



November 28, 2016

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

Submitted via [www.regulations.gov](http://www.regulations.gov).

**Comments of Consumer Reports and Consumers Union to the  
National Highway Traffic Safety Administration on the  
Request for Comment on Cybersecurity Best Practices for Modern Vehicles  
Docket No. NHTSA-2016-0104**

Consumer Reports and Consumers Union welcome the opportunity to comment on the Cybersecurity Best Practices for Modern Vehicles document developed by the National Highway Traffic Safety Administration (NHTSA).<sup>1</sup> The protection of vehicle cybersecurity is a critical element of motor vehicle safety, particularly as cars come to rely on electronics and software-based systems. We appreciate NHTSA's attention to this topic, including through its safety research and its push for the creation of the Automotive Information Sharing and Analysis Center (Auto ISAC),<sup>2</sup> its recall work,<sup>3</sup> and the completion of this document.

While we agree with most of NHTSA's recommendations to industry in the Best Practices, vehicle cybersecurity is too important to be left to voluntary measures. We urge NHTSA to develop a mandatory safety standard for cybersecurity based on sufficient public research and consultation with other federal agencies, and to require full reporting of cybersecurity considerations and vulnerabilities in the interim. Through these steps, NHTSA would ensure that companies put the safety and security of consumers first. The agency should be supported in this endeavor by Congress, which should provide NHTSA with adequate

---

<sup>1</sup> Consumers Union is the policy and mobilization arm of Consumer Reports, an independent, nonprofit organization that works side by side with consumers to create a fairer, safer, and healthier world. As the world's largest independent product-testing organization, Consumer Reports uses its more than 50 labs, auto test center, and survey research center to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

<sup>2</sup> See, e.g., National Highway Traffic Safety Administration, *NHTSA and Vehicle Cybersecurity* (2016) (online at [www.nhtsa.gov/staticfiles/administration/pdf/presentations\\_speeches/2016/NHTSAVehicleCybersecurity2016.pdf](http://www.nhtsa.gov/staticfiles/administration/pdf/presentations_speeches/2016/NHTSAVehicleCybersecurity2016.pdf)).

<sup>3</sup> NHTSA Recall Campaign 15V461000 (July 23, 2015) (online at [www-odi.nhtsa.dot.gov/owners/SearchResults?searchType=ID&targetCategory=R&searchCriteria.nhtsa\\_ids=15V461000](http://www-odi.nhtsa.dot.gov/owners/SearchResults?searchType=ID&targetCategory=R&searchCriteria.nhtsa_ids=15V461000)).

resources to carry out its important work and pass clarifying legislation, if needed, to confirm the agency's authority.<sup>4</sup>

Motor vehicles are increasingly networked, with today's cars having upward of 70 to 100 electronic control units and potentially containing as much as 100 million lines of software code—significantly more than a new passenger airplane.<sup>5</sup> On multiple occasions, Consumer Reports has covered vehicle privacy and cybersecurity issues, warned of their associated risks, and pressed for stronger federal protections.<sup>6</sup> In May 2015, at NHTSA's invitation, we visited the facility in which the agency's engineers research cybersecurity vulnerabilities to better understand how to protect vehicles.<sup>7</sup> We have explored potential threats to consumers' personal information related to dedicated short-range communications, and called for baseline, enforceable privacy and cybersecurity standards relating to these communications.<sup>8</sup> This experience leads us to conclude that cars can have major cybersecurity vulnerabilities just as a computer or a mobile device can—but unlike many connected products, a breach of safety-critical vehicle systems can have life-or-death consequences.

Given the seriousness of vehicle cybersecurity risks,<sup>9</sup> it should be an urgent priority of NHTSA's to propose binding minimum cybersecurity standards for manufacturers, in addition to the separate voluntary Best Practices that are the subject of these comments.<sup>10</sup> We agree with

---

<sup>4</sup> See "Short-staffed NHTSA struggles to handle car-hacking threats," AutoBlog (Oct. 2, 2015) (online at [www.autoblog.com/2015/10/02/short-staffed-nhtsa-struggles-to-handle-car-hacking-threats](http://www.autoblog.com/2015/10/02/short-staffed-nhtsa-struggles-to-handle-car-hacking-threats)); see also, e.g., Sen. Edward J. Markey and Sen. Richard Blumenthal, "Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & 'Cyber Dashboard' Rating System," press release (July 21, 2015) (online at [www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system](http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system)).

<sup>5</sup> Government Accountability Office, "Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-World Attack" at 7-8 (Mar. 2016) (online at [www.gao.gov/assets/680/676064.pdf](http://www.gao.gov/assets/680/676064.pdf)).

<sup>6</sup> See, e.g., "Can your car get hacked?" Consumer Reports (Apr. 30, 2015) (online at [www.consumerreports.org/cro/magazine/2015/06/can-your-car-get-hacked/index.htm](http://www.consumerreports.org/cro/magazine/2015/06/can-your-car-get-hacked/index.htm)); "What It's Like To Be Inside A Car When Hackers Take Control From Miles Away," Consumerist (July 21, 2015) (online at [consumerist.com/2015/07/21/what-its-like-to-be-inside-a-car-when-hackers-take-control-from-miles-away](http://consumerist.com/2015/07/21/what-its-like-to-be-inside-a-car-when-hackers-take-control-from-miles-away)); "Fiat Chrysler Recalling 1.4M Vehicles Amid Concerns Over Remote Hack Attacks," Consumerist (July 24, 2015) (online at [consumerist.com/2015/07/24/fiat-chrysler-recalling-1-4m-vehicles-amid-concern-over-remote-hack-attacks](http://consumerist.com/2015/07/24/fiat-chrysler-recalling-1-4m-vehicles-amid-concern-over-remote-hack-attacks)).

<sup>7</sup> "Keeping your car safe from hacking," Consumer Reports (May 7, 2015) (online at [www.consumerreports.org/cro/news/2015/05/keeping-your-car-safe-from-hacking/index.htm](http://www.consumerreports.org/cro/news/2015/05/keeping-your-car-safe-from-hacking/index.htm)).

<sup>8</sup> Consumers Union, "Consumer and Auto Safety Groups Call for Non-Commercial Use of the Auto-Safety Spectrum and Strong Privacy and Security Protections" (Aug. 24, 2016) (online at [consumersunion.org/news/consumer-and-auto-safety-groups-call-for-non-commercial-use-of-the-auto-safety-spectrum-and-strong-privacy-and-security-protections](http://consumersunion.org/news/consumer-and-auto-safety-groups-call-for-non-commercial-use-of-the-auto-safety-spectrum-and-strong-privacy-and-security-protections)).

<sup>9</sup> See, e.g., *Id.* at 12-19; Federal Bureau of Investigation, Department of Transportation, and NHTSA, "Motor Vehicles Increasingly Vulnerable to Remote Exploits" (Mar. 17, 2016) (online at [www.ic3.gov/media/2016/160317.aspx](http://www.ic3.gov/media/2016/160317.aspx)); Staff of U.S. Sen. Edward J. Markey, *Tracking & Hacking: Security and Privacy Gaps Put American Drivers at Risk* (Feb. 9, 2015) (online at [www.markey.senate.gov/imo/media/doc/2015-02-06\\_MarkeyReport-Tracking\\_Hacking\\_CarSecurity%202.pdf](http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf)); "One in Five Vehicle Vulnerabilities are 'Hair on Fire' Critical," Security Ledger (Aug. 11, 2016) (online at [securityledger.com/2016/08/one-in-five-vehicle-vulnerabilities-are-hair-on-fire-critical](http://securityledger.com/2016/08/one-in-five-vehicle-vulnerabilities-are-hair-on-fire-critical)).

<sup>10</sup> NHTSA, "Cybersecurity Best Practices for Modern Vehicles" (Oct. 24, 2016) (online at [www.nhtsa.gov/staticfiles/nvs/pdf/812333\\_CybersecurityForModernVehicles.pdf](http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf)).

