**Statement for the Record**

**House Energy and Commerce**

**Subcommittee on Consumer Protection and Commerce Hearing**

**"Promises and Perils: The Potential of Automobile Technologies"**

**Tuesday May 18, 2021, at 10:30 a.m. via Cisco Webex**

**Submitted by**

**Thomas M. Kowalick**

**Chair, Institute of Electrical and Electronics Engineers IEEE 1616: Standard for Motor Vehicle Event Data Recorders (MVEDRs)**

Thank you, Madam Chairwoman.

Today's hearing provides an opportunity to inform your committee about automotive technology being standardized by the Institute of Electrical and Electronic Engineers (IEEE) to reduce the risk of vehicle theft, odometer fraud, Vehicle Identification Number (VIN) cloning, crash data tampering and re-flashing of vehicle electronic networks towards greatly enhancing the cybersecurity of motor vehicles.

IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. IEEE's core purpose is to foster technological innovation and excellence for the benefit of humanity.

IEEE and its members inspire a global community to innovate for a better tomorrow through its more than 400,000 members in over 160 countries, and its highly cited publications, conferences, technology standards, and professional and educational activities.

IEEE is the trusted voice for engineering, computing, and technology information around the globe.

IEEE and its organizational units engage in coordinated public policy activities at the national, regional, and international levels in order to advance the mission and vision of securing the benefits of technology for the advancement of society.

Since the House Commerce and Energy committee jurisdiction includes: consumer affairs and consumer protection; consumer privacy and data security; cybersecurity; consumer product safety; product liability; motor vehicle safety; the Federal Trade Commission; the Consumer Protection Safety Commission; and the National Highway Traffic Safety Administration this IEEE standard will be very valuable towards enhancing cybersecurity of vehicle and highway safety.

No other standards setting organizations cover the scope and purpose of this standard.

**BACKGROUND**

The vehicle DLC (OBD-II) is regulated by the Code of Federal Regulations (CFR) 40 CFR 86.094-17(h)[1] and revisions for subsequent model years. It is standardized by the Society of Automotive Engineers (SAE) Vehicle Electrical Engineering Systems Diagnostic Standards Committee. The physical configuration of the output plug is specified under SAE J1962-2007[2] and thru the International Standards Organization (ISO) under ISO 15031-3-2004 and is increasingly used as an access point to other in-vehicle electronics systems, subsystems, computers, sensors, actuators and an array of electronic control modules (ECU) including airbag sensing diagnostic modules (SDM). The onboard DLC is also used as a serial port to retrieve data elements from on-board systems, subsystems, modules, devices and functions that collect and store data elements related to a vehicle crash such as a restraint control module (RCM) and an event data recorder (EDR) as per 49 CFR 563: Event Data Recorders.[3]

An EDR is a device or function in a vehicle that records a vehicle's dynamic, time-series data just prior to or during a crash, intended for retrieval after the crash. The National Highway Traffic Safety Administration (NHTSA) is responsible for general EDR regulatory oversight and requires the installation of EDR in vehicles to provide an accurate and unbiased understanding of a crash event.

According to the Driver Privacy Act of 2015, when the vehicle owner purchases or leases the vehicle they are considered owners of the Event Data Recorder (EDR) data that the vehicle generates and stores. However, the DLC port is so insecure that the FBI issued a public service announcement (available at https://www.ic3.gov/media/2016/160317.aspx and incorporated herein by reference in its entirety).

The IEEE 1616™ is under revision in 2021 to add information pertaining to motor vehicle event data recorder connector lockout apparatuses. The revised standard defines a lockout protocol for EDR output data accessibility by securing the DLC. This standard does not prescribe data security within the vehicle electronic control units (ECUs) or within the intra-vehicle communication and/or diagnostic networks but instead defines ways and means to permit uniform, but controlled access of electronic scan tools to the DLC for legitimate vehicle emissions status, maintenance and/or repair. This standard also defines a means of maintaining data security on the vehicle via a Near Field Communication (NFC) protocol.

