forward-collision warning, automatic-emergency braking, and lane keeping assist, which dramatically enhance safety. New technologies may not only prevent drivers from crashing, but may even do some or all of the driving for them. The safety implications of such emerging technologies are vast. Importantly, as these technologies become more widespread, manufacturers must ensure their safe

development and implementation.

To facilitate automotive safety innovation, to aid in the successful development and deployment of emerging automotive technologies, and to protect the public from potential flaws or threats associated with emerging automotive technologies, NHTSA is publishing, for guidance and informational purposes, this Enforcement Guidance Bulletin setting forth the Agency's current view of its enforcement authority and principles guiding its exercise of that authority. This includes guiding principles and best practices for use by motor vehicle and equipment manufacturers. NHTSA is not establishing a binding set of rules, nor is the Agency suggesting that one particular set of practices applies in all situations. The Agency recognizes that best practices vary depending on circumstances, and manufacturers remain free to choose the solution that best fits their needs and the demands of automotive safety. However, to address safety concerns associated with emerging technologies in a comprehensive way, and to advise regulated entities of the Agency's present views of certain enforcement subjects and issues, NHTSA submits this proposed Enforcement Guidance Bulletin for public comment. Based on the Agency's review and analysis of that input, it will develop and issue a final "Enforcement Guidance Bulletin" on this topic.

II. Legal and Policy Background

A. NHTSA's Enforcement Authority Under the Safety Act

The National Traffic and Motor Vehicle Safety Act, as amended ("Safety Act"), 49 U.S.C. 30101 et seq., provides the basis and framework for NHTSA's enforcement authority over motor vehicle and motor vehicle equipment defects and noncompliances with federal motor vehicle safety standards (FMVSS). This authority includes

investigations, administrative proceedings, civil penalties, and civil enforcement actions. While automation and other advanced technologies may modify motor vehicle and equipment design, NHTSA’s statutory enforcement authority is general and flexible, which allows it to keep pace with innovation. The Agency has the authority to respond to a safety problem posed by new technologies in the same manner it has responded to safety problems posed by more established automotive technology and equipment, such as carburetors, the powertrain, vehicle control systems, and forward collision warning systems – by determining the existence of a defect that poses an unreasonable risk to motor vehicle safety and ordering the manufacturer to conduct a recall. *See* 49 U.S.C. § 30118(b). This enforcement authority applies notwithstanding the presence or absence of an FMVSS for any particular type of advanced technology. *See, e.g., United States v. Chrysler Corp.*, 158 F.3d 1350, 1351 (D.C. Cir. 1998) (NHTSA “may seek the recall of a motor vehicle either when a vehicle has ‘a defect related to motor vehicle safety’ or when a vehicle ‘does not comply with an applicable motor vehicle safety standard.’”).¹

Under the Safety Act, NHTSA has authority over motor vehicles, equipment included in or on a motor vehicle at the time of delivery to the first purchaser (i.e., original equipment), and motor vehicle replacement equipment. *See* 49 U.S.C. § 30102(a)-(b). Motor vehicle equipment is broadly defined to include “any system, part, or component of a motor vehicle as originally manufactured” and “any similar part or component manufactured or sold for replacement or improvement of a system, part, or component.” 49 U.S.C. 30102(a)(7)(A)-(B). The Safety Act also gives NHTSA jurisdiction over after-market improvements, accessories, or additions to motor vehicles.

¹ A manufacturer’s obligation to recall motor vehicles and motor vehicle equipment determined to have a safety-related defect is separate and distinct from its obligation to recall motor vehicles and motor vehicle equipment that fail to comply with an applicable FMVSS. *See* 49 U.S.C. 30120.

See 49 U.S.C. 30102(a)(7)(B). All devices “manufactured, sold, delivered, or offered to be sold for use on public streets, roads, and highways with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death” are similarly subject to NHTSA’s enforcement authority. 49 U.S.C. 30102(a)(7)(C).

With respect to new and emerging technologies, NHTSA considers automated vehicle technologies, systems, and equipment to be motor vehicle equipment, whether they are offered to the public as part of a new motor vehicle (as original equipment) or as an after-market replacement(s) of or improvement(s) to original equipment. NHTSA also considers software (including, but not necessarily limited to, the programs, instructions, code, and data used to operate computers and related devices), and after-market software updates, to be motor vehicle equipment within the meaning of the Safety Act. Software that enables devices not located in or on the motor vehicle to connect to the motor vehicle or its systems could, in some circumstances, also be considered motor vehicle equipment. Accordingly, a manufacturer of new and emerging vehicle technologies and equipment, whether it is the supplier of the equipment or the manufacturer of a motor vehicle on which the equipment is installed, has an obligation to notify NHTSA of any and all safety-related defects. *See* 49 CFR part 573. Any manufacturer or supplier that fails to do so may be subject to civil penalties. *See* 49 U.S.C. 30165(a).

