Hughes Hubbard & Reed

NHTSA Issues Guidance on Connected Cars

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

On Monday, October 23, 2016, the National Highway Traffic Safety Administration ("NHTSA") issued "Cybersecurity Best Practices for Modern Vehicles," a proposed guidance for car manufacturers and suppliers of vehicle systems. The proposed guidance addresses cybersecurity concerns with connected cars and other vehicles with a focus on ensuring that vehicle systems are designed to "take appropriate and safe actions, even when an attack is successful." NHTSA is soliciting public comments on the proposed guidance for 30 days. Following that window, the proposed guidance will take effect, although it will only be voluntary and non-binding on the automotive industry.

The proposed guidance may be found on NHTSA's website: www.nhtsa.gov. We summarize the agency's main recommendations below.

General Cybersecurity Guidance

1. Follow the NIST Standards

NHTSA recommends that the automotive industry follow the National Institute of Standards and Technology's documented Cybersecurity Framework, which is structured around five principal functions: "Identify, Protect, Detect, Respond, and Recover." According to NHTSA, the industry's approach to cybersecurity protections for vehicles should:

- be built upon risk-based prioritized identification and protection of safety-critical vehicle control systems and personally identifiable information;
- provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field;
- design-in methods and measures to facilitate rapid recovery from incidents when they occur; and

- institutionalize methods for accelerated adoption of lessons learned across the industry through effective information sharing, such as through participation in the Automotive Information Sharing and Analysis Center ("Auto ISAC").

2. Adopt Information Technology Security Controls

The proposed guidance recommends that the automotive industry review and consider existing industry standards, such as the ISO 27000 series standards, and other best practices, such as the Center for Internet Security's Critical Security Controls for Effective Cyber Defense ("CIS CSC"). The CIS CSC are based on attack data pulled from various sources. While the controls do not specifically address automotive networks or devices, they may be adopted for the automotive industry. NHTSA suggests that the automotive industry consider the following CIS CSC recommendations:

- performing cybersecurity gap assessments,
- developing implementation roadmaps,
- effectively and systematically executing cybersecurity plans,
- integrating controls into vehicle systems and business operations, and
- reporting and monitoring progress through iterative cycles.

Automotive Industry Cybersecurity Guidance

1. Focus on Cybersecurity in the Vehicle Development Process

The proposed guidance calls on the automotive industry to engineer systems with the goal of making them safe from potential cybersecurity threats and vulnerabilities. Companies are urged to make cybersecurity a priority and to evaluate privacy and cybersecurity risks throughout the entire life cycle of a vehicle: conception, design, manufacture, sale, use, maintenance, resale and decommissioning. The safety of vehicle occupants and other road users should be the primary consideration in assessing cybersecurity risks.

The proposed guidance also encourages the automotive industry to establish rapid detection and remediation capabilities. If a cyber attack is detected, the safety risk to vehicle occupants and surrounding road users should be mitigated and the vehicle should be transitioned to a reasonable risk state.

2. Top-Down Emphasis on Product Cybersecurity

NHTSA recommends that companies prioritize vehicle cybersecurity and demonstrate management commitment to doing so by:

- allocating dedicated resources within the organization focused on researching, investigating, implementing, testing, and validating product cybersecurity measures and vulnerabilities;
- facilitating seamless and direct communication channels through organizational ranks related to product cybersecurity matters; and
- enabling an independent voice for vehicle cybersecurity related considerations within the vehicle safety design process.

NHTSA suggests that companies (i) appoint a high-level corporate officer to be exclusively and directly responsible for product cybersecurity and (ii) provide this executive with appropriate staff, authority and resources.

3. Greater Information Sharing

The proposed guidance stresses information sharing among industry members. It notes that the automotive industry has established the Auto ISAC, which became fully operational on January 19, 2016. While a large number of motor vehicle and equipment manufacturers are involved in the Auto ISAC, NHTSA encourages all members of the vehicle manufacturing industry to participate in it.

4. Implement a Vulnerability Reporting Policy

NHTSA suggests that automotive manufacturers enhance information sharing by implementing cybersecurity vulnerability reporting and disclosure policies. NHTSA envisions that automotive industry members will create their own policies or adopt policies used in other industries. Automotive industry members should make information on vulnerabilities available to cybersecurity researchers so that the information may be shared with other organizations that manufacture or design vehicle systems.