---

[1] https://www.govinfo.gov/app/details/CFR-2007-title40-vol18/CFR-2007-title40-vol18-sec86-094-17

[2] https://www.sae.org/standards/content/j1962_201207/

[3] https://www.govinfo.gov/app/details/CFR-2011-title49-vol6/CFR-2011-title49-vol6-part563

The Department of Homeland Security's US-CERT tasked the CERT Coordination Center (CERT/CC)[4] at Carnegie Mellon University's Software Engineering Institute (SEI) to study OBD devices to better understand the cybersecurity impact to consumers and the public. The CERT/CC analyzed a representative sample of these devices for vulnerabilities and found widespread failure to apply basic security principles. If these devices are compromised, the potential impact includes loss of privacy, vehicle performance degradation or failure, and potential injury. The goal of CERT/CC's research was to better inform consumers, enterprise fleet managers, insurance companies, and policy makers about the potential risks of these devices.

The NHTSA estimates that 91.6% of modern vehicles include EDRs.[5] When the Haddon Matrix is applied to crashes it cites pre-crash, crash and post-crash. The crash mode is generally the crash site. The 'window of opportunity' to misuse EDR date is from the time of the crash until the time that the data is downloaded by a trusted entity of the Court, such as law enforcement.

Additionally, the CERT/CC report notes, "In enterprise IT environments, the majority of attackers are assumed to be remote, attacking the systems over the Internet. A specific automobile would be difficult to identify on the Internet, if it is directly accessible at all. Attackers are also likely to use computer security vulnerabilities as enablers of other, more physical crimes. Therefore, the threat actors are likely to be local to a targeted vehicle, generally within Wi-Fi or Bluetooth range. This doesn't rule out remote attacks, as a compromised mobile device with Internet connectivity could be connected to the car via an OBD-II device, USB, Bluetooth, or Wi-Fi. A secondary risk of using these devices is that compromise of the manufacturer or operator's back-end server may allow an attacker to access any device connecting to its network. When a consumer decides to plug one of these devices into their vehicle, they are unintentionally moving the security boundary from the vehicle itself to the device manufacturer's network, associated services, and any other connected device."

The House Commerce and Energy Committee is well aware that aftermarket OBD-II devices have the potential to introduce serious safety and security risks to an automobile.[6] The design of the OBD-II port means that such a device has unlimited access to some or all of a car's internal networks. These OBD-II devices also have some sort of external interface that is accessible from outside of the car—typically Wi-Fi, Bluetooth, or cellular.

Thus, there remains a need to secure a vehicle's EDR data from cybersecurity attacks, particularly before, during and after a crash event, while at the same time providing a chain of custody of the vehicle's EDR data.

In some states, EDR data is not protected by the Fourth Amendment and may be obtained without a warrant. See Mobley v. State, 346 Ga.App. 641 (2018).

---

[4] https://www.kb.cert.org/vuls/

[5] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201210&RIN=2127-AK86

[6] https://republicans-energycommerce.house.gov/news/press-release/board-diagnostic-obd-ii-ports-within-your-car-potential-gateway-hackers/

Thus, the IEEE standard provides a system and method for installing a device to prevent unauthorized access to the EDR data or provide permission for others to install the device after a crash event.

In a recent letter NHTSA Deputy Administrator James C. Owens stated:

> It is worth noting that NHTSA does not take issue with efforts relating to data ownership, privacy, or serviceability, to the extent they do not affect motor vehicle safety. In fact, in NHTSA's published Cybersecurity Best Practices for Modern Vehicles document, section 9 recommends that the automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by authorized alternative third-party repair services.[7]

NHTSA's Cybersecurity Interests

As background, NHTSA's statutory authorities center on motor vehicle safety.[8] Accordingly, NHTSA's primary interest focuses on cybersecurity vulnerabilities that present potential vehicle safety consequences, which is a subset of the universe of cybersecurity. The increase in uses of software-intensive motor vehicle components, including telematics systems, introduces new and different risks to motor vehicle safety. Risks include the potential that the technological methods, tools, and capabilities could be compromised and used in ways that create unintended, and at times, unsafe outcomes. The specific possibility of a software vulnerability potentially being used by malicious actors to cause a crash or incident is the primary cybersecurity concern for NHTSA as the safety oversight agency for the automotive industry. NHTSA has authority to order vehicle recalls based on unreasonable risks to safety including those that may be caused by cybersecurity vulnerabilities.

