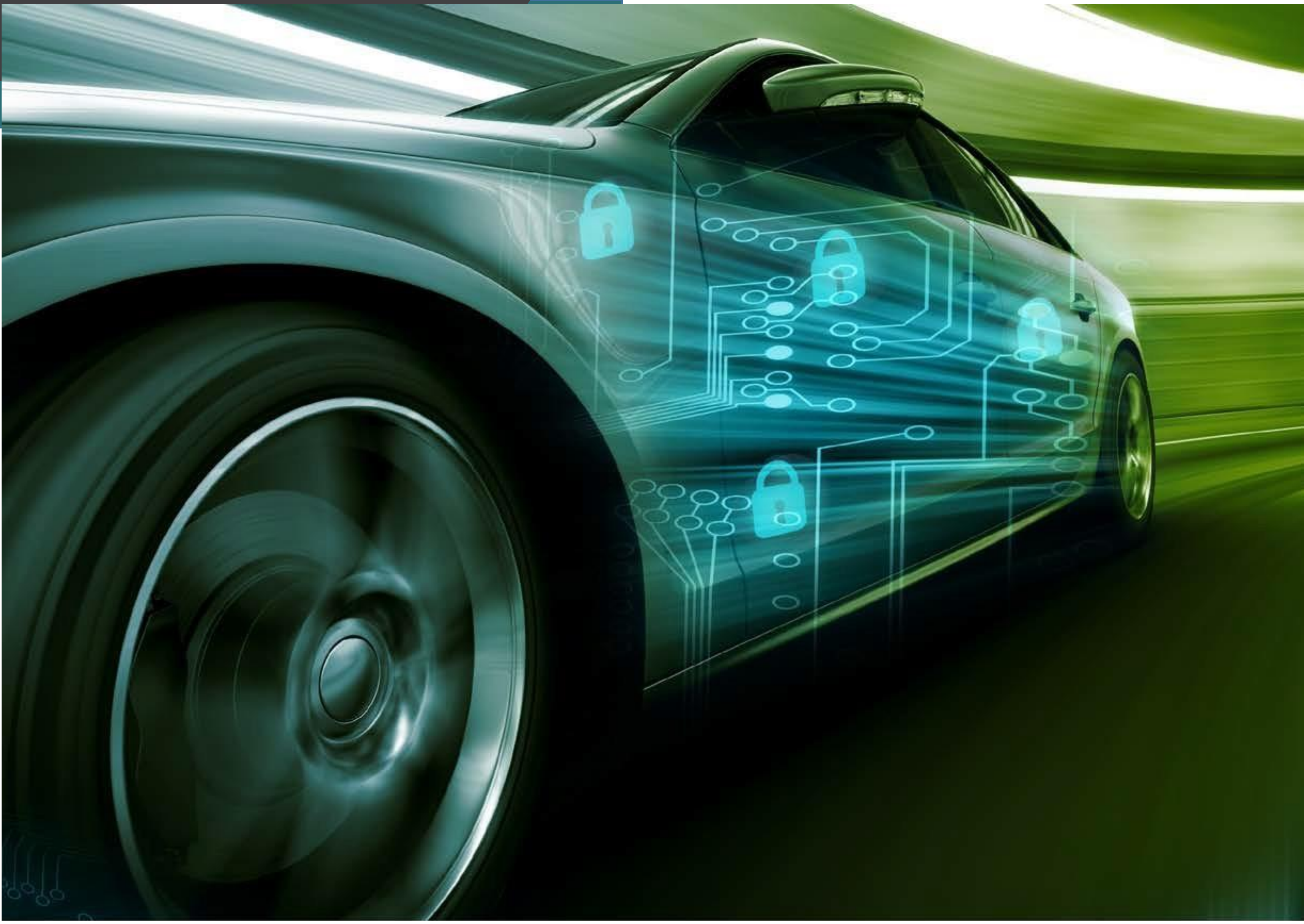


Automotive Cybersecurity Best Practices

Executive Summary

01 July 2019

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Version History

This is a living document, which will be periodically updated under direction of the Auto-ISAC Best Practices Working Group. We will track any updates in the table below.

