Gov't: Cybersecurity should be part of auto design process

October 24 2016

The government's highway safety agency says automakers should make cybersecurity part of their product development process by assessing risks and designing in protections.

Companies also should identify safety critical systems such as engine control computers and limit their exposure to attacks, under best practice guidelines released Monday by the National Highway Traffic Safety Administration.

The agency also wants automakers to limit access to car owners' personal data.

The guidelines aren't requirements but will go into effect after a 30-day public comment period.

"Our intention with today's guidance is to provide best practices to help protect against breaches and other security failures," said Transportation Secretary Anthony Foxx, who oversees NHTSA.

Many of the recommendations focus on computer software written to get engines to perform. The agency suggests that companies control who has access to firmware, the software that runs car computers, and limit the ability to modify it to thwart malware. The agency also recommends use of whole disk encryption to prevent unauthorized analysis of the software.

Automakers also should make plans to detect cyberattacks and respond rapidly to limit them.

The auto industry already is doing most of the recommendations and has set up its own best practices and information-sharing methods.