For years, NHTSA has worked to encourage industry to adopt improved cybersecurity practices, recognizing that cybersecurity risks are real, and that protection of safety-critical vehicle systems from malicious hacking attempts is vital to the safety of the motoring public. Telematics systems are an area of great concern to the agency, because such systems could allow actors to receive and/or send information to vehicles outside of the vehicle itself, and potentially interface with multiple vehicles at a time, and to do so without gaining physical access to the vehicle.

NHTSA published a *Cybersecurity Best Practices for Modern Vehicles* document to provide guidance to manufacturers and suppliers in developing strategies to make their vehicles more secure against malicious attacks and more resilient if such attacks are successful. This guidance encouraged manufacturers to harden safety-critical systems, identify and evaluate risk during system and vehicle development processes, and develop layers of protection throughout vehicles to protect against access by unauthorized third-parties and which are appropriate for the identified risks.

[7] https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf

[8] 49 U.S.C 30101 et seq.

See Existing Federal guidance and cybersecurity best practices [9]

SCOPE of IEEE-1616™: Standard for Motor Vehicle Event Data Recorders (MVEDRs)

1. Motor Vehicle Event Data Recorders (MVEDRs) collect, record, store and export data related to motor vehicle pre-defined events in usage history.

2. This standard defines a protocol for MVEDR output data compatibility and export protocols of MVEDR data elements.

3. This standard does not prescribe which specific data elements shall be recorded, but instead provides a data dictionary of data attributes.

4. This standard also defines a means of maintaining data security on the vehicle via a motor vehicle diagnostic link connector lockout apparatus (MVEDRCLA) by securing the vehicle output diagnostic link connector (DLC).

5. This standard does not prescribe data security within the vehicle electronic control units (ECUs) or within the intra-vehicle communication and/or diagnostic networks; it instead defines ways and means to permit uniform but controlled access of electronic scan tools to the DLC for legitimate vehicle emissions status, maintenance, and/or repair.

6. This standard also defines a Motor Vehicle Event Data Recorder Connector Lockout Apparatus (MVEDRCLA) and a Near Field Communication (NFC) protocol of safeguarding access to a vehicle's event data recorder (EDR) data by securing the vehicle output diagnostic link connector (DLC).

7. This standard is without prejudice to requirements of national or regional laws related to privacy, data protection and personal data processing.

8. This standard does not directly address related issues with regard to human health or human safety.

9. It is applicable to vehicles and their respective event data recorders for all types of motor vehicles licensed to operate on public roadways, whether offered as original or aftermarket equipment, whether stand-alone or integrated within the vehicle.

PURPOSE of IEEE-1616™

[9] https://csrc.nist.gov/News/2019/nist-publishes-nistir-8228

1. Many light-duty motor vehicles, and increasing numbers of heavy commercial vehicles, are equipped with some form of MVEDR.

2. These systems, which are designed and produced by individual motor vehicle manufacturers and component suppliers, are diverse in function, and proprietary in nature, however, the SAE J1962 vehicle DLC has a common design and pinout and is thus universally used to access event data recorder information.

3. Data access via the DLC can be accomplished by using scan tools or microcomputers and network interfaces.

4. This same DLC and network interface is also used for re-calibrating electronic control units on a vehicle.

5. Such ECU applications can include restraint controls, engine controls, stability controls, braking controls, etc.

6. This standard defines a protocol to protect against misuse of electronic tools which use the DLC to erase, modify or tamper with electronic controller or odometer readings, or to improperly download data.

7. Implementation of MVEDRCLA provides an opportunity to voluntarily achieve DLC security by standardizing a MVEDRCLA which will act to prevent vehicle tampering, which can include odometer fraud, illegal calibrations leading to emissions violations and theft of personal data.

8. Adoption of this standard will therefore make the common MVEDR/DLC data more secure and credible while still permitting accessibility to legitimate end users.

9. The continuing implementation of MVEDR systems provides an opportunity to voluntarily standardize data output and retrieval protocols to facilitate analysis and promote compatibility of MVEDR data.

10. Adoption of the standard will therefore make MVEDR data more accessible and useful to end users.

**Introduction to IEEE-1616™**

Crash information is critical to understanding causation leading up to the crash, occupant kinematics and vehicle performance during a crash, and post-crash events. Manufacturers, engineers, policy makers, researchers, and others rely on crash information to improve vehicle design, shape regulatory policy, develop injury criteria, detect vehicle defects, and resolve investigations and litigation.