Version Notes:

Version	Revision Date	Notes
v1.0	21 July 2016	
v1.1	01 July 2019	Performed periodic continuity and consistency refresh across all Best Practices documents

Contents

Version History 2
1.0 Context 4
2.0 Introduction 4
2.1 Overview 4
2.2 Purpose 4
2.3 Scope 5
2.4 Audience 5
2.5 Best Practices Development 5
2.6 Governance and Maintenance 6
2.7 Authority and Related References 6
3.0 Best Practices Overview 6
3.1 Incident Response 7
3.2 Collaboration and Engagement with Appropriate Third Parties 7
3.3 Governance 8
3.4 Risk Assessment and Management 9
3.5 Awareness and Training 9
3.6 Threat Detection, Monitoring and Analysis 10
3.7 Security Development Lifecycle 10
4.0 Best Practices Implementation 12
Appendix A: Glossary of Terms 13
Appendix B: Additional References and Resources 14
Appendix C: Acronyms 15

1.0 Context

As vehicles become increasingly connected and autonomous, the security and integrity of automotive systems is a top priority for the automotive industry. The Proactive Safety Principles released in January 2016 demonstrate the automotive industry's commitment to collaboratively enhance the safety of the traveling public. The objective of the fourth Principle, "Enhance Automotive Cybersecurity," is to explore and employ ways to collectively address cyber threats that could present unreasonable safety or security risks. This includes the development of best practices to secure the motor vehicle ecosystem.

To further this objective, the Automotive Information Sharing and Analysis Center ("Auto-ISAC") has undertaken the task of creating and maintaining a series of Automotive Cybersecurity Best Practices ("Best Practices"). The Best Practices cover organizational and technical aspects of vehicle cybersecurity, including governance, risk management, security development lifecycle, threat detection, monitoring and analysis, incident response, training and awareness, and collaboration and engagement with appropriate third parties.

The Best Practices expand on the Framework for Automotive Cybersecurity Best Practices published in January 2016 by the Alliance of Automobile Manufacturers ("Auto Alliance") and the Association of Global Automakers ("Global Automakers"). The Auto-ISAC closely collaborated with the two industry associations throughout Best Practices development. These Best Practices follow a precedent set by other ISACs and similar organizations that have developed best practices for their respective industries.

2.0 Introduction

2.1 Overview

This Executive Summary sets the framework for a series of Best Practice Guides focused on vehicle cybersecurity. Guides offer greater detail to complement the high-level Executive Summary, and are intended to provide the automotive industry with implementation guidance on the Key Cyber Functions defined in Section 3.0: Best Practices Overview.

2.2 Purpose

The Best Practices provide guidance on how individual companies can implement the "Enhance Automotive Cybersecurity" Principle within their respective organizations. This document is an Executive Summary of the Best Practices content.

The Best Practices provide forward-looking guidance without being prescriptive or restrictive. They are:

- **Not Required.** Organizations have the autonomy and ability to select and voluntarily adopt practices based on their respective risk landscapes and organizational structures.
- **Aspirational**. These practices are forward-looking, and voluntarily implemented over time, as appropriate.
- **Living**. The Auto-ISAC plans to periodically update this Executive Summary and Best Practices content to adapt to the evolving automotive cybersecurity landscape.

The Best Practices adhere to a risk-based approach to help automakers and industry stakeholders manage and mitigate vehicle cybersecurity risk. This risk-based approach enables all organizations—regardless of size, vehicle technology, or cybersecurity maturity—to tailor Best Practice implementation in a manner appropriate to their systems, services, and organizational structures.

