

COLLABORATION AND ENGAGEMENT WITH APPROPRIATE THIRD PARTIES

Best Practice Guide
Version 1.3



Traffic Light Protocol: White.

This information may be shared in public forums.

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	29 March 2017	
v1.1	10 July 2017	Changed from TLP Amber to TLP Green for release to industry stakeholders via request on Auto-ISAC website
v1.2	18 January 2018	Changed from TLP Green to TLP White for release to the public via request on Auto-ISAC website
v1.3	01 July 2019	Performed periodic continuity and consistency refresh across all Best Practice documents

Contents

Version History.....	i
1.0: Introduction	1
1.1 BEST PRACTICES OVERVIEW.....	1
1.2 PURPOSE.....	1
1.3 SCOPE.....	1
1.4 AUDIENCE	2
1.5 AUTHORITY AND GUIDE DEVELOPMENT.....	2
1.6 GOVERNANCE AND MAINTENANCE	3
2.0: Collaboration and Engagement in Vehicle Cybersecurity	3
2.1 RELEVANT THIRD PARTIES	3
2.2 “THE OPENNESS SPECTRUM”	4
2.3 RISKS OF COLLABORATION AND ENGAGEMENT	6
2.4 BENEFITS OF COLLABORATION AND ENGAGEMENT	6
3.0: Best Practices	8
3.1 METHODS OF COLLABORATION AND ENGAGEMENT	8
3.2 BEST PRACTICES FOR INFORMATION SHARING	8
3.3 BEST PRACTICES FOR EVENTS.....	11
3.4 BEST PRACTICES FOR PROGRAMS.....	13
Appendix A: Glossary of Terms.....	16
Appendix B: Additional References and Resources	17
Appendix C: Acronyms.....	19

1.0: Introduction

1.1 BEST PRACTICES OVERVIEW

This Best Practice Guide is one in a series intended to provide the automotive industry with guidance on the Key Cyber Functions defined in the [Automotive Cybersecurity Best Practices Executive Summary](#):

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

Guides offer greater detail to complement the high-level Executive Summary. This Guide aligns to the “Collaboration and Engagement with Appropriate Third Parties” Function. Each organization may use the Best Practices and this Guide as appropriate for their unique systems, processes, and risks.

1.2 PURPOSE

The purpose of this Guide is to assist heavy and light-duty vehicle OEMs, suppliers and auto industry stakeholders with collaborating and engaging appropriate third parties as part of their vehicle cybersecurity activities.

This Guide provides forward-looking guidance without being prescriptive or restrictive. These best practices are:

- **Not Required.** Companies have autonomy and can decide which of these practices to select and can adopt these practices based on their respective risk landscapes and organizational structures.
- **Aspirational.** These practices are forward-looking, and voluntarily implemented over time, as appropriate.
- **Living.** Auto-ISAC plans to periodically update this Guide to adapt to the evolving automotive cybersecurity landscape.

1.3 SCOPE

This Guide discusses voluntary third-party collaboration and engagement (3PCE), which is focused on enhancing vehicle cybersecurity, with third parties across the connected vehicle ecosystem. The Guide will describe the benefits, decision factors, and methods for voluntary 3PCE.

The scope of the Guide covers all phases of the vehicle lifecycle, including design, development, and post-production. These phases are described in Figure 1 below.

COLLABORATION AND ENGAGEMENT WITH APPROPRIATE THIRD PARTIES

Traffic Light Protocol: White (May be shared in public forums)



FIGURE 1: VEHICLE LIFECYCLE PHASES

These best practices do not encompass actions that are explicitly required by U.S. or international regulations, state laws, or legal agreements between private entities. For example, the Guide does not cover contractually-obligated sharing with suppliers. However, organizations may use these practices to inform voluntary engagement activities they pursue with their suppliers. The Guide also does not include engagement with consumers—as they are not a third party. Examples to clarify scope are listed in Figure 2.