NHTSA is charged with reducing deaths, injuries, and economic losses resulting from motor vehicle crashes. *See* 49 U.S.C. 30101. Part of that mandate includes ensuring that motor vehicles and motor vehicle equipment, including new technologies, perform in ways that “protect[] the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable

risk of death or injury in an accident.” 49 U.S.C. 30102(a)(8). This responsibility also includes the nonoperational safety of a motor vehicle. *Id.* In pursuit of these safety objectives, and in the absence of adequate action by the manufacturer, NHTSA is authorized to determine that a motor vehicle or motor vehicle equipment is defective and that the defect poses an unreasonable risk to safety. *See* 49 U.S.C. 30118(b) and (c)(1).

B. Determining the Existence of a Defect

Under the Safety Act, a “defect” includes “any defect in performance, construction, a component, or material of a motor vehicle or motor vehicle equipment.” 49 U.S.C. 30102(a)(2). It also includes a defect in design. *See United States v. General Motors Corp.*, 518 F.2d 420, 436 (D.C. Cir. 1975) (“*Wheels*”). A defect in an item of motor vehicle equipment (including hardware, software and other electronic systems) may be considered a defect of the motor vehicle itself. *See* 49 U.S.C. 30102(b)(1)(F).

Congress intended the Safety Act to represent a “commonsense” approach to safety and courts have followed that approach in determining what constitutes a “defect.” *Wheels*, 518 F.2d at 436. *Accord Center for Auto Safety, Inc. v. National Highway Traffic Safety Administration*, 342 F. Supp. 2d 1, 15 (D.D.C. 2004); *Clarke v. TRW, Inc.*, 921 F. Supp. 927, 934 (N.D.N.Y. 1996). For this reason, a defect determination does not require an engineering explanation or root cause, but instead “may be based exclusively on the performance record of the component.” *Wheels*, 518 F.2d at 432 (“[A] determination of a ‘defect’ does not require any predicate of a finding identifying engineering, metallurgical, or manufacturing failures.”). Thus, a motor vehicle or item of equipment contains a defect if it is subject to a significant number of failures in normal operation, “including those failures occurring during ‘specified use’ or resulting from predictable abuse, but not

including those resulting from normal deterioration due to age and wear.”² *Center for Auto Safety*, 342 F.2d at 13-14 (citing *Wheels*, 518 F.2d at 427).

A “significant number of failures” is merely a “non-de minimus” quantity; it need not be a “substantial percentage of the total.” *Wheels*, 518 F.2d at 438 n.84. Whether there have been a “significant number of failures” is a fact-specific inquiry that includes considerations such as: the failure rate of the component in question; the failure rates of comparable components; and the importance of the component to the safe operation of the vehicle. *Id.* at 427. In addition, where appropriate, the determination of the existence of a defect may depend upon the failure rate in the affected class of vehicles compared to that of other peer vehicles. *See United States v. Gen. Motors Corp.*, 841 F.2d 400, 412 (D.C. Cir.1988) (“X-Cars”). Finally, to constitute a defect, the failures must be attributable to the motor vehicle or equipment itself, rather than the driver or the road conditions. *See id.*

It must be noted, however, that in some circumstances, a crash, injury, or death need not occur in order for a vulnerability or safety risk to be considered a defect. The Agency relies on the performance record of a vehicle or component in making a defect determination where the engineering or root cause is unknown. *See Wheels*, 518 F.2d at 432. Where, however, the engineering or root cause is known, the Agency need not proceed with analyzing the performance record. *See id.*; *see also United States v. Gen. Motors Corp.*, 565 F.2d 754, 758 (D.C. Cir. 1977) (“Carburetors”) (finding a defect to be safety-related if it “results in hazards as potentially dangerous as sudden engine fire, and

² “The protection afforded by the [Safety] Act was not limited to careful drivers who fastidiously observed speed limits and conscientiously complied with manufacturer’s instructions on vehicle maintenance and operation. . . . [the statute provides] an added area of safety to an owner who is lackadaisical, who neglects regular maintenance . . .” *Wheels*, 518 F.2d at 434.

where there is no dispute that at least some such hazards ... can definitely be expected to occur in the future.”). For software or other electronic systems, for example, when the engineering or root cause of the vulnerability or risk is known, a defect exists regardless of whether there have been any actual failures.