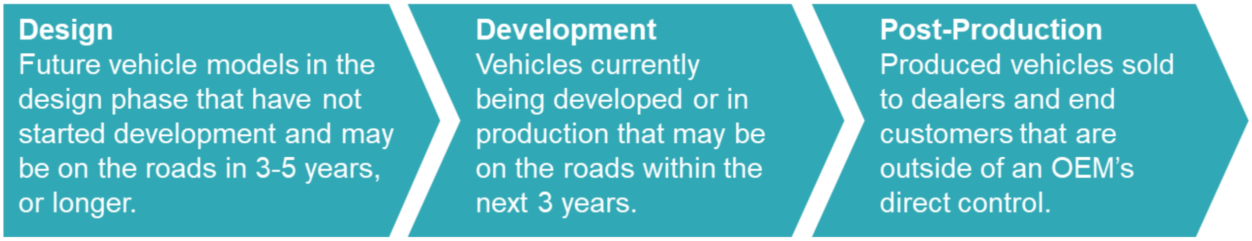
Cybersecurity experts agree that a future vehicle with zero risk is unobtainable and unrealistic. The Best Practices emphasize risk management, including the identification of risks and implementation of reasonable risk-reduction measures.

2.3 Scope

The Best Practices focus on product cybersecurity within the connected vehicle ecosystem and across the vehicle lifecycle. They refer primarily to U.S. light-duty, on-road vehicles but are applicable to other automotive markets, including heavy-duty and commercial vehicles. The Best Practices content intentionally leaves room for flexibility to allow for individualized implementation and to support international application by global automakers.

While Members share a common commitment to vehicle cybersecurity, their electrical architectures, connected services, and organizational compositions vary. Accordingly, the Best Practices do not prescribe specific technical or organizational solutions. The Auto-ISAC will update the Best Practices over time to address emerging cybersecurity areas and reflect the constantly evolving cyber landscape. Please see Section 2.1 for more information.

The scope of the Best Practice Guides will cover all phases of the vehicle lifecycle, including design, development, and post-production. These phases are described in Figure 1 below.



Design
Future vehicle models in the design phase that have not started development and may be on the roads in 3-5 years, or longer.

Development
Vehicles currently being developed or in production that may be on the roads within the next 3 years.

Post-Production
Produced vehicles sold to dealers and end customers that are outside of an OEM's direct control.

FIGURE 1: VEHICLE LIFECYCLE PHASES

2.4 Audience

The Best Practices are written for use by light-duty and heavy-duty vehicle OEMs, light-duty and heavy-duty vehicle suppliers, and commercial vehicle companies (e.g. fleets, carriers). They may also provide insights for other stakeholders across the connected vehicle ecosystem, including dealers and aftermarket suppliers.

2.5 Best Practices Development

The Auto-ISAC Best Practices Working Group facilitated work on this Guide with support from Booz Allen Hamilton. The Working Group is comprised of over 140 representatives from Auto-ISAC Member organizations. The Working Group also coordinated with several external stakeholders while developing the Best Practices, including several U.S. government agencies and other ISACs. The Auto-ISAC Board of Directors approves all Best Practice documents developed by and based on the recommendation of this Group.

2.6 Governance and Maintenance

The Auto-ISAC Best Practices Standing Committee is responsible for the maintenance of the Best Practice Guides and Executive Summary, which will undergo periodic refreshes to incorporate, as appropriate, lessons learned, new policies, updated or new engineering standards, and the like. These activities are supported by the Best Practices Working Group.

The Executive Summary is available as a Traffic Light Protocol (TLP) White document, making it available to the public on the Auto-ISAC website.

Best Practice Guides will be rolled out in phases and marked with the appropriate TLP classification and require the Auto-ISAC's Board of Directors' approval for release:

- **First 3 months after publication: TLP Amber** - available exclusively to Auto-ISAC Members
- **3 to 9 months after publication: TLP Green** - released by request to industry stakeholders
- **9 months after publication: TLP White** - released to the public via the Auto-ISAC website (www.automotiveisac.com), subject to Board of Directors confirmation.

