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 toward 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 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 Automotive Information Sharing and Analysis Center ("Auto-ISAC"), the auto industry developed seven robust Automotive Cybersecurity Best Practice guides to assist automotive ecosystem partners in identifying, monitoring, prioritizing, assessing, and responding 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.

COLLABORATION AND PARTNERSHIPS

As part of its proactive cybersecurity efforts, the auto industry maintains important collaborations with key stakeholders.

Public Sector Partnerships: The auto industry has active public-private partnerships with:

- U.S. Department of Transportation and NHTSA
- U.S. Department of Homeland Security ("DHS") and its Science and Technology Directorate
- U.S. Department of Commerce, NIST, and the National Telecommunications and Information Administration
- U.S. Department of Energy

These collaborations have led to efforts to (a) develop an auto industry software bill of materials ("SBOM") proof of concept; (b) collaborate on advanced technology workforce development and certification; and (c) conduct forward-looking research and development.

Auto-ISAC: In 2015, the Auto-ISAC was created. Proactively partnering with DHS and leveraging organizational principles from similar sector-specific information sharing programs, the Auto-ISAC now includes over 60 members, representing a broad range of industry stakeholders.

Security Researchers: Security researchers are instrumental in helping the auto industry proactively identify cyber threats and vulnerabilities before they are exploited. Their expertise helps inform the drafting of security safeguards, tools, and operating procedures. The industry engages security researchers to test and evaluate product security, including through vulnerability disclosure and bug bounty programs.

DID YOU KNOW?
NHTSA is the federal entity responsible for motor vehicle safety regulation and enforcement. Through its Safety Act (49 U.S.C. 30101 et seq.) authority, NHTSA has ordered vehicle recalls due to cybersecurity vulnerabilities that pose risks to safety.

LOOKING AHEAD

Remaining nimble and adaptive in the face of a rapidly, dynamic cybersecurity threat environment is paramount for the auto industry. The growing digital and connected ecosystem introduces several complexities and cybersecurity risks that are no longer confined to the vehicle itself or controlled solely by the auto industry.

The relationship among vehicles, connected infrastructure, products, and services, as well as with consumers, is fueling automotive innovation, and, thus, cybersecurity must remain at the core. Consumer trust and our cleaner, safer, and smarter transportation future depend on it.