March 15, 2021

SUBMITTED ELECTRONICALLY VIA REGULATIONS.GOV

Dr. Cem Hatipoglu
Associate Administrator for Vehicle Safety Research
National Highway Traffic Safety Administration
Department of Transportation
1200 New Jersey Avenue S.E., West Building
Washington D.C. 20590-0001

Re: *Request for Comments on Cybersecurity Best Practices for the Safety of Modern Vehicles,* Docket No. NHTSA-2020-0087, 86 Fed. Reg. 2481 (January 12, 2021)

Dear Dr. Hatipoglu:

The Alliance for Automotive Innovation ("Auto Innovators") appreciates this opportunity to provide input to the National Highway Traffic Safety Administration ("NHTSA") in response to its request for public comments on the updated draft cybersecurity best practices document titled *Cybersecurity Best Practices for the Safety of Modern Vehicles* ("Cybersecurity Best Practices"). Given the dynamic nature of the cybersecurity landscape, Auto Innovators welcomes this update to the Cybersecurity Best Practices.

Every year, our lives become more connected to and dependent on the digital world. Products and services that once only existed in the physical world are now part of our connected society. Automobiles are no exception.

As physical machines evolve into increasingly software-dependent and connected platforms, technology is reshaping the relationship between vehicles and their users. In the past, the main, or only, external input for a vehicle was the driver or occupants of the vehicle. That is no longer the case. Innovative vehicle technologies - combined with the integration of vehicles into a broader ecosystem of connected infrastructure, devices, features, and stakeholders – can unlock a wide range of benefits in safety, fuel efficiency, and convenience. This transformation also provides consumers with new - and, increasingly, remote - ways of interacting and engaging with vehicles, opening doors to innovative businesses, technologies, and services.

The benefits of this transformation have the potential to be profound, driving us to a cleaner, safer, and smarter future. Yet, the technologies at the forefront of this evolution – including connectivity, electrification, automation– may also introduce new threats and risks. These increasingly digital, rather

than mechanical, challenges are also no longer isolated to the confines of the vehicle. They extend to the vast ecosystem of connections and stakeholders, introducing factors outside an automaker's control.

Security is crucial to realizing the safety, privacy, environmental and societal benefits of vehicles with advanced technologies. The automotive industry understands the realities of a connected world and takes cybersecurity risks seriously. That is why it has been working proactively and collaboratively to build security into the products and services that will define the future of transportation.

Identifying and Minimizing Risk

Cybersecurity begins with risk management, the application of robust processes and procedures to identify and manage risk throughout the product lifecycle. As recognized by multiple government agencies, industry sectors and academics, the cyber threat is not a problem that can ever be eliminated, but rather a risk that must be constantly managed and mitigated. In short, because there is no one "right" answer to cybersecurity, risk management is integral to any successful cybersecurity program.

Fortunately, risk management is not a new concept to the auto industry. For decades, the auto industry has relied on robust risk management standards and practices to develop and deploy life-saving safety technologies. Leveraging this expertise in combination with lessons learned from other sectors, the industry is adapting cybersecurity risk management strategies to meet the challenges and complexities of the modern vehicle. These include industry-developed best practices and standards and risk management frameworks developed by federal partners, including the National Institute of Standards and Technology ("NIST") Cybersecurity Framework.

The auto industry is building on these existing resources. For the first time ever, the two largest standards bodies for the auto industry, the International Organization for Standardization (ISO) and SAE International (SAE), have come together to develop a single, global standard for vehicle cybersecurity, ISO/SAE 21434. The multi-year effort has brought together more than 100 experts from 14 nations, spanning a diverse group of public and private sector organizations. Once finalized, ISO/SAE 21434 will articulate a clear and standardized approach, built upon existing best practices, for managing cybersecurity risk throughout the lifecycle of the vehicle – from design through decommissioning.

Sharing Information

One of the central pillars of effective cybersecurity is information sharing, especially between the public and private sector. The private sector owns and operates the vast majority of the U.S.'s critical infrastructure but does not have ready access to the information and resources available to government that may help protect those national assets. The U.S., therefore, has long relied on a public-private partnership model, built around 16 critical infrastructure sectors, to protect the nation's critical infrastructure.

Automotive transportation is not covered as an existing critical infrastructure sector. However, with increased automotive connectivity, automakers and government partners recognized a need for greater collaboration across industry and with public sector partners. As a result, in 2015, the auto industry proactively created an Information Sharing and Analysis Center (ISAC) in partnership with the U.S. Department of Homeland Security. The Automotive ISAC ("Auto-ISAC") now includes more than 50 members.

Developing and Applying Best Practices

In addition to providing a forum to share threat information, the Auto-ISAC has brought the industry together on collaborative, forward-leaning initiatives to enhance cybersecurity throughout the entire motor vehicle value chain. Notably, one of the first projects launched by the Auto-ISAC was the development of a robust series of Automotive Cybersecurity Best Practices ("Best Practices"). The Best Practices build upon the Framework for Automotive Cybersecurity Best Practices, released in January 2016 by the former industry trade associations, the Alliance of Automobile Manufacturers and the Association of Global Automakers.