2.7 Authority and Related References

The Best Practices do not form an assessment or compliance framework, and do not mandate prescriptive requirements. Each stakeholder will determine if and/or how to apply the Best Practices internally.

The Best Practices incorporate concepts from other standards and frameworks created by the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), SAE International, and other organizations. Many of the Best Practices either build on established ideas in those references or are adapted to address unique dimensions of the motor vehicle ecosystem. Specific documents are referenced in Section 3.0: Best Practices Overview.

In addition, the Best Practices' scope and content reflect a thorough review and benchmark of other ISAC and industry best practices that address information technology, supply chains, and manufacturing security. The Best Practices do not restate existing best practices for these areas.

3.0 Best Practices Overview

The Best Practices include seven Key Cybersecurity Functions, which are the highest level of Best Practice categorization and guide management of vehicle cyber risk. The Auto-ISAC may periodically add a Guide for a new Function to address the evolving vehicle cyber risk landscape. These Functions currently include:

1. Incident Response
2. Collaboration and Engagement with Appropriate Third Parties
3. Governance
4. Risk Assessment and Management

5. Awareness and Training
6. Threat Detection, Monitoring and Analysis
7. Security Development Lifecycle

A summary of each is below. Together, these Functions cover the diverse factors affecting cybersecurity across the connected vehicle ecosystem. The Functions influence each other, and many Best Practices have applicability across Functions and vehicle lifecycle phases.

Auto-ISAC has developed supplemental Best Practice Guides to provide Members and appropriate industry stakeholders additional information and implementation guidance for each of the seven functional areas. Please reach to Auto-ISAC to learn more about requesting access to the Guides, and see Section 2.6 for information on their release cycles.

3.1 Incident Response

An incident response plan documents processes to inform a response to cybersecurity incidents affecting the motor vehicle ecosystem. Best Practices include protocols for recovering from cybersecurity incidents in a reliable and expeditious manner, and ways to ensure continuous process improvement. The Best Practices framework for incident response includes four key focus areas: prepare, find, fix and close.

Best Practices for Incident Response include:

- **Prepare** to help ensure the organization is able to efficiently and effectively respond. This may include: documenting a plan and call sheet; establishing roles and responsibilities, including decision authorities; testing the plans through exercises and training
- **Find** incidents quickly to help mitigate potential impact. This may include: identifying, validating, classifying and escalating potential incidents using a severity matrix that's aligned to clear escalation protocols
- **Fix** incidents by activating a team to rapidly contain, mitigate, remediate and recover from the risk. This may include executing technical response activities (e.g. root cause analysis, containment, forensics), managing business risk through complementary corporate response (e.g. communications, legal, regulatory), and coordinating across workstreams
- **Close** each incident. This may include debriefs to assess effectiveness of response procedures to determine necessary procedure or policy changes; evaluation, implementation and monitoring any longer-term remediation actions; and updates of the plan

Incident Response Best Practices leverage *NIST SP 800-61: Computer Security Incident Handling Guide, ISO/IEC 27035:2011 Information Security Incident Management,* and other established resources.

3.2 Collaboration and Engagement with Appropriate Third Parties

Defending against cyber attacks often requires collaboration among multiple stakeholders to enhance cyber threat awareness and cyber attack response. When faced with cybersecurity challenges, the industry is committed to engaging with third parties, including industry partners, industry organizations, government, academia, researchers and media, as appropriate. The Best Practices framework for this function outlines three core methods under which third party collaboration and engagement (3PCE) activities typically fall: information sharing, events and programs.

