Information Technology Industry Council

December 8, 2014

Docket Management Facility
U.S. Department of Transportation
1200 New Jersey Avenue SE.
West Building Ground Floor, Room W12-140
Washington, DC 20590-0001

Submitted at: http://www.regulations.gov/#!submitComment;D=NHTSA-2014-0108-0001

RE: ITI comments in response to Docket No. NHTSA-2014-0108: "Request for Comment on Automotive Electronic Control Systems Safety and Security"

To Whom It May Concern:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to Docket No. NHTSA-2014-0108, "Request for Comment on Automotive Electronic Control Systems Safety and Security."

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry.[1] ITI's 60 members comprise the world's leading innovation companies, including global manufacturers of ICT products who are committed to providing consumers with products that are safe, secure, and meet all appropriate requirements for electromagnetic interference and other technical areas. Further, as both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. We acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms. We recognize the goal of the National Highway Transportation Safety Administration's (NHTSA) to examine the need for electronic systems safety standards in passenger motor vehicles, as well as to look at cybersecurity considerations of electronic components and connected vehicles. We welcome the chance to share these comments and to continue to work with NHTSA to answer further questions and share our industry's experience and expertise in these areas.

In our response we are focusing specifically on the cybersecurity related-questions in which we have particular expertise. We have copied below in bold those questions to which we are responding.

[1] See www.itic.org

Cybersecurity-related questions

Cybersecurity is rightly a priority for all governments. The ICT industry shares the goal with governments of improving cybersecurity and therefore our interests are fundamentally aligned. In an effort to better inform the public cybersecurity discussion, in 2011 ITI published a comprehensive set of Cybersecurity Principles for Industry and Government.[2] ITI's six principles aim to provide a useful and important lens through which any efforts to improve cybersecurity should be viewed. To be effective, efforts to enhance cybersecurity must:

1. Leverage public-private partnerships and build upon existing initiatives and resource commitments;
2. Reflect the borderless, interconnected, and global nature of today's cyber environment;
3. Be able to adapt rapidly to emerging threats, technologies, and business models;
4. Be based on effective risk management;
5. Focus on raising public awareness; and
6. More directly focus on bad actors and their threats.

The ITI principles remain salient to this day and underpin any feedback ITI provides governments on their cybersecurity efforts—including the U.S. Administration and U.S. Congress as well as global governments—and also guide the comments we provide below on NHTSA's cybersecurity-related questions.

III b. Security Needs To Prevent Unauthorized Access to Electronic Components

Statement from NHTSA RFC: *Cybersecurity, within the context of road vehicles, is the protection of vehicular electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation….NHTSA has been actively researching existing cybersecurity standards and best practices in automotive and other industries. In reviewing the practices of other industries in dealing with cybersecurity issues, NHTSA has identified two general process-oriented approaches to addressing cybersecurity concerns. The first is design and quality control processes that focus on cybersecurity issues throughout the lifecycle of a product. The second is dealing with cybersecurity issues through establishing robust information sharing forums such as an Information Sharing and Analysis Center (ISAC). This section discusses the agency's findings regarding each of these strategies….*

…Security process standards and information sharing forums fit in a larger, more comprehensive automotive cybersecurity assurance approach. In general terms, there are four major pieces to the agency's research approach:

1. Preventive methods and techniques…

a. Encryption and/or authentication on communication networks;
b. different communication approaches or protocols; segmentation/isolation of safety-critical system control networks;
c. strong authentication controls for remote access to vehicles;
d. gateway controls between interfaced vehicle networks; etc.

[2] See http://www.itic.org/dotAsset/0e3b41c2-587a-48a8-b376-9cb493be36ec.pdf

Other approaches in the field of prevention research include….
2. Real-time intrusion detection methods…
3. Real-time response methods…
4. Treatment methods…

Comments Requested

(1) We seek comment on any technical areas of automotive cybersecurity *that the agency could focus on* in its further research.

(a) Specifically, are there particularly vulnerable or strong design architectures that the agency should further examine?

(b) What additional types of techniques (either in real world occurrences or as a part of research) have persons used to gain unauthorized access to vehicle systems? What types of systems were such persons able to gain access to?

(c) What is the public's view on the differences in cybersecurity risks associated with an intrusion that requires use of in-cab physical interfaces (e.g. OBD-II port) versus close-proximity wireless interfaces (e.g. Bluetooth) versus long-range wireless means (e.g. cellular/satellite links)?

ITI appreciates NHTSA's interest in contributing its experience and expertise to research in automotive cybersecurity. In doing so, we urge NHTSA to ensure that it collaborates closely and regularly with the ICT industry as well as the automotive industry. Many of the cybersecurity issues about which NHTSA is interested—such as design architectures, gaining unauthorized access, and types of interfaces—are not necessarily automotive-specific and there may be extensive work ongoing by the ICT industry in these areas already. NHTSA should also coordinate with and leverage existing efforts on cyber-physical systems. One such example NHTSA should consider is the NIST Cyber-Physical Systems Public Working Group (CPS PWG), which has been launched to bring together experts to help define and shape key aspects of CPS to accelerate its development and implementation across multiple industry sectors.[3]

(2) We seek comment on security process standards.

(a) What security process standard alternatives are available? How do these standards differ and are there standards that are more suitable for application to the automotive industry versus others?

(b) Could security assurance be handled within a modified framework of existing safety process standards (such as FMEAs, FTAs, ISO 26262) or does "design for security" require its own process?