Administrator Rosekind when he said in January 2016 that 100% adoption across the industry is needed for safety-critical issues, and that “that’s where you need regulation.”<sup>11</sup>

More recently, however, NHTSA indicated in the Federal Automated Vehicles Policy guidance that it considers more research to be required before proposing a regulatory standard.<sup>12</sup> We disagree. Given the abundant work that has already taken place in the private sector, at the National Institute for Standards and Technology (NIST), and at NHTSA itself, NHTSA is well-positioned to at least issue an advance notice of proposed rulemaking as soon as practicable. The agency could conduct any additional research it may need to undertake as the proposal moves through the regulatory process and the agency receives public input. In the interim, the agency should take an active role in not just encouraging, but requiring, that companies take cybersecurity seriously by reporting cybersecurity considerations and vulnerabilities to both NHTSA and others in the industry.

As NHTSA pursues a rulemaking on cybersecurity, we urge the agency to also take into account the following recommendations and other considerations directly related to the Best Practices guidance it has produced:

**NHTSA should require rigorous and independent third-party auditing in addition to companies’ self-audits.** While it is important for companies to do their own self-audits—and the components that NHTSA recommends for these audits are generally appropriate—these are insufficient to ensure that a vehicle’s cybersecurity protections are strong enough. We urge NHTSA to require rigorous and independent third-party risk assessments, penetration tests, and review of organizational decisions. This step would help to ensure that a car’s systems are evaluated by entities without a financial self-interest in the conclusion.

**Cybersecurity researchers should have broad access to incident and risk data.** We are concerned that companies will be reluctant to allow external cybersecurity researchers adequate access to data. These external experts—who may have a perspective and expertise that a company lacks—are an important resource for identifying and addressing cybersecurity risks. NHTSA should go beyond simply encouraging companies to establish a policy for interacting with external researchers. The agency should clearly indicate its detailed expectations for companies’ interactions with external researchers and consider writing rules that require an appropriate degree of researcher access.

**Information sharing is critical.** The Best Practices rightly encourage companies to give data to the Auto ISAC in order to share cybersecurity incident and risk data with other companies in as close to real time as possible. NHTSA’s proposal for a vulnerability reporting/disclosure program going beyond the Auto ISAC is promising, and we urge the agency to take an active role in pushing companies to establish and participate in such a program. We also urge NHTSA to take all necessary steps to ensure that it receives the information it needs to reliably assess the safety of a vehicle with regard to potential cybersecurity issues.

---

<sup>11</sup> “NHTSA chief vows action this year on cybersecurity,” *Automotive News* (Jan. 19, 2016) (online at [www.autonews.com/article/20160119/OEM06/160119727/nhtsa-chief-vows-action-this-year-on-cybersecurity](http://www.autonews.com/article/20160119/OEM06/160119727/nhtsa-chief-vows-action-this-year-on-cybersecurity)).

<sup>12</sup> National Highway Traffic Safety Administration (NHTSA), *Federal Automated Vehicles Policy* at 21 (Sept. 20, 2016) (online at [www.nhtsa.gov/nhtsa/av/pdf/Federal\\_Automated\\_Vehicles\\_Policy.pdf](http://www.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf)).

**We strongly support NHTSA’s proposed Fundamental Vehicle Cybersecurity Protections, including the use of encryption, and urge all companies to implement them.**

Overall, the fundamental protections that NHTSA identifies represent useful building blocks for the rulemaking that we urge NHTSA to initiate. We especially support NHTSA’s recommendation for companies to use encryption to prevent the unauthorized recovery and analysis of firmware, as well as to prevent the breach of communications between external servers and the vehicle. In addition, we strongly agree with NHTSA that companies should limit the use of network servers on vehicle electronic control units to essential functionality, in the interest of reducing potential attack vectors. We also agree that it is critical for companies to log cybersecurity events in a way that maintenance personnel can detect trends. These logs should be accessible by any qualified maintenance personnel, not just those who work for the company that designed or manufactured the vehicle or system. Finally, while it is important for companies to restrict the ability to modify firmware in unsafe ways, we urge NHTSA to at a minimum ensure that consumers can receive reliable and timely information about modifications that occur and can check on the frequency with which their car’s firmware is being updated.

