NHTSA Updates Cybersecurity Best Practices for New Vehicles

Guidance builds upon research, learnings and progress since 2016

September 7, 2022 | Washington, DC

The U.S. Department of Transportation's National Highway Traffic Safety Administration released *Cybersecurity Best Practices for the Safety of Modern Vehicles*, an update to its 2016 edition. The document describes NHTSA's guidance to the automotive industry for improving vehicle cybersecurity for safety.

"As vehicle technology and connectivity develop, cybersecurity needs to be a top priority for every automaker, developer, and operator," said Dr. Steven Cliff, NHTSA's Administrator. "NHTSA is committed to the safety of vehicles on our nation's roads, and these updated best practices will provide the industry with important tools to protect Americans against cybersecurity risks."

The 2022 Cybersecurity Best Practices leverage agency research, industry voluntary standards, and learnings from the motor vehicle cybersecurity research over the past several years, and is updated based on public comments received on the draft that was published in the Federal Register in 2021. Though the document is non-binding, it contains important best practices that will influence the industry going forward.

NHTSA routinely assesses cybersecurity risks as well as emerging best practices and will consider future updates to these best practices as motor vehicles, motor vehicle equipment, and their cybersecurity evolve.

For more on NHTSA's cybersecurity work, please visit our website.

Contact:

NHTSA

NHTSA Media

NHTSAmedia@dot.gov

202-366-9550