In Scope	Out of Scope
<ul style="list-style-type: none">• Engaging with NHTSA to communicate progress and priorities• Co-facilitating an information exchange event with business partners• Sharing vulnerability information with researchers under an NDA or MOU	<ul style="list-style-type: none">• Engaging with NHTSA as mandated by legal reporting requirements• Participating in mandated training as part of a business contract• Sharing vulnerability information, which is necessary to execute contracted work, with business partners

FIGURE 2: SAMPLE 3PCE ACTIVITIES TO ILLUSTRATE GUIDE SCOPE

1.4 AUDIENCE

This Guide was 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). It may also provide insights for other stakeholders across the connected vehicle ecosystem.

Within these organizations, the primary audience is individuals and teams responsible for developing and executing 3PCE for their organization.

1.5 AUTHORITY AND GUIDE DEVELOPMENT

The Auto-ISAC Best Practices Working Group wrote this Guide, with support from Booz Allen Hamilton vehicle cybersecurity SMEs, who facilitated the Guide's development. The Working Group comprised representatives from several Members and partners, including:

AT&T	FCA	Infineon	Mobis
Auto Alliance	Ford	Kia	Nissan
BMW Group	General Motors	Lear	NXP
Continental	Global Automakers	LG	Subaru
Cooper Standard	Harman	Magna	Toyota
Cummins	Honda	Mazda	Volkswagen
Delphi	Honeywell	Mercedes-Benz	Volvo

DENSO

Hyundai

Mitsubishi Motors

ZF

The Working Group also coordinated with several external stakeholders while developing this Guide, including NHTSA, NIST, US-CERT, and CERT-CC.

1.6 GOVERNANCE AND MAINTENANCE

The Auto-ISAC Best Practices Standing Committee is responsible for the maintenance of the Guide, which will undergo periodic refreshes to incorporate, as appropriate, lessons learned, new policies, updated or new engineering standards, and the like.

This Guide will be rolled out in phases and marked with the appropriate Traffic Light Protocol (TLP) classification:

- **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

2.0: Collaboration and Engagement in Vehicle Cybersecurity

This section answers the “who,” “when,” and “why” to participate in 3PCE.

2.1 RELEVANT THIRD PARTIES

Automotive industry companies are part of a broad and expanding ecosystem. To enhance vehicle cybersecurity, these companies may collaborate and engage with several types of third parties across the connected vehicle ecosystem.



Industry Partners. Industry partners are organizations that are directly involved in the design, manufacturing, selling, and maintenance of on-road vehicles. Collaboration and engagement among industry partners helps enhance awareness of vehicle cybersecurity matters that may impact their products or services. These groups include original equipment manufacturers (OEMs), the OEM supply chain (Tiers 1, 2, and 3), network providers (e.g. telecommunications providers), software providers, service providers (e.g. consulting firms, security vendors), dealers, carriers, fleet owners and operators, infrastructure operators (e.g. Smart Cities, V2X), aftermarket manufacturers and suppliers, and independent repair shops.



Industry Organizations. Industry organizations include parties that either consist of or represent industry partners to support a particular cause related to vehicle cybersecurity, such as standards development, safety and security, information sharing, or training. This group includes automotive trade associations, standards bodies, and Auto-ISAC. These groups play a significant role in automotive cybersecurity industry efforts.



Government. Government third parties include U.S. and international agencies that play a role in the connected vehicle ecosystem. These include U.S. and international regulatory agencies (e.g. NHTSA), non-regulatory federal agencies, state and local governments, law enforcement agencies, and intergovernmental agencies (e.g. INTERPOL). Collaboration and engagement with this group can help foster policy decisions that enable vehicle cybersecurity advancements.



Academia. This group consists of universities and educational organizations that are involved in programs, studies, research, and testing related to connected vehicle products and services. Collaboration with academia is mutually beneficial; Industry can solve current and future cybersecurity challenges while expanding research opportunities for academic institutions.



Researchers. This group include the labs, consortia, research organizations, and individual researchers and hobbyists comprising the “white-hat” connected vehicle research community. This group conducts vehicle cybersecurity research and testing on vehicles for the benefit of public safety and awareness. They can help organizations stay apprised of the most up-to-date findings and leverage researcher expertise to improve vehicle cybersecurity. 3PCE with the “black-hat” research community is out of scope for this Guide.



Media. The media includes public content forums and advertising platforms that showcase automotive-related stories. When content is accurate, the media offers an effective way to communicate with current and potential customers about vehicle cybersecurity, raise awareness about threats, and identify and respond to vehicle cybersecurity-related news.