C. Determining an Unreasonable Risk to Safety

In order to support a recall, a defect must be related to motor vehicle safety. *United States v. General Motors Corp.*, 561 F.2d 923, 928-29 (D.C. Cir. 1977) (“*Pitman Arms*”). In the context of the Safety Act, “motor vehicle safety” refers to an “unreasonable risk of accidents” and an “unreasonable risk of death or injury in an accident.” 49 U.S.C. § 30102(a)(8). Thus, while the defect analysis has generally entailed a retrospective look at how many failures have occurred (*see Wheels, Center for Auto Safety*, and *Pitman Arms*), the safety-relatedness question is forward-looking, and concerns the hazards that may arise in the future. *See, e.g., Carburetors*, 565 F.2d at 758.

In general, for a defect to present an “unreasonable risk,” there must be a likelihood that it will cause or be associated with a “non-negligible” number of crashes, injuries, or deaths in the future. *See, e.g., Carburetors*, 565 F.2d at 759. This prediction of future hazards is called a “risk analysis.” *See, e.g., Pitman Arms*, 561 F.2d at 924 (Leventhal, J., dissenting) (“GM presented a ‘risk analysis’ which predicts the likely number of future injuries or deaths to be expected in the remaining service life of the affected models”). A forward-looking risk analysis is compelled by the purpose of the Safety Act, which “is not to protect individuals from the risks associated with defective vehicles only after serious injuries have already occurred; it is to prevent serious injuries stemming from established defects *before* they occur.” *Carburetors*, 565 F.2d at 759

(emphasis added).

If the hazard is sufficiently serious, and at least some harm, however small, is expected to occur in the future, the risk may be deemed unreasonable. *Carburetors*, 565 F.2d at 759 (“In the context of this case . . . even an ‘exceedingly small’ number of injuries from this admittedly defective and clearly dangerous carburetor appears to us ‘unreasonably large.’”). In other words, where a defect presents a “clearly” or “potentially dangerous” hazard, and where “at least some such hazards” – even an “exceedingly small” number – will occur in the future, that defect is necessarily safety-related. *See Carburetors*, 565 F.2d 754. This is so regardless of whether any injuries have already occurred, or whether the projected number of failures/injuries in the future is trending down. *See id.* at 759. Moreover, a defect may be considered “per se” safety-related if it causes the failure of a critical component; causes a vehicle fire; causes a loss of vehicle control; or suddenly moves the driver away from steering, accelerator, and brake controls – regardless of how many injuries or accidents are likely to occur in the future. *See Carburetors*, 565 F.2d 754 (engine fires); *Pitman Arms*, 561 F.2d 923 (loss of control); *United States v. Ford Motor Co.*, 453 F. Supp. 1240 (D.D.C. 1978) (“Wipers”) (loss of visibility); *United States v. Ford Motor Co.*, 421 F. Supp. 1239, 1243-1244 (D.D.C. 1976) (“Seatbacks”) (loss of control). Similarly, where it is alleged that a defect “is systematic and is prevalent in a particular class [of motor vehicles or equipment], . . . this is prima facie an unreasonable risk.” *Pitman Arms*, 561 F.2d at 929.

III. Guidance and Recommended Best Practices: Safety-Related Defects, Unreasonable Risk, and Emerging Technologies

Consistent with the foregoing background, NHTSA’s enforcement authority concerning safety-related defects in motor vehicles and equipment extends and applies

equally to new and emerging automotive technologies. This includes, for example, automation technology and equipment, as well as advanced crash avoidance technologies. Where an autonomous vehicle or other emerging automotive technology causes crashes or injuries, or has a manifested safety-related failure or defect, and a manufacturer fails to act, NHTSA will exercise its enforcement authority to the fullest extent. Similarly, should the Agency determine that an autonomous vehicle or other new automotive technology presents a safety concern, the Agency will evaluate such technology through its investigative authority to determine whether the technology presents an unreasonable risk to safety.

To avoid violating Safety Act requirements and standards, manufacturers of emerging technology and the motor vehicles on which such technology is installed are strongly encouraged to take steps to proactively identify and resolve safety concerns before their products are available for use on public roadways. The Agency recognizes that much emerging automotive technology heavily involves electronic systems (such as hardware, software, sensors, global positioning systems (GPS) and vehicle-to-vehicle (V2V) safety communications systems). The Agency acknowledges that the increased use of electronic systems in motor vehicles and equipment may raise new and different safety concerns. However, the complexities of these systems do not diminish manufacturers' duties under the Safety Act – both motor vehicle manufacturers and equipment manufacturers remain responsible for ensuring that their vehicles or equipment are free of safety-related defects or noncompliances, and do not otherwise pose an unreasonable risk to safety. Manufacturers are also reminded that they remain responsible for promptly reporting to NHTSA any safety-related defects or

noncompliances, as well as timely notifying owners and dealers of the same.

In assessing whether a motor vehicle or piece of motor vehicle equipment poses an unreasonable risk to safety, NHTSA considers the likelihood of the occurrence of a harm (i.e., fire, stalling, or malicious cybersecurity attack), the potential frequency of a harm, the severity of a harm, known engineering or root cause, and other relevant factors. Where a threatened harm is substantial, low potential frequency may not carry as much weight in NHTSA's analysis.

