ALLIANCE FOR AUTOMOTIVE INNOVATION

Securing the Future of Personal Mobility

The Auto Industry's Approach to Cybersecurity

Technologies that are transforming personal mobility – including connectivity, electrification, and automation – are driving us towards a cleaner, safer, and smarter transportation future. These innovations have the potential to bring profound benefits to consumers, the economy, the environment, and society, but they also introduce new cybersecurity challenges. The integration of vehicles into a broader ecosystem of connected infrastructure, devices, features, and stakeholders also involves a number of factors outside the control of the auto industry. Securing the entire motor vehicle ecosystem is crucial to realizing the benefits of automotive innovation. The auto industry is doing its part by proactively building cybersecurity into its products and services.

RISK MANAGEMENT

Government agencies, various industry sectors, academia, and other stakeholders have acknowledged that cybersecurity risk cannot be eliminated, only managed and mitigated. Building on its expertise in managing safety-related risk, the auto industry has actively adapted well-respected cybersecurity risk management frameworks from other contexts and industries, such as the National Institute of Standards and Technology ("NIST") Cybersecurity Framework. Such adaptation has facilitated industry-specific resources and standards to address the unique challenges and complexities of securing the motor vehicle ecosystem in this increasingly digital and connected world.

STANDARDS AND BEST PRACTICES

The auto industry continues to leverage various cybersecurity standards and best practice resources.

- **GLOBAL STANDARD:** In 2021, the two largest standards bodies for the auto industry – ISO and SAE – finalized a single, global standard for vehicle cybersecurity. This novel multi-year effort brought together more than 100 experts from 17 countries, spanning a diverse group of over 80 public and private sector organizations. ISO/SAE 21434 provides the industry with robust processes and procedures to manage cybersecurity risk throughout the lifecycle of the vehicle – from design through decommissioning.

- **BEST PRACTICE GUIDES:** Working through the Auto-ISAC, the auto industry developed seven robust Automotive Cybersecurity Best Practice guides to assist automotive ecosystem partners to identify, monitor, prioritize, assess, and respond to vehicle cybersecurity risks.

- **NHTSA GUIDANCE:** In 2016, following input from industry, security researchers, and other stakeholders, the National Highway Traffic Safety Administration ("NHTSA") released its Cybersecurity Best Practices for Modern Vehicles. Building on industry and agency progress since 2016, NHTSA released a draft update of these Best Practices in late 2020.