- Best Practices for Collaboration and Engagement with Appropriate Third Parties may include: **Information Sharing**: Participate in efforts to share threat intelligence, vulnerability research and best practices. Information sharing activities benefit from identifying appropriate information to share, engaging the right internal parties, and setting clear processes to take in and act on received information, as well as a process to push information out to third parties
- **Events**: Engage with third parties through focused activities to bring together diverse groups of experts (e.g. tabletops, hackathons, conferences). Organizations can maximize the benefits of 3PCE events by identifying and participating in a variety of event types, designing events to engage third parties, or participating in externally-led events
- **Programs**: Identify longer-term initiatives to pool resources toward a specific goal (e.g. coordinated disclosure, standards development, professional exchanges and certifications). Organizations can maximize the benefits of 3PCE programs by identifying and participating in a variety of program types, designing programs to engage third parties, or participating in externally-led programs

Collaboration and Engagement Best Practices leverage *NIST SP 800-150: Guide to Cyber Threat Information Sharing, ISO/IEC 27010:2012—Information Security Management for Inter-sector and Inter-organizational Communications*, and other established resources.

3.3 Governance

Effective governance aligns a vehicle cybersecurity program with an organization's broader mission and objectives. Furthermore, strong governance can help to foster and sustain a culture of cybersecurity. Best Practices do not dictate a particular model of vehicle cybersecurity governance but provide considerations for organizational design to align functional roles and responsibilities. The Best Practice framework for governance revolves around three key elements: design, build and operate. While these priorities are important for all programs, specific activities are most effective when they are customized to meet the unique needs of each company.

Best Practices for Governance may include the following tasks:

- **Design**:
  - Define and communicate the program's scope
  - Articulate the mission and vision
  - Identify key functions
- **Build**:
  - Organize within the program—activate the leadership, set clear decision authorities and create a staffing model (e.g. functional, geographic, matrixed)
  - Engage across the business—integrate with partners across the organization (e.g. IT, legal, supply chain), and define and execute against expectations for leadership-level communications

- **Operate**:
    - Develop policies and processes
    - Manage performance through metrics
    - Maintain consistent and transparent process for resource allocation
-

Governance Best Practices leverage guidelines included in *ISO/IEC 27001—Information Security Management* and other cybersecurity management references.

3.4 Risk Assessment and Management

Risk assessment and management strategies mitigate the potential impact of cybersecurity vulnerabilities. Best Practices focus on processes for identifying, categorizing, prioritizing, and treating cybersecurity risks that could lead to safety and data security issues. Risk management processes can help automakers identify and protect critical assets, assist in the development of protective measures, and support operational risk decisions.

Best Practices for Risk Assessment and Management mayinclude the following tasks:

- Define the overall **scope and requirements** associated with implementing a cyber risk assessment methodology
- Integrate various types of security assessments into appropriate phases of a vehicle or product's lifecycle to ensure appropriate **coverage**
- Document **roles and responsibilities** to help stakeholders understand expectations for their roles, tasks and timing
- Determine the appropriate cadence for risk assessments throughout the **risk lifecycle**, as the risk scores may periodically change
- Formalize a **risk tolerance** profile to inform decision-making; risk tolerance may vary by lifecycle phase, and is typically determined by evaluating risk acceptance criteria
- Define consistent methods to evaluate risk assessment **results** and determine **risk treatment plan** (e.g. contain, remediate, avoid, transfer, accept)
- Consistently **communicate** risk to leadership and stakeholders, ideally using non-technical terminology to help them compare vehicle cybersecurity risks to other more traditional enterprise risks
- Integrate risk management processes and standards into **governance** of business operations, and monitor and enforce **compliance**

Risk Assessment and Management Best Practices leverage *NIST 800-30: Guide for Conducting Risk Assessments* and other established resources.

3.5 Awareness and Training

Training and awareness programs help cultivate a culture of security and enforce vehicle cybersecurity responsibilities. The Best Practices emphasize training and awareness programs throughout an organization to strengthen stakeholders' understanding of cybersecurity risks. This capability is typically comprised of four fundamental activities: Design, Develop, Implement, and Improve. These four activities provide a framework that companies can use to design their own programs.