It can be helpful to establish a set of evaluation criteria to help vet and prioritize external third parties, like those listed above, before collaborating and engaging on sensitive topics.

2.2 “THE OPENNESS SPECTRUM”

This Guide does not prescribe a particular level of external collaboration and engagement. Rather, organizations can determine the right level of openness based on their individual vehicle cybersecurity objectives and their unique risk landscape (Figure 3).

This Guide does not prescribe that organizations seek a particular level of external engagement. Rather, it aims to define characteristics and decision factors for determining appropriate levels of engagement, across the “openness spectrum,” based on certain situational variables, including risk levels, timing, cost, and organizational capability. Organizations may choose to position themselves at different points of the spectrum at different times and with different third parties.

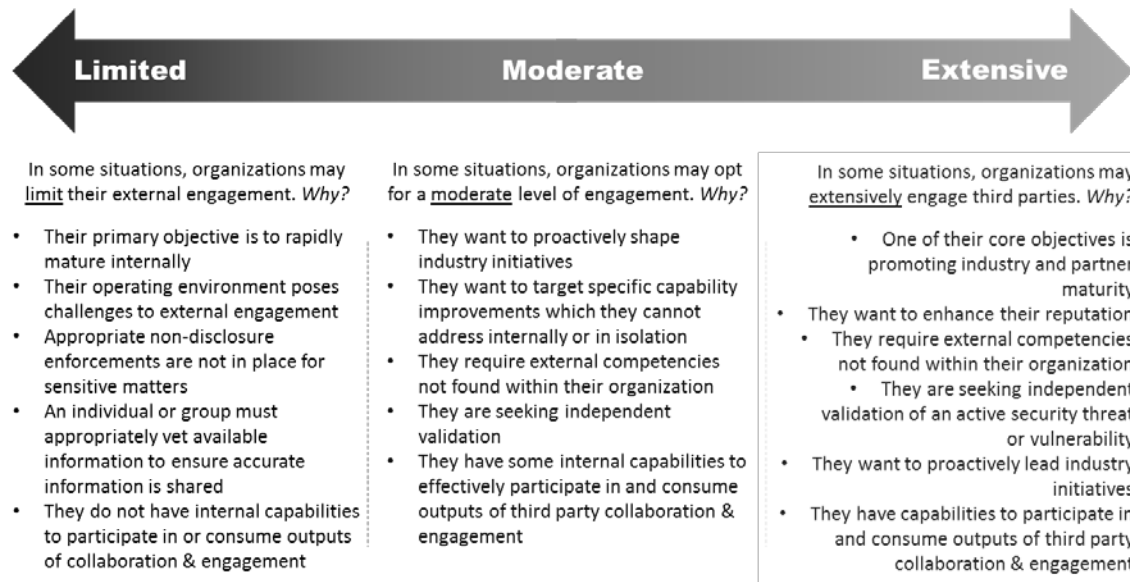


FIGURE 3: OPENNESS SPECTRUM AND CONSIDERATIONS

At times, organizations may want to maximize 3PCE, but face **roadblocks**. Examples of these potential roadblocks and sample **mitigation strategies** include:

- **Potential Roadblock:** Concerns over real or perceived anti-trust issues, and exposure of intellectual property.
 - **Potential Mitigation:** Use appropriate anti-trust warnings and create and communicate appropriate non-disclosure agreements (see Section 3.2 for additional measures)
- **Potential Roadblock:** Lack of clarity internally regarding domestic and international regulatory requirements.
 - **Potential Mitigation:** Communicate with government relations personnel and regulators to gain clarity regarding expectations. (see Section 3.2 for additional measures)
- **Potential Roadblock:** Concerns over adversarial market exposures.
 - **Potential Mitigation:** Establish relationships dedicated to a specific objective with a small set of collaborators to demonstrate value and build trust in third party resources. (see Section 3.4 for additional measures)
- **Potential Roadblock:** Lack of sufficient tools and technology.
 - **Potential Mitigation:** Share costs for technical infrastructure that allows for efficient and secure engagement with third parties. (see Sections 3.2 and 3.3 for additional measures)
- **Potential Roadblock:** Lack of proactive measures to establish communications channels.
 - **Potential Mitigation:** Establish non-disclosure agreements (NDAs) and mutually identify points of contact for critical third parties

The mitigations listed above are just a sample set. Please see the full list of Best Practices below for additional mitigation ideas.

