AUTO ALLIANCE
DRIVING INNOVATION®

GlobalAutomakers

# Framework for Automotive Cybersecurity Best Practices

## I. INTRODUCTION

The automobile industry is currently undergoing an unprecedented wave of innovation, as automakers are pioneering groundbreaking technologies that are making cars and trucks safer than ever before. But the industry is also presented with emerging challenges in the area of cybersecurity. The members of the Alliance of Automobile Manufacturers ("Auto Alliance") and the Association of Global Automakers ("Global Automakers") believe that by proactively and collaboratively addressing potential cybersecurity challenges the industry can continue producing safe vehicles that incorporate modern and robust security protections.

The members are committed to this proactive approach, and in advance of material real-world threats, announced the formation of an Automotive Information Sharing and Analysis Center (Auto-ISAC) in the summer of 2015.

The Auto-ISAC initiative was preceded by the establishment of Consumer Privacy Protection Principles for Vehicle Technologies and Services in 2014, which are among the first and most comprehensive commitments to consumer data privacy in the Internet of Things sectors.

Likewise, the auto industry is not waiting for cyber threats[1] to metastasize into safety risks within the automotive world before addressing resilience methods. Our members have come together once again to identify industry best practices for vehicle cybersecurity.

To support our commitment to enhancing cybersecurity, the members of the Auto Alliance and Global Automakers have developed this Framework for Automotive Cybersecurity Best Practices ("Framework"). This Framework can serve as the foundation for the development of voluntary industry-wide Automotive Cybersecurity Best Practices ("Best Practices").

The Framework is intended to support the ongoing efforts of the automobile industry on cybersecurity matters. The Framework draws upon established cybersecurity frameworks

[1] For the purposes of this document the term "cyber threat/s" has been retained from the National Institute of Standards and Technology's *Glossary of Key Information Security Terms 2013 2nd Revision*, and is meant to apply to automobiles. The *Glossary* defines cyber threats as: "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."

as well as upon existing cybersecurity measures that have already been implemented by many automakers. The Framework centers on the following overarching and guiding principles:

1) Vehicle security by design.
2) Risk assessment and management.
3) Threat detection and protection.
4) Incident response.
5) Collaboration and engagement with appropriate third parties.

The Best Practices will expand upon these five guiding principles and provide tools for industry members as they refine their threat awareness, detection, prevention, protection, mitigation and response measures. The Best Practices are also intended to be flexible in the face of the rapidly evolving cybersecurity landscape, as well as to permit implementation in a manner consistent with the unique needs and circumstances of individual companies.

The members of the Auto Alliance and Global Automakers recognize that cyber threats exist in nearly every sector of the economy, and will likely continue to grow. This Framework and the forthcoming Best Practices will help further increase industry preparedness as cybersecurity threats emerge.

## II. FRAMEWORK FOR AUTOMOTIVE CYBERSECURITY BEST PRACTICES

Software- and hardware-based technologies in vehicles provide important safety and environmental benefits, in addition to enhancing the overall driving experience. The members of the Auto Alliance and Global Automakers recognize that it is important to provide cybersecurity for these systems so that consumers can benefit from innovative safety and environmental technologies, as well as from the features and services that they desire. While individual manufacturers have already made great strides in the area of cybersecurity, the members of the Auto Alliance and Global Automakers have developed this Framework in order to further enhance and complement those efforts.

The Best Practices Framework can help guide the development and refinement of industry-wide Automotive Cybersecurity Best Practices. This Framework is inspired by the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[2], SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (currently in draft format), and other cybersecurity models. This Framework also reflects engagement within the automotive industry and with other relevant stakeholders. Members of the Auto Alliance and Global Automakers intend to continue this collaboration in the development and refinement of the Best Practices contemplated by the Framework.

The use of the Framework and the forthcoming Best Practices will be a voluntary member decision made independently by each automaker.

Neither the Framework, nor the Best Practices, is intended to replace applicable laws and regulations, where they exist. Therefore, the documents should be interpreted as subject to and superseded by applicable laws and regulations.

