WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

CTIA’s IoT Cybersecurity Certification Program May Inform the Future of Transportation and Smart Cities

September 19, 2018

AUTHORS

Renee R. Gregory | Jill Guidera Brown

Background

In late August 2018, CTIA, the trade association representing the U.S. wireless communications industry, released its Cybersecurity Certification Test Plan for IoT Devices (“Test Plan”), establishing a baseline for device security on wireless networks. The Test Plan is unique in that its testing requirements and plans were developed specifically for, and in collaboration with, nationwide wireless providers. Specifically, the Test Plan defines testing requirements for the CTIA Cybersecurity Certification Program for managed Internet of Things (“IoT”) devices connecting to either LTE or Wi-Fi networks to exchange data with other devices, vehicles, home appliances, infrastructure elements, and more. CTIA-authorized test labs will begin accepting devices for testing in October 2018.

Proponents of connected and self-driving cars and smart cities should take note of the Certification Program as they increasingly integrate LTE and Wi-Fi and participate in the larger IoT ecosystem.

The CTIA Cybersecurity Certification Program Draws From Existing Cybersecurity Frameworks

The Test Plan draws from and adapts existing cybersecurity frameworks, and each testing procedure is accompanied by reference to relevant sections of existing standards, most notably the National Institute of Standards and Technology (“NIST”) Cybersecurity Framework. Recognizing the need for a tailored approach to cybersecurity, NIST itself identifies that its framework is “not a one-size-fits-all approach to managing cybersecurity risk.” While the Test Plan highlights existing standards, CTIA-authorized test labs will develop the specific testing procedures and equipment in accordance with program-specific requirements set forth by CTIA.

The Test Plan is organized into three categories of testing, moving from core IoT device security features in the first category, to security elements of increasing device complexity, sophistication and manageability in the second and third categories:

Category 1:

- Terms of service and privacy policies
- Password management
- Authentication
- Access controls
- Patch management
- Software upgrades

Category 2:

- Audit log
- Multi-factor authentication
- Remote deactivation
- Secure boot
- Threat monitoring
- IoT device identity

Category 3:

- Encryption of data at rest
- Digital signature generation and validation
- Tamper evidence
- Design-in features

Future Developments in Transportation and Smart Cities May Put the Wireless Industry in the Driver's Seat

Similarly to any device connected to the internet, connected and self-driving cars and smart city devices are vulnerable to malicious attacks and human error, raising significant public safety concerns and legal risk. For example, in 2015 researchers were able to exploit vulnerabilities in a vehicle's infotainment system and remotely control the driving and safety functionalities of the car on the road. As a result, in July 2018 the U.S. District Court for the Southern District of Illinois certified a class of consumers in a suit against the same auto manufacturer for cybersecurity defects in cars' cellular connections.

To combat those risks, local governments, automotive manufacturers and suppliers, and wireless communications industry leaders may turn collectively to the CTIA Cybersecurity Certification Program as a roadmap for building secure systems from the ground up. The program could supplement or even replace existing non-binding guidance documents and voluntary consensus standards, described below, that address security concerns inherent in the deployment of smart cities, connected cars, and automated driving systems. Measured against these various approaches to standardizing transportation and smart city-related IoT, the CTIA Cybersecurity Certification Program is unique not only because it was developed from the perspective of the wireless communications industry that enables IoT connectivity, but also because it puts cybersecurity front and center in developing new IoT technologies and applications.

Smart cities

Recognizing a need for a more cohesive framework for implementation of smart city technologies, which naturally take a city-by-city approach, NIST formed a working group of academics and policymakers and in early 2018 published a draft Consensus Framework for Smart Cities Architectures. This framework considers cybersecurity challenges in the context of open data policies, interoperability, and standardization across smart city systems.

Connected cars

Development of security and connectivity standards for connected cars has been largely driven by the automotive industry in partnership with engineers and transportation policy makers, assuming a transportation-specific standard for vehicle-to-vehicle ("V2V") and vehicle-to-infrastructure ("V2I") communications: Dedicated Short Range Communications ("DSRC"). For instance, the U.S. Department of Transportation's Intelligent Transportation Systems Joint Program Office and the National Highway Traffic Safety Administration ("NHTSA") have collaborated with technology and automotive industry stakeholders such as the Society of Automotive Engineers International ("SAE") and the Institute of Electrical and Electronics Engineers to develop connected vehicle standards based on DSRC. However, the wireless industry has recently developed a cellular-based vehicle-to-everything ("V2X") standard that may replace DSRC.

Autonomous vehicles

While no overarching federal law governing autonomous vehicles exists today, the U.S. House of Representatives has passed, and the Senate has proposed, self-driving vehicles legislation that would impose on manufacturers an obligation to maintain a written cybersecurity plan.

In parallel, in September 2017, the U.S. Department of Transportation (“DOT”) and NHTSA issued Automated Driving Systems 2.0: A Vision for Safety, voluntary guidance for stakeholders implementing automated driving systems. The voluntary DOT/NHTSA guidance does not prescribe specific technical or operational data security measures, though it generally encourages entities to implement cybersecurity protections. In particular, the guidance recommends that entities undergo regular assessment of cybersecurity risks consistent with best practices set forth by NIST, NHTSA, SAE, and “other relevant organizations”– a list to which CTIA may now be added.

***

The enhanced cybersecurity risks raised by connected and self-driving cars and smart city infrastructure highlight the need for cybersecurity standards specifically tailored to IoT devices. Additionally, as next-generation transportation and smart cities both are undergoing a period of rapid growth and development, there is now a unique opportunity to consider cybersecurity starting in the design phase. When taken in combination with existing legal and regulatory frameworks and industry best practices, the CTIA Cybersecurity Certification Program may provide helpful guidance for stakeholders as they develop smart, secure, and connected communities and transportation systems.

If you have any questions regarding this client alert, please contact the following attorneys or the attorney with whom you regularly work.

Renee R. Gregory
202 303 1104
rgregory@willkie.com

Jill Guidera Brown
202 303 1217
jgbrown@willkie.com

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.