**The Best Practices should include stronger guidance on information privacy.**

NHTSA should address issues such as de-identification and data minimization, and encourage limits on the retention of consumers’ personal information. We urge the agency to base its views of appropriate privacy protection, as well as the definition of “personal data,” on stronger measures than the White House Consumer Privacy Bill of Rights. We have serious concerns with this proposal, including that it: (1) does not adequately define what constitutes sensitive information, or provide consumers with meaningful choices about their data; (2) does not explicitly protect large categories of personal information, such as geolocation data, business records, and data “generally available to the public”; (3) gives companies broad leeway to determine the protections that consumers will receive; and (4) generally offers protections to consumers only if a company identifies a risk of harm, according to its own judgment.<sup>13</sup>

**We support the broad scope of the Best Practices.** The broad applicability of the Best Practices—to all individuals and organizations manufacturing and designing vehicle systems and software, not just motor vehicle and equipment manufacturers—is appropriate. Preventing cybersecurity breaches that could harm motor vehicle safety in networked vehicles requires diligence from companies that traditionally have not been considered part of the auto industry.

**We generally support the layered approach for cybersecurity outlined by NHTSA, as well as the agency’s recommendations for company documentation.** We appreciate NHTSA’s emphasis on fail-safe or fall-back solutions to ensure that vehicle systems take appropriate and safe actions even when an attack is successful. We also support NHTSA’s emphasis on the need for companies to consider privacy and cybersecurity factors very early in the product design cycle, with a goal of designing systems free of safety risks. Furthermore, it is

---

<sup>13</sup> See Consumers Union, “Consumers Union statement on White House discussion draft of Consumer Privacy Bill of Rights Act” (Feb. 27, 2016) (online at [consumersunion.org/news/consumers-union-statement-on-white-house-discussion-draft-of-consumer-privacy-bill-of-rights-act](http://consumersunion.org/news/consumers-union-statement-on-white-house-discussion-draft-of-consumer-privacy-bill-of-rights-act)); Letter from 14 consumer and privacy advocates to President Barack Obama (Mar. 2, 2016) (online at [consumerfed.org/pdfs/150302\\_consumerprivacy\\_President\\_letter.pdf](http://consumerfed.org/pdfs/150302_consumerprivacy_President_letter.pdf)).

appropriate for NHTSA to ask companies to keep detailed documentation of their cybersecurity programs, to periodically assess their effectiveness, and to keep records of any identified and reported vulnerability, exploit, or incident. We urge NHTSA to require this documentation—and its reporting to the agency—to ensure that the relevant documents are available to the agency, cybersecurity researchers, and independent auditors as they validate the safety of a vehicle with regard to security vulnerabilities.

**NHTSA should account for aftermarket devices designed to improve vehicle cybersecurity.** We agree with NHTSA that aftermarket devices should include strong cybersecurity protections, since they could affect the safety of a vehicle. We also urge the agency to consider that aftermarket devices should not be viewed solely as potential threats to vehicle safety. Aftermarket innovation, driven by consumer demand for privacy and security, may yield devices that improve the protection provided by a vehicle to safety-critical or personal information. NHTSA should monitor the marketplace to ensure that the use or installation of such devices is not inappropriately restricted by vehicle manufacturers or other companies.

**Consumers should retain the ability to have their vehicle serviced by the entity of their choice.** We are pleased that NHTSA is urging the auto industry to provide cybersecurity protections that do not unduly restrict access by authorized alternative third-party repair services. NHTSA should further detail the section on Serviceability to ensure that consumers can take their car to the auto service center or mechanic of their choice. The agency's changes to this section should include defining an undue restriction on access to mean a restriction that is not demonstrably justifiable by safety factors, and defining an authorized service to mean a service that is competent—regardless of whether it has been sanctioned by any particular entity.

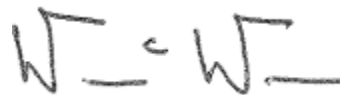
In conclusion, NHTSA's work on automotive cybersecurity is crucial to motor vehicle safety, and we thank the agency for completing the Best Practices. However, additional steps should be taken to ensure that consumers are protected in their cars and that NHTSA receives the information and resources it needs to adequately oversee companies and protect public safety and privacy on the roads. We urge NHTSA to take action, without delay, on the recommendations we make in these comments.

Thank you for your consideration.

Respectfully submitted,



Laura MacCleery  
Vice President  
Consumer Policy and Mobilization  
Consumer Reports



William C. Wallace  
Policy Analyst  
Consumers Union