Software installed in or on a motor vehicle – which is motor vehicle equipment – presents its own unique safety risks. Because software often interacts with a motor vehicle's critical safety systems (i.e., systems encompassing critical control functions such as braking, steering, or acceleration) the operation of those systems could be substantially altered by after-market software updates. Additionally, software located outside the motor vehicle (i.e., portable devices with vehicle-related software applications) could be used to affect and control a motor vehicle's safety systems. If software has manifested a safety-related performance failure, or otherwise presents an unreasonable risk to safety, then the software failure or safety-risk constitutes a defect compelling a recall.

In the case of cybersecurity vulnerabilities, NHTSA will weigh several factors in determining whether a vulnerability poses an unreasonable risk to safety (and thus constitutes a safety-related defect), including: (i) the amount of time elapsed since the vulnerability was discovered (e.g., less than one day, three months, or more than six months); (ii) the level of expertise needed to exploit the vulnerability (e.g., whether a layman can exploit the vulnerability or whether it takes experts to do so); (iii) the

accessibility of knowledge of the underlying system (e.g., whether how the system works is public knowledge or whether it is sensitive and restricted); (iv) the necessary window of opportunity to exploit the vulnerability (e.g., an unlimited window or a very narrow window); and, (v) the level of equipment needed to exploit the vulnerability (e.g., standard or highly specialized).

NHTSA uses those factors, and others, to help assess the overall probability of a malicious cybersecurity attack. The probability of an attack includes circumstances in which a vulnerability has been identified, but no actual incidents have been documented or confirmed. Confirmed field incidents may increase the weight NHTSA places on the probability of an attack in its assessment. Even before evidence of an attack, it is foreseeable that hackers will try to exploit cybersecurity vulnerabilities. For instance, if a cybersecurity vulnerability in any of a motor vehicle's entry points (e.g., Wi-Fi, infotainment systems, the OBD-II port) allows remote access to a motor vehicle's critical safety systems (i.e., systems encompassing critical control functions such as braking, steering, or acceleration), NHTSA may consider such a vulnerability to be a safety-related defect compelling a recall.

Manufacturers should consider adopting a life-cycle approach to safety risks when developing automated vehicles, other innovative automotive technologies, and safety compliance programs and other business practices in connection with such technologies. A life-cycle approach would include "elements of assessment, design, implementation, and operations as well as an effective testing and certification program." National Highway Traffic Safety Administration, *A Summary of Cybersecurity Best Practices*, (Oct. 2014),

http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812075_CybersecurityBestPractices.pdf. Considering hardware, software, and network and cloud security, manufacturers should consider developing a simulator, using case scenarios and threat modeling on all systems, sub-systems, and devices, to test for safety risks, including cybersecurity vulnerabilities, at all steps in the manufacturing process for the entire supply chain, to implement an effective risk mitigation plan. *See id.*

Manufacturers of emerging technologies and the motor vehicles on which such technology is installed have a continuing obligation to proactively identify safety concerns and mitigate the risks of harm. If a manufacturer discovers or is otherwise made aware of any defects, noncompliances, or other unreasonable risks to safety after the vehicle and/or technology has been in safe operation for some time, then it should strongly consider promptly contacting the appropriate NHTSA personnel to determine the necessary next steps. Where a manufacturer fails to adequately address a safety concern, NHTSA, when appropriate, will explicitly address that concern through its enforcement authority.

APPLICABILITY/LEGAL STATEMENT: This proposed Enforcement Guidance Bulletin sets forth NHTSA's current views on the topic of emerging automotive technology and suggests guiding principles and best practices to be utilized by motor vehicle and equipment manufacturers in this context. This proposed Bulletin is not a final agency action and is intended as guidance only. This proposed Bulletin does not have the force or effect of law. This Bulletin is not intended, nor can it be relied upon, to create any rights enforceable by any party against NHTSA, the U.S. Department of Transportation, or the United States. These recommended practices do not establish any

defense to any violations of the Safety Act, or regulations thereunder, or violation of any statutes or regulations that NHTSA administers. This Bulletin may be revised in writing without notice to reflect changes in the Agency's views and analysis, or to clarify and update text.

Authority: 49 U.S.C. 30101-30103, 30116-30121, 30166; delegation of authority at 49 CFR 1.95 and 49 CFR 501.8.

Issued in Washington, D.C. on March 25, 2016 under authority delegated pursuant to 49 CFR 1.95.

Paul A. Hemmersbaugh
Chief Counsel

BILLING CODE: 4910-59-P
[FR Doc. 2016-07353 Filed: 3/29/2016 4:15 pm; Publication Date: 4/1/2016]