4910-59-M

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

Docket No. NHTSA-2016-0104

Request for Comment on

Cybersecurity Best Practices for Modern Vehicles

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

ACTION: Request for public comment.

SUMMARY: NHTSA invites public comment on its *Cybersecurity Best Practices for Modern Vehicles*. The document is available for a 30 day comment period at http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

DATES: You should submit your comments early enough to ensure that Docket Management receives them no later than **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments should refer to the docket number above and be submitted by one of the following methods:

- Federal Rulemaking Portal: http://www.regulations.gov. Follow the online instructions for submitting comments.
- Mail: Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue, S.E., West Building Ground Floor, Room W12–140, Washington, DC 20590-0001.
- Hand Delivery: 1200 New Jersey Avenue, S.E., West Building Ground Floor, Room W12–140, Washington, DC, between 9 a.m. and 5 p.m. ET, Monday through Friday, except Federal Holidays.

- *Instructions*: For detailed instructions on submitting comments and additional information on the rulemaking process, see the Public Participation heading of the SUPPLEMENTARY INFORMATION section of this document. Note that all comments received will be posted without change to http://www.regulations.gov, including any personal information provided.
- *Privacy Act*: Anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the Federal Register published on April 11, 2000 (65 FR 19477-78). For access to the docket to read background documents or comments received, go to http://www.regulations.gov or the street address listed above. Follow the online instructions for accessing the dockets.

FOR FURTHER INFORMATION CONTACT: For technical issues: Mr. Arthur Carter of NHTSA's Office of Vehicle Crash Avoidance & Electronic Controls Research at (202) 366–5669 or by email at *arthur.carter@dot.gov*. For legal issues: Mr. Steve Wood of NHTSA's Office of Chief Counsel at (202) 366-5240 or by email at *steve.wood@dot.gov*.

SUPPLEMENTARY INFORMATION

A top NHTSA priority is enhancing vehicle cybersecurity to mitigate cyber threats that could present unreasonable safety risks to the public or compromise sensitive data such as personally identifiable information. And, the agency is actively engaged in approaches to improve the cybersecurity of modern vehicles. The agency has been conducting research and actively engaging stakeholders to identify effective methods to address the vehicle cybersecurity challenges. For example, in January 2016, NHTSA convened a public vehicle cybersecurity

roundtable meeting in Washington, DC to facilitate diverse stakeholder discussion on key vehicle cybersecurity topics. Over 300 individuals attended this meeting. These attendees represented over 200 unique organizations that included 17 Original Equipment Manufacturers (OEMs), 25 government entities, and 13 industry associations. During the roundtable meeting, the stakeholder groups identified actionable steps for the vehicle manufacturing industry to effectively and expeditiously address vehicle cybersecurity challenges. As a follow up, NHTSA held a meeting with other government agencies in February 2016 to discuss possibilities for collaboration among Federal partners to help the industry improve vehicle cybersecurity.

As a result of the extensive public and private stakeholder engagement, NHTSA has developed a set of best practices for the automotive industry that the agency believes will further automotive cybersecurity. The agency notes that the Alliance of Automobile Manufacturers and the Association of Global Automakers, through the Auto Information Sharing and Analysis Center (Auto ISAC), released a "Framework for Automotive Cybersecurity Best Practices" on July 22, 2016.[1] The primary goal of the NHTSA best practices, therefore, is to not supplant the industry-led efforts, but, rather, to support this effort and provide the agency's views on how the broader automotive industry (including those who are not members of the Auto ISAC) can develop and apply sound risk-based cybersecurity management practices to their product development processes. The document will also help the automotive sector organizations effectively demonstrate and communicate their cybersecurity risk management approach to both the public and internal and external stakeholders. NHTSA intends for the document to be updated with some frequency as new information, research, and practices become available.

NHTSA invites public comments on all aspects of these best practices, including how to make the best practices more robust, what gaps remain and whether there is sufficient research

[1] https://www.automotiveisac.com/best-practices/

and/or practices to address those gaps.

Public Participation

How do I prepare and submit comments?

Your comments must be written and in English. To ensure that your comments are filed correctly in the docket, please include the docket number of this document in your comments.

Your comments must not be more than 15 pages long (49 CFR 553.21). NHTSA established this limit to encourage you to write your primary comments in a concise fashion. However, you may attach necessary additional documents to your comments. There is no limit on the length of the attachments.

Please submit one copy (two copies if submitting by mail or hand delivery) of your comments, including the attachments, to the docket following the instructions given above under ADDRESSES. Please note, if you are submitting comments electronically as a PDF (Adobe) file, we ask that the documents submitted be scanned using an Optical Character Recognition (OCR) process, thus allowing the agency to search and copy certain portions of your submissions.

How do I submit confidential business information?

If you wish to submit any information under a claim of confidentiality, you should submit three copies of your complete submission, including the information you claim to be confidential business information, to the Office of the Chief Counsel, NHTSA, at the address given above under FOR FURTHER INFORMATION CONTACT. In addition, you may submit a copy (two copies if submitting by mail or hand delivery), from which you have deleted the claimed confidential business information, to the docket by one of the methods given above under

ADDRESSES. When you send a comment containing information claimed to be confidential business information, you should include a cover letter setting forth the information specified in NHTSA's confidential business information regulation (49 CFR Part 512).

Will the agency consider late comments?

NHTSA will consider all comments received before the close of business on the comment closing date indicated above under DATES. To the extent possible, the agency will also consider comments received after that date.

How can I read the comments submitted by other people?

You may read the comments received at the address given above under COMMENTS. The hours of the docket are indicated above in the same location. You may also see the comments on the Internet, identified by the docket number at the heading of this notice, at http://www.regulations.gov.

Please note that, even after the comment closing date, NHTSA will continue to file relevant information in the docket as it becomes available. Further, some people may submit late comments. Accordingly, the agency recommends that you periodically check the docket for new material.

Anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the Federal Register published on April 11, 2000 (65 FR 19477-78) or you may visit http://www.dot.gov/privacy.html.

Authority: Sec. 31402, Pub. L. 112-141.

Issued in Washington, DC on October 24, 2016 under authority delegated in 49 CFR part 1.95.

_____

Nathaniel Beuse

Associate Administrator for

Vehicle Safety Research

[Billing Code 4910-59-M]

[FR Doc. 2016-26045 Filed: 10/27/2016 8:45 am; Publication Date: 10/28/2016]