Through extensive collaboration and engagement, the Auto-ISAC facilitated the development of seven Best Practice guides to "assist automotive industry stakeholders with identifying, prioritizing, treating, and monitoring vehicle cybersecurity risks."[1] The seven Best Practice guides, which are available to the public, address:

1. Incident Response
2. Collaboration and Engagement with Appropriate Third Parties
3. Governance
4. Risk Assessment and Management
5. Awareness and Training
6. Threat Detection, Monitoring and Analysis
7. Security Development Lifecycle

In addition to the Auto-ISAC Best Practice, the industry also benefits from guidance documents and other products developed by federal stakeholders, including NHTSA's Cybersecurity Best Practices. Informed by engagement with industry, security researchers, and other stakeholders, the NHTSA Cybersecurity Best Practices remains an important document that helps articulate the agency's expectations for motor vehicles.

Continuing Collaboration Between Public and Private Stakeholders:

While the Auto-ISAC represents an important mechanism for sharing threat information, managing the cyber threat requires extensive collaboration with public and private stakeholders. In everything from research and development, to vulnerability identification and management, the auto industry continues to work with a wide range of stakeholders to keep pace with the cyber threat.

Through partnerships with federal agencies, the auto industry is working collaboratively with public sector partners to adapt and advance the cyber tools, techniques, and capabilities of the industry. These partnerships extend across the federal government and includes important collaborations with the U.S. Department of Transportation, the National Telecommunications and Information Administration, the

---

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

Department of Energy, NIST, and DHS. This remains an important area for continued dialogue, collaboration, and engagement between industry and federal partners.

As you are well aware, over the past decade, several high-profile research demonstrations have highlighted the potential risks, and associated public response, of vehicle hacking. As motor vehicles become more connected, companies, researchers and others have and continue to devote significant time, resources, and increasingly sophisticated capabilities towards examining and understanding how to mitigate vulnerabilities in the motor vehicle ecosystem.

Whether working directly with companies or independently, security researchers are now an important stakeholder in the motor vehicle value chain to help identify threats or vulnerabilities before they are potentially exploited. Their expertise also assists companies as they build security safeguards, tools, and operating procedures into vehicles and their communications links. Like other sectors, in the past several years, the auto industry has embraced this new partner. This includes employing white hat hackers and security research firms to test and validate products to help identify potential vulnerabilities, establishing vulnerability disclosure programs to facilitate engagement with the research community, sponsoring and presenting at cybersecurity research conferences, and participating in NTIA's multi-stakeholder process on vulnerability disclosure to help inform and facilitate engagement between the research community and development community.

Cybersecurity Best Practices Recommendations

With respect to the update to the Cybersecurity Best Practices itself, Auto Innovators offers the following recommendations.

Foster Harmonization

As more stakeholders develop products focused on – or applicable to - automotive cybersecurity, it is important to ensure alignment, to the extent practicable, among those disparate efforts. To the extent feasible, NHTSA should help ensure alignment and harmonization between its Cybersecurity Best Practices and ongoing international work related to standards, regulations, and other relevant practices.

To this end, we appreciate NHTSA's efforts to align this update to the Cybersecurity Best Practices with the forthcoming ISO/SAE 21434. However, we believe there may be additional opportunities to further align the Cybersecurity Best Practices with the standard, as well as other relevant international standards.

Further, we encourage NHTSA to explore opportunities to enhance alignment between the Cybersecurity Best Practices, industry standards, and the recently adopted UN regulations for automotive cybersecurity and over-the-air updates. As the party leading the translation/implementation of the UN regulations to the 1998 Agreement, NHTSA has an opportunity to help shape this process in a manner that offers the greatest opportunity for international alignment and harmonization on automotive cybersecurity.

Finally, we encourage NHTSA to consider the technical comments submitted by SAE TEVEES18A – Cybersecurity Systems Engineering Committee. Auto Innovators may follow-up with additional technical comments, as necessary.

Keep Pace with the Threat Landscape

NHTSA should continue to update this best practice document as appropriate going forward to keep pace with the rapidly evolving threat landscape, as well as to reflect important cybersecurity-related work and actions by industry, standards bodies, and other stakeholders.

We also recommend NHTSA create a section in the best practice document on emerging risks where there may not be established best practices yet to treat these risks. This section could include high-level recommendations to encourage industry-wide collaboration to establish best practices to treat those risks.

Even with a multi-layer defense, automakers must remain nimble and adaptive to keep pace with the rapid and dynamic evolution of cyber threats. Locking in what seems proactive now may not be so effective when the future demands another approach. The processes and practices being developed by automakers, governments, standards bodies, and multi-sector industry partners all contribute to managing and mitigating this emerging risk. This work should be monitored and incorporated, as necessary.

Conclusion:
Auto Innovators appreciates the opportunity to comment on this important update to the Cybersecurity Best Practices. We look forward to continuing to work with NHTSA and federal partners on this important topic.

Sincerely,

John Ohly
Senior Director, Strategy, Advocacy, and Technology Policy
Alliance for Automotive Innovation