(3) We seek comments on security performance standards. In contrast to the process standards (that establish methods for considering cybersecurity risks during product design), we use the term "performance standard" to mean standards that evaluate the cybersecurity performance (or resilience) of a system after production of the final product.

(a) What types of metrics are available to test a vehicle's ability to withstand a cyber-attack?

[3] See http://www.nist.gov/cps/

(b) Are there any common design characteristics that help ensure a minimum level of security from unauthorized access to a vehicle's electronic control systems?
(c) What performance-based tests, methods, and processes are available for security assurance of automotive electronic control systems?
(d) Are there hardware, software, watchdog algorithm, etc. requirements or criteria that would help differentiate algorithm designs that are more secure against cyber-attack?

We have some observations and responses to questions 2 and 3 above. Cybersecurity standards—both process and performance—are essential to cybersecurity. However, it is important to stress there is no one "cybersecurity standard" or set of practices applicable across the board, even in a particular vertical industry. Cybersecurity is complex, including many moving parts, responsible parties, and standards. Industry uses a range of global standards and companies contribute to developing such standards on a global, voluntary, and consensus basis through numerous organizations including formal standards development bodies as well as consortia and alliances. In addition, global industry continually establishes new standardization efforts addressing emerging technologies and cybersecurity risk concerns. Many of these standardization efforts focus on areas NHTSA lists above, such as algorithm design.

We are concerned that, by asking about specific process and performance security standards, NHTSA may be assuming that particular cybersecurity standards are more useful or appropriate than others and might deserve government endorsement, guidelines, or even mandates. We strongly caution NHTSA to avoid setting any requirements as to particular cybersecurity process or performance standards the automotive industry should use in the United States. Doing so would have at least four negative consequences:

- Government mandates to use certain standards would lock industry into particular solutions that may be effective against certain threats at a given point in time, but would not be able to meet future, as-yet-unknown challenges. Such a static approach would stymie industry's ability to innovate new security approaches and standards, as well as the ability of the auto industry to deploy new security solutions quickly that are essential to meet evolving threat challenges (e.g. timely patches to onboard vehicular software flaws, updates to future data encryption algorithms). The resulting scenario would actually decrease security in automotive electronic control systems;
- A NHTSA mandate to use specific safety design processes standards that are vertically rooted in automotive industry development practices for hardware and software (such as ISO 26262) would overlap and conflict with existing ICT industry security standards (such as ISO 27001) which include processes for the protection of data, regardless of the type of device on which it is stored. Technology neutrality will be critical as drivers are increasingly provided with opportunities to integrate devices with their vehicles and export data from older vehicles to newer models;
- A NHTSA mandate would create U.S.-specific automotive electronics control cybersecurity requirements, which are not realistic given the global nature of both the auto and ICT industries; and

- A NHTSA mandate would signal that the U.S. government believes government mandates and country-specific approaches to automotive cybersecurity are acceptable. This could likely empower other governments—many of which watch U.S. government cybersecurity policies very closely—to similarly enact their own mandates, balkanizing the security standards used in the global market for U.S. automotive and ICT companies. Foreign governments' cybersecurity-related policies and regulations that deviate from global approaches have become a top trade concern of the U.S. ICT industry and U.S. Government. Together, we devote significant resources to trying to roll back such policies in other countries and having the U.S. government set a positive example in terms of avoiding mandates on industry to use particular cybersecurity standards is a key tool in our arsenal.

ITI recommends that NHTSA begins collaborating directly with NIST to understand the risk-based security methodologies used by critical infrastructure sectors (including transportation) and captured in the Cybersecurity Framework. As NIST continues to work on the Framework, NHTSA should engage in providing input directly to complement efforts of automotive and technology industry participants who are using or planning to use the Framework to bolster their own security practices.

We also are concerned with the following specific items:

- ***The reference in question 3a to "metrics" to test a vehicle's ability to withstand a cyber attack.*** Attempting to measure a system's resistance to attacks would require that we focus on specifically identified attacks. Unfortunately, we face a constantly changing and evolving threat landscape in which such focused metrics would not only be meaningless but also detract us from responding to new threats. Cybersecurity risk management is a continual, adaptive, and evolving process, not an end state. Security is a point in time, and measuring "more secure" is not really achievable. The goal is better resilience and better risk management.
- ***The reference in question 3b to "ensuring a minimum level of security."*** Again, giving the constantly changing nature of cyber threats, security cannot be ensured. Risks can be managed and resilience improved.

Electromagnetic Compatibility (EMC)

ITI members also have significant expertise with additional technical areas under consideration. In the area of electromagnetic compatibility (EMC), we support the effort of NHTSA and the automotive industry to provide adequate levels of emissions control and immunity in their electronic systems. While we are not able to offer a detailed response on EMC at this time, we welcome the chance to share our perspective as these questions are further considered.

Conclusion

As the use of electronics—including networked systems—in motor vehicles continues to grow, industry and government stakeholders are contemplating related policy issues, such as cybersecurity and electromagnetic compatibility. We urge the NHTSA to leverage and contribute to existing industry (including ICT industry) and government expertise and work in these areas so that the agency can thoughtfully consider the potential implications of policies related to motor vehicles and work with all stakeholders to come to effective policies.

We hope our comments will receive due consideration. Please consider ITI a resource on these issues moving forward. If you have any questions, do not hesitate to contact me at dkriz@itic.org.

Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy