crowell moring

CLIENT ALERT

NHTSA Proposes Cybersecurity Best Practices for Automakers

Nov.01.2016

On Monday, October 24, the National Highway Traffic Safety Administration (NHTSA) proposed a set of voluntary cybersecurity best practices for manufacturers and designers of vehicle systems and software. Consistent with its July 2015 discussion of vehicle cybersecurity, NHTSA's proposals focus on hardening system architecture to reduce the overall risk of attacks and designing safeguards to permit safe and appropriate vehicle action should attacks succeed. Utilizing a deliberately flexible approach to address "cybersecurity vulnerabilities [that] could impact safety of life," NHTSA calls for vehicle stakeholders to make cybersecurity "an organizational priority" and to develop a "risk-based approach" to confront dynamic cybersecurity threats.

Key Recommendations

By and large, NHTSA's proposed best practices build on pre-existing standards. Central is the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which has already been widely accepted by public and private sector entities, including the Federal Trade Commission. The Framework employs an iterative and flexible approach to cybersecurity, focusing on the core principles of Identify, Protect, Detect, Respond, and Recover. NHTSA recommends that industry also adopt other widely accepted cybersecurity standards and practices, such as the ISO 27000 series, the Center for Internet Security (CIS) Critical Security Controls, security-by-design principles, and information-sharing through the Auto ISAC.

Among NHTSA's more specific recommendations, it urges that vehicle stakeholders:

- Tightly control software developers' post-sale access to onboard technology.
- Protect cryptographic and password keys used to access or diagnose vehicle electronic systems by enabling them each to access a single vehicle, not multiple vehicles.
- Limit internal and external ability to access diagnostic tools, or access and modify firmware, including by restricting the functionality that can be affected.
- Minimize and safeguard communications to back-end servers, communications between vehicle systems, and the vehicle's connection to wireless networks, including through use of message authentication and encryption when appropriate.
- Isolate and segment processors, networks, and external connectors, and minimize unnecessary network services.
- Maintain an "immutable log of events" to support threat assessment and to permit reconstruction of events and analysis of flaws if a breach occurs.
- Enact self-auditing programs that include periodic risk assessments, rigorous cybersecurity testing, and regular self-review.
- Anticipate and address cybersecurity issues associated with aftermarket devices and components.

- Protect serviceability and consumer choice by avoiding cybersecurity protections that "unduly restrict access by authorized alternative third-party repair services."

Legal Significance

The just-released NHTSA guidance is non-binding. It does, however, suggest that NHTSA may eventually utilize its safety mandate "to cover vehicle cybersecurity," even though no binding safety standards yet exist. Recent enforcement actions in other contexts demonstrate that best practices can become enforceable – for example, by the FTC with regard to the NIST Cybersecurity Framework, or by the California Attorney General with regard to the CIS Critical Security Controls. NHTSA's principles may also foreshadow regulatory or legislative action to come.

Still, few of the cybersecurity principles announced by NHTSA's proposed guidance are novel. Many are contained within existing best practices documents like the Auto Alliance's Cybersecurity Best Practices and the Society of Automotive Engineers' Cybersecurity Guidebook. NHTSA's guidance in essence encourages the continued development and implementation of these self-governing standards.

Broader Context

NHTSA's guidance comes in the midst of the agency's regulatory push in the cybersecurity arena. Just weeks ago, the agency issued its Federal A.V. Policy, which contained extensive cybersecurity directives tailored to highly automated vehicles. NHTSA urged Congress in January 2016 to enact heightened safety standards for motor vehicles equipped with onboard electronic systems. And in the summer of 2015, the agency ordered the recall of more than 1.4 million vehicles after two researchers wirelessly hacked into a dashboard connectivity system.

The guidance also comes after cyber hacking has gained momentum in the legal world with recent hackability suits across many industries. In the same vein, the National Conference of State Legislatures has noted that at least 26 states have considered cybersecurity legislation so far in 2016.

Conclusion

This NHTSA guidance represents the agency's latest foray into the regulation of cybersecurity standards for the auto industry. It pushes principles that for many are already best practices and continues the trend toward harmonizing federal agency interpretations of reasonable cybersecurity practices around well-established principles. While non-binding, future regulatory, legislative, or enforcement actions may transform NHTSA's proposed best practices into requirements.

To read this Guidance in its entirety, visit this link. NHTSA will be accepting comments regarding its proposed cybersecurity best practices until November 28, 2016.

Our team welcomes the opportunity to discuss NHTSA's guidance in further detail.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Scott L. Winkelman
Partner – Washington, D.C.
Phone: +1 202.624.2972
Email: swinkelman@crowell.com

Danielle Rowan
Associate – Washington, D.C.
Phone: +1 202.624.2681
Email: drowan@crowell.com

Justin Kingsolver
Associate – Washington, D.C.
Phone: +1 202.624.2927
Email: jkingsolver@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com