Best Practices for Awareness and Training may include:

- **Design** awareness and training programs by assessing needs of the business (e.g. targeted, role-specific training vs. broad awareness campaign), scoping the program and developing a strategy and plan
- **Develop** the program by acquiring or developing awareness content and products, acquiring or developing training curricula and fostering culture of learning
- **Implement** the program by communicating the strategy plan, conducting training activities and distributing products, and conducting training
- **Improve** the program on a regular basis by monitoring, reporting, analyzing effectiveness and identifying improvement opportunities

Awareness and Training Best Practices leverage *NIST SP 800-50: Building an Information Technology Security Awareness and Training Program* and other established cybersecurity training resources.

3.6 Threat Detection, Monitoring and Analysis

Proactive cybersecurity through the detection of threats, vulnerabilities, and incidents empowers automakers to mitigate associated risk and consequences. Threat detection processes raise awareness of suspicious activity, enabling proactive remediation and recovery activities.

Best Practices for Threat Detection, Monitoring and Analysismay include:

- Define a **threat detection and analysis** process by understanding the automotive threat environment, developing a threat team structure and operating model, and defining stakeholder roles and responsibilities.
- Define **threat intelligence** requirements that will help **identify sources** and the collection process.
- Establish a **threat monitoring** process by defining priorities and identifying various techniques and approaches
- Define a **threat analysis** methodology that includes threat event identification, validation and verification and necessary action to take
- Establish a process and develop or acquire the right toolset to **organize, store and share** information for maximum effectiveness

Threat Detection, Monitoring and Analysis Best Practices leverage *NIST 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations*, *ISO/IEC 30111: Vulnerability Handling Procedures*, and other established resources.

3.7 Security Development Lifecycle

Secure vehicle design involves the integration of hardware and software cybersecurity features during the product development process. Principles of the automotive Security Development Lifecycle (SDL) help ensure that appropriate cybersecurity protections are identified in the early stages of design (e.g.

during vehicle electrical architecture planning), when implementation costs are lower and there is time to consider design interactions that might affect cybersecurity. The SDL applies to entities that design and develop vehicles or vehicle components, including hardware and software. This includes organizations using traditional waterfall ("V-model") development cycles, more iterative Agile methodologies, and/or hybrid models.

Best Practices for the Security Development Lifecycle include:

- **Pre-Development**: Consider existing system architectures that constrain future design decisions. Identify lessons learned from previous design cycles to incorporate. Additionally, organizations may want to define the types of cyber risks that are acceptable and unacceptable for the final product.
- **Design and Development**:
    - Develop a comprehensive superset of all required cybersecurity specifications that can be tailored to a component based upon its features during initial **requirements design**
    - During the **design** phase, ensure requirements are clear and testable; drive understanding of threats and risks to the system; utilitize a system architecture that can help mitigate identified threats and risks; and embrace cybersecurity principles
    - Focus on security in **implementation** (e.g. through coding standards, code analysis and traceability mechanisms) to help ensure the effort put into requirements analysis and secure design is not lost during implementation
    - Promote security **testing and verification** to prove the implemented systems are working properly, and evaluate whether a system was developed according to the requirements and specifications; this includes checking if security design principles (e.g. "Least Privileges") have been specified and implemented properly for the target system
- **Post-Development**: Monitor vehicle cybersecurity issues that emerge post-development, during vehicle operations and maintenance, to provide a feedback loop for the requirements and design phases of the automotive SDL process to aid in continuous improvements in security

SDL Best Practices leverage *SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, NIST 800-64: Security Considerations in the Systems Development Lifecycle, NIST SP 800-121 Guide to Bluetooth Security, NIST SP-127: Guide to Securing WiMAX Wireless Communications, ISO 17799: Mobile Phone Security*, and other established resources.

4.0 Best Practices Implementation

The Best Practices are not intended to, nor should be interpreted to, obligateanyone to take specific action or measures. Each stakeholder has unique needs and capabilities with respect to cybersecurity. Therefore, the Best Practices may not be applicable to some organizations or parts of organizations. Accordingly, these Best Practices offer suggested measures.

