PRIVACY AND DATA SECURITY ALERT

OCTOBER 25, 2016

SHOOK
HARDY & BACON

KEY TAKEAWAYS FROM NHTSA'S PROPOSED GUIDANCE ON CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES

The National Highway Traffic Safety Administration (NHTSA) recently issued proposed guidance titled *Cybersecurity Best Practices for Modern Vehicles* based on public feedback collected by NHTSA in addition to the National Institute of Standards and Technology's (NIST's) Framework for Improving Critical Infrastructure Cybersecurity. Key takeaways from the guidance include:

1. Consider cybersecurity in the vehicle development process.

NHTSA emphasizes the importance of making cybersecurity a priority through an ongoing process of risk evaluation. It recommends the auto industry:

- Use guidance, best practices and design principles derived from NIST, NHTSA, industry associations, and Auto ISAC, and consider adopting SAE International's J3061 Recommended Practice *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*.
- Identify risks, analyze potential threats, and establish rapid detection and remediation capabilities.
- Collect information on any potential attack that may be analyzed and shared with industry through Auto ISAC.
- Fully document any actions, changes, design choices, and analyses.

2. Prioritize leadership on product cybersecurity.

NHTSA recommends companies appoint a high-level corporate officer to be responsible for product cybersecurity. The agency believes a top-down approach demonstrates the seriousness of managing cybersecurity risks and engendering a proactive culture in which cybersecurity protections are considered early in the design phases of product development cycles.

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Mayela Montenegro
dd 949.975.1741
mmontenegro@shb.com

Doug Robinson
dd 949.975.1725
dwrobinson@shb.com

Al Saikali
dd 305.960.6923
asaikali@shb.com

To show their commitment to cybersecurity, companies can take the following actions:

- Allocate resources focused on researching, investigating, implementing, testing, and validating product cybersecurity measures and vulnerabilities.
- Facilitate direct communication channels through organizational ranks.
- Enable an independent voice for cybersecurity considerations within the vehicle safety design process.

3. Share information.

NHTSA encourages private companies, nonprofit organizations, executive departments, agencies, and other entities to share information regarding cybersecurity risks and incidents, and to collaborate. NHTSA also advocates membership in the Auto ISAC.

4. Create a vulnerability reporting/disclosure policy.

NHTSA advises companies to create their own vulnerability reporting/disclosure policies. Such policies would provide any external cybersecurity researcher with guidance on how to disclose vulnerabilities to the organization.

5. Develop a vulnerability/exploit/incident response process.

NHTSA advises the automotive industry to develop a documented process for responding to incidents, vulnerabilities and exploits. This process would involve the following:

- Outline roles and responsibilities for each responsible group within the organization to ensure a rapid response.
- Define metrics to assess the effectiveness of the response process.
- Report all incidents, exploits and vulnerabilities to the Auto ISAC.
- Periodically run response capability exercises to test the effectiveness of the disclosure policy operations and internal response processes.

6. Conduct self-audits.

NHTSA recommends that the automotive industry document the details related to the cybersecurity process for both auditing and accountability. Such documentation may include risk assessments, penetration test results and organizational decisions. Additionally, it advises industry to:

- Develop and use a risk-based approach to assess vulnerabilities and potential impacts that consider the entire supply chain of operations.
- Use penetration tests where qualified testers are deployed to identify vulnerabilities.
- Establish procedures for internal review and documentation of cybersecurity-related activities, such as producing an annual report on the state of cybersecurity practices.

7. Implement fundamental vehicle cybersecurity protections.

Lastly, NHTSA recommends a series of actions to move toward a more cyber-aware posture:

- *Limit developer/debugging access in production devices:* Control developer access to an electronic control unit (ECU) for deployed units by eliminating access or limiting to authorized privileged users.
- *Control keys:* Protect from disclosure keys or password providing unauthorized, elevated level of access to vehicle computing platforms.
- *Control vehicle maintenance diagnostic access:* Limit diagnostic features to a specific mode of vehicle operation.
- *Control access to firmware:* Consider encryption as a useful tool to prevent unauthorized recovery and analysis of firmware.
- *Limit ability to modify firmware:* This would make it more challenging for malware to be installed on the vehicles and firmware updating systems.
- *Control proliferation of network ports, protocols and services:* Limit the use of network servers on vehicle ECUs to essential functionality.

- *Use segmentation and isolation techniques in vehicle architecture design:* Use logical and physical isolation techniques to separate processors, vehicle networks, and external connections to limit and control pathways from external threat vectors to cyber-physical features of vehicles.
- *Control internal vehicle communications:* Avoid sending safety signals as messages on common data buses.
- *Log events:* Maintain a log of events concerning cybersecurity attacks or successful breaches; any such log should be scrutinized periodically to detect trends of cyber-attack.
- *Control communication to back-end servers:* Employ widely accepted encryption methods in any IP-based operational communication between external servers and the vehicle.
- *Control wireless interfaces:* Industry should plan for and design-in features that could allow for changes in network routing rules to be quickly propagated and applied to one, a subset or all vehicles.

The agency is accepting public comments on the proposed guidance until November 28, 2016.