



DAILY NEWS

# Automakers expected to move on cybersecurity controls that exceed regulator expectations

August 25, 2016 | **Joshua Higgins**

It is unlikely automotive industry regulators will mandate cybersecurity controls more rigorous than those currently being developed and deployed by the private sector, according to an industry source, despite moves by regulators to potentially halt deployment of some technologies until cybersecurity plans are in place.

“[Original Equipment Manufacturers] have a lot to lose by not addressing [cybersecurity],” said Monique Lance of Argus Cyber Security, one of the top cybersecurity companies working with the auto industry. “They have so much at stake.”

Lance told *Inside Cybersecurity* that automakers aren't waiting for regulations to emerge because they want to be able to deploy revolutionary safety and consumer features – and autonomous vehicles – and know that cybersecurity is critical to the success of these new products.

“We're working with them to enable them to address and to protect the future of automobiles,” Lance said.

Though regulation of cybersecurity in the auto industry is top of mind among industry stakeholders as the Federal Communications Commission **considers a proposal** halting deployment of auto communications technologies until cybersecurity plans have been developed and approved, Lance said it is unlikely that regulators will raise the bar higher than automakers' own bar for themselves on cybersecurity, citing a need for a team effort to address auto security and privacy.

“It's about everyone banding together to make sure we can enjoy this connectivity revolution,” Lance said.

Regulators will play an important role to “bond and seal” the best practices and standards developed by industry, mandating that all auto manufacturers implement at the very least the industry-accepted best practices in securing their products, Lance said.

The National Highway Traffic Safety Administration, which has taken the lead on most cyber issues in the sector, has **pledged to work collaboratively** with the automakers on cyber, stressing that forthcoming cybersecurity guidance from NHTSA will be consistent with best practices put out by industry this summer.

The guide was not “created in a vacuum,” said Transportation Secretary Anthony Foxx during an automotive cybersecurity summit in Detroit last month.

“We hope that our guidance will break new ground on how we address cybersecurity,” Foxx said.

Leaders of the industry group that developed the recently released industry best practices have agreed that NHTSA's approach to security thus far has complemented the industry's approach.

“We need to lift the industry together,” said Jonathan Allen, director of the auto industry's information sharing and analysis center. “This industry has not yet had a catastrophic event. They're trying to get out in front of it.”

Foxx applauded the work industry has done so far, stressing industry's own vested interest in protecting its technology and data from hackers.

“Ultimately it is in the interest of industry for the consumer to have confidence that the information they are generating is being protected and they have control over it,” Foxx said.

NHTSA has given no indication of interest in developing regulations for cybersecurity thus far. However, the FCC Wednesday ended a public comment period on a petition to stop deployment of “dedicated short range communications” technology until automakers offer the regulator a plan to secure the automotive devices connected to the DSRC network from cyber attacks. – *Joshua Higgins (jhiggins@iwpnews.com)*

5310

---

## RELATED NEWS

- **Senior Commerce official cites 'high-level interest' in regulatory alignment**
  - **Cyber commission urged to endorse non-regulatory approach to securing data**
  - **FCC members review plan for cyber 'assurance meetings' with industry**
  - **FCC cyber chief optimistic on prospects for confidential 'assurance meetings' with industry**
  - **FTC's Ramirez calls for legislation shoring up security, privacy of Internet of Things**
  - **New FCC proposal requires cybersecurity plans for use of 5G spectrum**
  - **Role of FTC emerges as key sticking point in debate over FCC privacy rules**
-

## **FEATURES**

**Daily News**

**Cyber Reg Watch**

**Documents**

**The Editor Reports**

**Sector Initiatives**

**Weekly Analysis**

**Special Reports**

## **ABOUT**

**About Us**

**Privacy Policy**

**Terms and Conditions**

## **TOPICS**

**Congress**

**Cyber Physical**

**Data-Breach**

**Deterrence**

**Election 2016**

**Framework**

**Information Technology**

**Info-Sharing**

**Insurance**

**International**

**Internet Of Things**

Inside Cybersecurity is a subscription-based premium news service for policy professionals who need to know about evolving federal policies to protect cyberspace.

## **CONTACT US**

✉ [cybersecurity@iwpnews.com](mailto:cybersecurity@iwpnews.com)

☎ 703-416-8500

**Follow us on Twitter**