Motor vehicles have markedly transitioned from mechanical machines with mechanical controls to highly technological vehicles with integrated electronic systems and sensors. Modern automobiles

generate, utilize, and analyze electronic data to improve vehicle performance, safety, security, comfort and emissions. Surrounding a crash, capture of a subset of vehicle data on an MVEDR makes important information readily available for medical responders, crash investigators, and researchers. The degree of societal benefit from MVEDRs is directly related to the number of vehicles operating with an MVEDR and the ability to retrieve and utilize these data. Having standardized data definitions and formats allows the capture of vehicle crash information.

The P1616 Working Group of IEEE recognizes the value of improved crash information in improving the knowledge of what happens before, during, and after a motor vehicle crash. Such insights will provide major benefits to society and significantly improve the science of motor vehicle crashes. This standard defines a protocol for MVEDR output data compatibility and export protocols of MVEDR data elements

The impact of improved crash data goes beyond just understanding the dynamics of a crash; it affects a myriad of important societal and business functions. With that in mind, the Working Group solicited input from a range of end users to help identify important data element and critical uses of motor vehicle crash data. Both individual crash events and aggregate data have value for end users, depending on the application and data used.

Some users and uses include the following:

- Automotive industry: Data-driven design of vehicles, using larger numbers of crashes across a continuum of severity; early evaluation of system and vehicle design performance; and international harmonization of safety standards.
- Insurance industry: Help to identify fraudulent claims, costing more than $20 billion annually; improve risk management; expedite claims and decrease administrative cost. Insurers require accurate crash data for subrogation of claims and recovery of expenses.
- Government: Promulgating and evaluating standards; identifying problem injuries and mechanisms; stipulating injury criteria and investigating defects. State and local officials require crash information to identify problem intersections and road lengths, to determine hazard countermeasures, and to evaluate the effectiveness of safety interventions.
- Researchers: Human factors research, such as the man-machine interface; crash causation, the effects of aging and medical conditions, and fatigue; biomechanics research on human response to crashes, harmonized dummy development, and injury causation.
- Medical providers: On-scene field triage of motor vehicle crash victims; improved diagnostic and therapeutic decisions; automatic notification of emergency providers; better organization of trauma and EMS system resources.
- The Public: Better policies, vehicle design, emergency response, roadway design, and driving habits; lowered insurance costs, decreased possibility for fraud; fewer crashes and more efficient systems.

In the United States, an estimated 80 million motor vehicles already use some type of event-recording equipment that collects not only acceleration and deceleration speed but also braking and steering data. Proponents of standard data recorders hope the crash data they collect will be a useful complement to accident information gathered from victims and eyewitnesses.

However, the implementation of event data recorders (EDRs) has not been without controversy.

The United States Department of Transportation (USDOT) Docket Management System (DMS) contains over 1000 submissions reflecting the pros and cons of a decade-long debate amongst automakers, government regulators, safety and privacy advocates, and the public.

The National Highway Traffic Safety Administration (NHTSA) Rule on Event Data Recorders (49 CFR 563 does not address issues generally within the realm of state law, such as the following:

- The ownership of EDR data
- How EDR data can be used/discovered in civil litigation
- How EDR data may be used in criminal proceedings
- Whether EDR data may be obtained by the police without a warrant
- Whether EDR data may be developed into a driver-monitoring tool
- The nature and extent that private parties will have or may contract for access to EDR

The Congressional Research Service (CRS) Report R43651 "Black Boxes" in Passenger Vehicles: Policy Issues cites IEEE standards. Can technology also protect privacy? While NHTSA was studying EDR technology, the Institute of Electrical and Electronics Engineers (IEEE) issued in 2004 the first universal, voluntary standard specifying minimal performance characteristics for memory devices in autos, trucks, buses, ambulances, and fire trucks. IEEE Standard 1616™ is an international protocol issued to help manufacturers develop black boxes with up to 86 data elements that will survive in crash situations. IEEE and others have argued that NHTSA's pending EDR regulation does not go far enough to protect owners' privacy. In 2010, IEEE issued a new Standard 1616a™, which specifies a lockout system to block unauthorized access that could otherwise lead to data tampering, odometer fraud, and VIN theft. It argued that such steps are necessary to ensure that motorists embrace the EDR technology in the long run. With this lockout standard, a motorist would have a separate key which would lock access to the OBD-II connector (as well as the EDR). Note. IEEE-1616™a is being incorporated into IEEE-1616™-2021.