### *The Cybersecurity Best Practices Framework*

The objective of the Framework and the forthcoming Automotive Cybersecurity Best Practices is the safety and security of the overall vehicle ecosystem. Protecting safety-critical systems and our customers' identifiable personal data are of course of paramount importance. To that end, automotive engineers already have developed a substantial number of cybersecurity measures, including implementing security techniques to help defend against unauthorized access to systems and unauthorized modification of

[2] The Auto Alliance and Global Automakers recognize that the NIST Framework for Improving Critical Infrastructure Cybersecurity was designed to address critical infrastructure systems, not consumer products. That being said, it is our intent that the Best Practices will address the aforementioned five guiding principles as they would apply to specific issues of motor vehicle cybersecurity. Specifically, the Best Practices will be available as tools that guide automobile manufacturers as they (a) *identify* cybersecurity threats as well as vehicle components and associated networks that should be protected from cyber threats, (b) *protect* motor vehicles, drivers and their passengers from such threats, (c) timely *detect* cyber incidents, (d) develop mechanisms to *respond* to cybersecurity threats, and (e) develop strategies to *recover* from cyber attacks.

software, and collaborating through organizations such as SAE International to evaluate challenges and technical solutions for cybersecurity concerns.

The forthcoming Best Practices will build on these measures to further the industry's core commitments to safety and data security in the motor vehicle ecosystem. The Best Practices aim to address cybersecurity measures in automotive systems that will help defend against unauthorized electronic access to the vehicle, and protect the operation of systems critical to vehicle safety.

The Best Practices will also address measures in automotive systems that should help secure identifiable personal data and other sensitive information in vehicles and vehicle-related information systems.

This section describes the Framework for Automotive Cybersecurity Best Practices that shapes the development and maturation of Automotive Cybersecurity Best Practices by the members of the Auto Alliance and Global Automakers to help mitigate the risk of unauthorized and unlawful access to vehicle systems. The Framework is comprised of the following:

**1) Vehicle security by design.**

It is important to consider cybersecurity during the design and development of vehicle technologies and services. The automotive industry is already incorporating security into the vehicle development process, including by designing security features into hardware as protective functions for vehicle control system and communications-based functions like navigation satellite radio, and telematics, and using "threat modeling" as a design process to both test systems for vulnerabilities and simulate attacks to test security and design controls.
The members of the Alliance and Global Automakers intend to build on these existing security-by-design processes in the Best Practices. As discussed above, providing both automotive safety and data security entails security by design (e.g. designing security features into the hardware and software of a motor vehicle). Security by design requires an understanding of the threat landscape so that potential cybersecurity threats can be anticipated, and protections against such threats can be built into the vehicle's software programs and hardware components.

**2) Risk assessment and management.**

Risk assessment and management strategies can help assess the potential impact of identified cybersecurity risks and discovered vulnerabilities, and assist in the development of protective measures.

Risk assessment is important for identifying vulnerabilities and understanding the possible consequences to persons or property should these vulnerabilities be exploited. Cybersecurity risks can be catalogued and tiered based upon known vulnerabilities, the extent to which such vulnerabilities may be exploited, and the severity of the potential consequences of a real world event. This process allows for prioritization of internal resources to appropriately address cybersecurity vulnerabilities.

The forthcoming Best Practices will consider processes for the identification of potential cybersecurity threat vectors to motor vehicles. Identified vulnerabilities can be compared to other vulnerabilities identified both internally and externally, including through consultation with the Auto-ISAC and other industry stakeholders.

**3) Threat detection and protection.**

A key cybersecurity premise is that the threat landscape continually evolves and sophisticated attacks are designed to circumvent even the most robust and well-designed defense system.

Accordingly, the development of capabilities to detect cyber incidents, protect against cyber attacks, and mitigate the consequences of a successful cyber incident is an important goal. This principle complements defenses obtained through security by design that are intended to stop cyber attacks before they impact a system. The Best Practices will reflect that these capabilities must also be carefully designed to both protect critical vehicle systems functionality and respond in ways that do not interfere with vehicle safety.

Intrusion detection and mitigation capabilities also apply to third parties, such as suppliers, dealers, repair partners, and others in the vehicle ecosystem. Those entities, while not directly under the control of automobile manufacturers, may represent channels by which cyber-attackers can penetrate vehicles or manufacturer systems. The Best Practices will include strategies for engaging with tier one suppliers, manufacturers of aftermarket devices, and service centers to increase awareness that their services and parts could present cybersecurity vulnerabilities.