5. Implement an Incident Response Process

The proposed guidance calls on members of the automotive industry to implement a documented process for responding to incidents, vulnerabilities and exploits. This process would cover impact assessment, containment, recovery and remediation actions, as well as associated testing.

NHTSA recommends that industry members report incidents to the Auto ISAC as soon as possible and to the United States Computer Emergency Readiness Team ("US-CERT") in accordance with the US-CERT Federal Incident Notification Guidelines. Industry members may also report incidents to the industrial control systems CERT.

NHTSA further proposes that the automotive industry define metrics to periodically assess the effectiveness of their response processes and document details of each identified and reported vulnerability, exploit or incident. Industry members should periodically run response capability exercises to test the effectiveness of their disclosure policy and internal response processes.

6. Engage In Self-Auditing

In addition to implementing a cybersecurity process based on a sound systems-engineering approach, NHTSA recommends that automotive industry members document the details related to the cybersecurity process to allow for both auditing and accountability. This documentation may include risk assessments, penetration test results and organizational decisions. These documents should be retained throughout the expected life span of the associated product.

Risk Assessments
Risk assessments should consider vulnerabilities and potential impacts throughout the supply chain. At a minimum, organizations should (i) assess cybersecurity risks to safety-critical vehicle control functions and personally identifiable information and (ii) design assessments to cover internal vehicle networks, external wireless networks, and any interface that an electronic control unit presents to the world. To guide their risk assessments, industry members should ask the following questions:

- What are the functions?
- What are the implications if they were compromised?
- What are the potential safety hazards that could be exposed by these vulnerabilities?
- What is the safety risk to society and the value risk to the organization?
- What can be done to minimize exposure to the potential loss or damage?

- What design decisions could be made with respect to the risk assessment process?
- Who/what are the threats and vulnerabilities?

Penetration Testing and Documentation
NHTSA also recommends penetration tests. These tests should be done by qualified testers who have not been part of the development team and are highly incentivized to identify vulnerabilities. With respect to such testing, organizations should maintain written reports that document the disposition of any cybersecurity vulnerabilities.

If a vulnerability is fixed, the details of the fix should to be documented. If a vulnerability is not addressed, the reasoning behind the acceptability of the underlying risk should also be documented.

Self-Review
The automotive industry should establish procedures for internal review and documentation of cybersecurity-related activities. One suggested approach is for members of the automotive industry to produce annual reports on their cybersecurity practices. Among other things, the annual reports could discuss the current state of implemented cybersecurity controls, findings from self-auditing activities, and records maintenance.

7. Fundamental Vehicle Cybersecurity Protections

NHTSA recommends:

- limiting developer/debugging access in production devices and electronic control units;
- protecting and securing keys and passwords;
- limiting access to vehicle maintenance diagnostics;
- controlling access to firmware;
- limiting the ability to modify firmware;
- limiting network ports, protocols and services to essential functionality only;
- using segmentation and isolation techniques in vehicle architecture design;
- controlling internal vehicle communications and safety messages;
- logging cybersecurity events to detect trends in cyber-attacks;
- using encryption to protect communications between the vehicle and external servers; and
- controlling connections to cellular wireless networks.

Additional Recommendations

Education

NHTSA believes that an educated workforce is crucial to improving the cybersecurity posture of motor vehicles. It encourages industry members not to limit cybersecurity educational activities to the current workforce or to technical individuals, but to support activities that will enrich the future workforce and non-technical individuals. NHTSA suggests that manufacturers, suppliers, and other stakeholders work together with NHTSA to help support these educational efforts.

Aftermarket Devices and Serviceability

The proposed guidance also addresses third parties, such as aftermarket device manufacturers and third-party service providers. Consumers may bring aftermarket devices (e.g., insurance dongles) and personal equipment (e.g., cell phones) into cars and connect them with vehicle systems through manufacturer-provided interfaces

(Bluetooth, USB, OBD-II port, etc.). Both the automotive industry and the aftermarket device manufacturers therefore need to consider the risks presented by these devices and provide reasonable protections.

NHTSA also recommends that the automotive industry consider the serviceability of vehicle components and systems by individuals and third parties. It encourages the automotive industry to provide strong vehicle cybersecurity protections that do not unduly restrict access by authorized third-party repair services.

Related People

Seth D. Rothman

Tyler Grove

Related Areas of Focus

Data Privacy & Cybersecurity