Cybersecurity is a priority for Auto-ISAC Members and stakeholders across the connected vehicle ecosystem. These Best Practices can guide effective risk management and further enhance the security and resiliency of the automotive industry.

Members of the Auto-ISAC are committed to updating the Best Practices over time as the connected vehicle ecosystem's risk landscape evolves.

Appendix A: Glossary of Terms

Key terms used in this document are defined below.

TERM	DEFINITION
Best Practices	Guidance on how individual companies can implement organizational and technical practices to enhance vehicle cybersecurity. They are: • **Not Required.** Organizations have the autonomy and ability to select and voluntarily adopt practices based on their respective risk landscapes and organizational structures. • **Aspirational**. These practices are forward-looking, and voluntarily implemented over time, as appropriate. • **Living**. The Auto-ISAC plans to periodically update this Executive Summary and Best Practices content to adapt to the evolving automotive cybersecurity landscape.
Best Practice Guides	A series of Guides that cover organizational and technical aspects to enhance vehicle cybersecurity. These Auto-ISAC documents are intended to provide the automotive industry with implementation guidance on the Key Cybersecurity Functions defined in Section 3.0 of this document. The Auto-ISAC may periodically add a Guide for a new Function to address the evolving vehicle cyber risk landscape.
Key Cybersecurity Functions	The highest level of Best Practice categorization to guide management of vehicle cyber risk. Together, these Functions cover the diverse factors affecting cybersecurity across the connected vehicle ecosystem. The Functions influence each other, and many Best Practices have applicability across Functions and vehicle lifecycle phases. The Auto-ISAC may add new Functions over time to address the evolving vehicle cyber risk landscape.
Vehicle Ecosystem	The components and infrastructure on or connected to the vehicle (e.g. hardware and software, intellectual property, mobile applications, customer data, vehicle data, supplier/manufacturing networks, applications, processes and organizations that directly or indirectly touch the vehicle and may play a role in vehicle cybersecurity).
Vehicle Cybersecurity	The activities, processes, and capabilities that protect, detect, and respond to cybersecurity occurrences (e.g. remote control, unauthorized access, disruption, manipulation) that actually or potentially result in adverse consequences to a vehicle, connected infrastructure, or information that the vehicle processes, stores, or transmits.

Appendix B: Additional References and Resources

This Executive Summary referenced several existing best practice and standards documents and organizations. The following References and Resources provide additional content and expertise for companies to consider in conjunction with this Executive Summary. Each Best Practice Guide also provides additional detailed references and resources related to that particular Function.

REFERENCES
ISO 17799: Mobile Phone Security
ISO/IEC 27001—Information Security Management
ISO/IEC 27010:2012—Inter-sector and Inter-organizational Communications
ISO/IEC 27035:2011 Information Security Incident Management
ISO/IEC 30111: Vulnerability Handling Procedures
NHTSA: Cybersecurity Best Practices for Modern Vehicles
NIST 800-30: Guide for Conducting Risk Assessments
NIST SP 800-50: Building an Information Technology Security Awareness and Training Program
NIST SP 800-61: Computer Security Incident Handling Guide
NIST 800-64: Security Considerations in the Systems Development Lifecycle
NIST SP 800-121 Guide to Bluetooth Security
NIST SP-127: Guide to Securing WiMAX Wireless Communications
NIST 800-137: Continuous Monitoring for Federal Information Systems and Organizations
NIST SP 800-150: Guide to Cyber Threat Information Sharing
SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

RESOURCES
Industry Associations, such as Auto Alliance and Global Automakers
International Organization for Standardization (ISO)
National Institute of Standards and Technology (NIST)
SAE International

Appendix C: Acronyms

3PCE	Third-Party Collaboration and Engagement
Auto-ISAC	Automotive Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
SAE	Society of Automotive Engineers
SDL	Security Development Lifecycle
TLP	Traffic Light Protocol