REGULATION & ADVOCACY

Petitions were denied on this basis: "Despite the purported availability of such devices, we have still not seen evidence of tampering during our real world data collections, and the petitioner provided no new information that would suggest that we should reconsider our previous denial of this request."

PROVIDING NEW EVIDENCE: Since NHTSA denials there have been motor vehicle event data recorders (EDRs) installed in 91% of U.S. light vehicles, hundreds of YouTube videos were created showing how to erase crash data and reset air bags, worldwide there were increases in vehicle theft and examples of data tampering on major news networks The FBI issued a public service announcements about OBD ports and the USDOJ announced numerous large scale odometer fraud convictions. Tragically, the NHTSA research on cybersecurity is reactive vs. proactive.

To date, NHTSA denied all letters of recommendations submitted to the docket, recommendations via meetings at NHTSA headquarters, petitions and petitions for reconsideration to enhance vehicle cybersecurity.[10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21]

The Electronic Privacy Information Center (EPIC) web site at https://www.epic.org/privacy/edrs/ is updated frequently.

## CONCLUSION

## NHTSA's 'BLIND-SPOT' is BALANCING TECHNOLOGY FORESIGHT UNCERTAINTIES AND CONSUMER PROTECTION IN EDR REQUIREMENTS

The NHTSA "safety only" mandate ignores consumer protection, consumer acceptance and privacy issues. Simply put, NHTSA erroneously requires quantitative evidence that a sizable problem exists (regarding tampering of EDRs and odometer roll-back) before it will act. In reality, NHTSA would in fact be creating a sizable problem by mandating EDRs in light vehicles without providing owners of the vehicle basic consumer protection. The owner of the vehicle, not the automaker should control access to this device (EDR) since it is widely known that In-vehicle electronic modules are subject to tampering, spoliation of evidence, undetectable surveillance, unauthorized access, misuse of data, and mischief.

---

[10] https://www.regulations.gov/document/NHTSA-2008-0019-0006

[11] https://www.regulations.gov/document/NHTSA-2006-25666-0438

[12] https://www.regulations.gov/document/NHTSA-2008-0004-0007

[13] https://www.regulations.gov/document/NHTSA-2008-0004-0012

[14] https://www.regulations.gov/document/NHTSA-2008-0004-0013

[15] https://www.regulations.gov/document/NHTSA-2012-0177-1046

[16] https://www.regulations.gov/document/NHTSA-2008-0004-0014

[17] https://www.regulations.gov/document/NHTSA-2008-0004-0001

[18] https://www.regulations.gov/document/NHTSA-2008-0004-0015

[19] https://www.regulations.gov/document/NHTSA-1999-5218-0009

[20] https://www.regulations.gov/document/NHTSA-2006-25666-0457

[21] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201010&RIN=2127-AK71

Thus, common sense dictates that more emphasis is needed on sealing access to the data at the federally-mandated On-Board Diagnostics (OBD-II) download connector port, located under the dash in virtually all modern vehicles, therefore establishing a chain of custody and preventing tampering.

NHTSA should adhere to the National Technology Transfer Advancement Act (CNTTAA) and incorporate by reference IEEE-1616™ into 49 CFR 563: Event Data Recorders. The IEEE EDR standards offer vehicle owners, fleets, rentals and lessor's accountability, protection and security. Use of IEEE standards would be consistent with applicable law and would improve motor vehicle safety by preventing a consumer backlash towards implementing EDR technology. Use of IEEE EDR standards would be practical. The IEEE EDR standard provides a promising countermeasure addressing the safety promise and challenges of 21st Century in-vehicle automotive networks and vehicular electronics. Specifically, vehicle owners must "own" the EDR data, become "aware "of EDRs existence and functioning and must "control access" to the EDR data in their vehicles.