**4) Incident response and recovery.**

An incident response plan documents processes used to help respond to cybersecurity incidents affecting the motor vehicle ecosystem. A comprehensive response plan that develops increased awareness and capabilities and that establishes communications protocols between automotive manufacturers, suppliers, cybersecurity researchers, and government agencies could assist

industry stakeholders in coordinated efforts to address discovered vulnerabilities and enhance product security.

The forthcoming Best Practices aim to address incident response plans that may include processes to activate response teams, notify an internal chain-of-command, and trigger response activities to assess and counter cyber attacks. A comprehensive incident response plan provides strategic flexibility for managing many types of cyber incidents and takes into account internal resources and, where appropriate, external resources likely needed to support incident response measures.

The development of protocols for recovering from cybersecurity incidents is also important for ensuring consistent approaches for making available updates to vehicles in a reliable and expeditious manner based on specific circumstances.

**5) Collaboration and engagement with appropriate third parties.**

Defending against cyber attacks often requires collaborative engagement between multiple stakeholders. There are benefits to building partnerships across the vehicle ecosystem, including sharing of cyber threat trends and proven techniques with third parties to defend against cyber attacks.

The Best Practices will continue the commitment of members of the Auto Alliance and Global Automakers to engage with third parties, including peer organizations, suppliers, cybersecurity researchers, government agencies and the Auto-ISAC. This will include working with suppliers to ensure the appropriate utilization of cybersecurity measures, and maintaining clear communication channels. The Auto Alliance and Global Automakers members will work to advance Best Practices related to coordinated vulnerability research disclosures.

## III. AUTOMOTIVE INDUSTRY BEST PRACTICES DEVELOPMENT APPROACH

The Auto Alliance and Global Automakers members have developed a joint Association Working Group to develop and coordinate the scope and content of the Best Practices document(s), and the Working Group is meeting regularly to ensure that progress is being made toward these goals and objectives. The following section outlines the specific activities that members of the Alliance and Global Automakers will continue to engage in to build upon the concepts outlined in this Best Practices Framework.

- **Continued Review of Existing Best Practices.** The intent of this effort is to develop an informed consensus around certain existing best practices that could either be adopted or adapted for use by the automotive industry in addition to those already being incorporated as part of the product development cycle. The Working Group will continue to review existing cybersecurity best practices that

may be applicable to the automotive industry and will monitor new best practices as they are released. This effort is designed to minimize the potential for duplicative or conflicting cybersecurity practices, both within the automotive industry and across industry sectors.

- **Priority Issue Identification.** The aforementioned review is designed to be used as a tool for further prioritizing the cybersecurity issues that can be addressed and take actionable steps that advance the goals of the Best Practices effort.

- **Engagement of Independent Experts.** As appropriate, the Auto Alliance and Global Automakers will seek independent experts to work with OEMs and other key industry stakeholders during the development of Best Practices based on this Framework document. Such experts may assist in the ongoing review of existing best practices and may work with members to develop consensus-driven best practices that expand upon approaches already being utilized in the industry.

- **External Stakeholder Engagement.** At various stages throughout the Best Practices development process, the Auto Alliance and Global Automakers intend to, as appropriate, work with members to engage in discussions with external stakeholders, such as automotive suppliers, aftermarket product manufacturers, cybersecurity researchers, and relevant government agencies.

- **Industry Engagement Work Sessions.** The Alliance and Global Automakers will organize a series of industry work sessions focusing on issues related to best practices. These sessions are important for potential industry participants (*e.g.* manufacturers, suppliers, etc.), so that they can clearly understand the various implications of certain best practices approaches.

It is the intent of Auto Alliance and Global Automakers members to work as expeditiously as possible toward the development of robust industry Best Practices. In 2016, Auto Alliance and Global Automakers members are leading an ongoing effort to roll out issue-specific sets of best practices that are consistent with the guiding principles outlined in this Framework.

## IV. CONCLUSION

Members of the Auto Alliance and Global Manufacturers are fully committed to identifying and sharing policies and procedures that help address automotive cybersecurity. The members of the Auto Alliance and Global Manufacturers understand

that this is a process that demands great urgency, but also careful thought. For this reason, this Framework has been developed to provide a foundation for developing consensus around industry best practices.