Given these goals, it it recommended that the House Energy and Commerce Committee direct NHTSA to amend 49 CFR 563: Event Data Recorders by adding the following:

563.13 Motor Vehicle Event Data Recorder Connector Lockout Apparatus (MVEDRCLA). Each manufacturer of a motor vehicle equipped with an EDR shall ensure that a motor vehicle event data recorder connector lockout apparatus (MVEDRCLA) as standardized by the Institute of Electrical and Electronics Engineers (IEEE 1616-2021) to help protect the security, integrity, and authenticity of the data that are required by this part is attached to the vehicle's SAE J1962 (150/015 15031-3) vehicle diagnostic link connector (OLC) at the point of motor vehicle sale, including leased and rented vehicles.

DEFINITION: Connector Lockout Apparatus (CLA) is a device or mechanism to secure a vehicle diagnostic link connector (DLC) as standardized by IEEE-1616™-2021.

IEEE 1616 will be issued in 2021 at https://www.ieee.org/standards/buy-standards.html

ADDITIONAL RESOURCES:

American Civil Liberties (ACLU) AMICUS Brief see https://www.aclu.org/legal-document/mobley-v-state-amicus-brief

Code of Federal Regulation (CFR) 563: Event Data Recorder. See https://www.govinfo.gov/content/pkg/CFR-2011-title49-vol6/pdf/CFR-2011-title49-vol6-part563.pdf

Congressional Research Service (CRS) Report R43651 “Black Boxes” in Passenger Vehicles: Policy Issues. See https://crsreports.congress.gov/product/pdf/R/R43651

Congressional Research Service (CRS) IF Autonomous Vehicles: Emerging Policy Issues at https://crsreports.congress.gov/product/pdf/R/R44940

ECE/TRANS/WP.29/2020/123: 01 Series of Amendments for UN Regulation No.[XXX], UN Regulation on uniform provisions concerning the approval of motor vehicles with regard to the Event Data Recorder. See https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-07-60e.pdf

European Commission (EC) VERONICA II Final Report at https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/pdf/projects/veronica.pdf

Electronic Privacy Information Center (EPIC) Cahen v. Toyota Motor Corporation: Whether drivers can sue for privacy and security vulnerabilities in connected cars at https://epic.org/amicus/cahen/

Electronic Privacy Information Center (EPIC) COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER TO THE NATIONAL HIGHWAY TRANSPORTATION SAFETY ADMINISTRATION (NHTSA) see https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf

National Conference of State Legislatures (NCSL) Privacy of Data from Event Data Recorders: State Statutes at https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx

National Institute Standards Technology (NIST) Automotive and Industrial Data Security presentation https://csrc.nist.gov/CSRC/media/Presentations/Automotive-and-Industrial-Data-Security/images-media/presentation-2_weimerskirch.pdf

National Research Council (NRC) of the National Academies of Sciences (NAS) Transportation Research Board (TRB) Special Report 308: The Safety Challenge and Promise of Automotive Electronics [ISBN 978-0-309-22304-1] see https://www.nap.edu/catalog/13342/trb-special-report-308-the-safety-challenge-and-promise-of-automotive-electronics

U.S. Congress https://www.scribd.com/document/401616402/Internet-of-Things-IoT-Cybersecurity-Improvement-Act-of-2019

U.S. Congress DRIVER'S PRIVACY ACT OF 2015 see https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf

Federal Bureau of Investigation (FBI) see https://www.ic3.gov/Media/Y2016/PSA160317

Federal Trade Commission (FTC) See https://www.ftc.gov/policy/advocacy/advocacy-filings/2016/11/comment-jessica-l-rich-director-bureau-consumer-protection

Society of Automotive Engineers (SAE) Automotive Cybersecurity at https://www.sae.org/cybersecurity/

USDOT/NHTSA: Vehicle Cybersecurity at
https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

U.S. Congress https://www.scribd.com/document/401616402/Internet-of-Things-IoT-Cybersecurity-Improvement-Act-of-2019

U.S. Congress DRIVER'S PRIVACY ACT OF 2015 see https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf

Respectfully Submitted on May 17, 2021

Thomas M. Kowalick

Thomas M. Kowalick

305 South Glenwood Trail

Southern Pines, North Carolina

28387

mvedr@ieee.org