2.3 RISKS OF COLLABORATION AND ENGAGEMENT

3PCE can also carry risk, particularly when organizations do not implement relevant 3PCE Best Practices. Organizations will benefit from identifying and proactively addressing the risks, including the sample list highlighted below, to ensure that 3PCE helps—not hurts—vehicle cybersecurity efforts.

Risks associated with 3PCE may include:

- Mismanaged resource allocation leading to deficiencies in other parts of the organization
- Sharing of incorrect or misleading information that could burn resources and weakens cyber defense posture
- Disruption of established strategy or processes
- Accidental disclosure of intellectual property or other sensitive information
- Premature exposure of industry vulnerabilities before providing appropriate time for the affected parties to react and mitigate an issue
- Increased levels of shared information, requiring time to filter and prioritize issues
- Confusion resulting from inconsistent or unclear reporting and response protocols

The Best Practices described in Section 3.0 may help organizations mitigate these risks as they “move right” on the Openness Spectrum.

2.4 BENEFITS OF COLLABORATION AND ENGAGEMENT

Working with appropriate third parties can deliver a wide variety of possible business benefits, including: reducing vehicle cyber risk, enhancing operational performance, and reducing costs. Organizations that often operate on the middle or right side of the “openness spectrum” discussed in Section 2.2 may experience these benefits more frequently than those who tend to limit engagement.

A primary way 3PCE benefits organizations is by **mitigating vehicle cyber risk**. Examples of this include:

- Developing improved awareness of threat landscape through collective intelligence, such as vulnerabilities, threats, actions, tools, techniques, and protocols, and indicators of compromise
- Understanding context of potential vehicle cyber events
- Assessing potential risk to the organization’s cyber posture
- Improving incident response capabilities
- Having established relationships and lines of communication in place for when things go wrong, which can help expedite response
- Integrating cybersecurity expertise to aid development of vehicle cybersecurity solutions
- Applying traditional IT Security principles to related elements of the connected vehicle ecosystem
- Identifying alternative testing strategies, techniques, and solutions
- Educating vehicle cybersecurity ecosystem stakeholders (e.g. business partners, dealers, government organizations) to mitigate potential industry-wide risk
- Seeking independent evaluation of product cybersecurity capabilities
- Sharing best practices and standards across similar organizations
- Expanding access to adjacent technology

- Gaining knowledge of prior experiences, strategy, and solutions
- Participating in industry benchmarking to inform cyber priorities

3PCE pertaining to vehicle cybersecurity can also help **improve business performance**. Examples of this include:

- Developing external relationships that can be leveraged during crisis management
- Increasing capacity through outsourcing
- Improving quality and design resulting from increased understanding of and attention to internal products
- Reducing reliance on singular technology partners, avoiding the “lock-in” effect

3PCE pertaining to vehicle cybersecurity can also help organizations to **lower costs**. Examples of this include:

- Reducing duplication of efforts across organizations
- Sharing risk of investment when multiple organizations contribute
- Expanding research opportunities through aggregation of multiparty technical and financial resources
- Shortening development time for cyber solutions, leading to reduced development costs
- Improving incident response coordination, lowering the impact of a cyber event

Other potential benefits of 3PCE regarding vehicle cybersecurity may include:

- Enhancing industry reputation, leading to increased consumer confidence
- Improving recruiting opportunities
- Increasing readiness for the emergence of mobility solutions
- Creating new opportunities for innovation and “out-of-the-box” thinking
- Increasing access to global markets
- Controlling external messaging around notable events

3.0: Best Practices

The purpose of this section is to define the primary methods for 3PCE and provide implementation guidance specific to these methods. Organizations may augment these Best Practices and accompanying narrative with the References listed in Appendix B.

3.1 METHODS OF COLLABORATION AND ENGAGEMENT

Effective 3PCE must be customized to meet the unique needs of each organization. To provide meaningful and actionable Best Practices, this Guide defines three high-level 3PCE methods under which 3PCE activities typically fall. Some activities align to multiple methods and their corresponding best practices and thus may benefit from multiple sets of Best Practices.

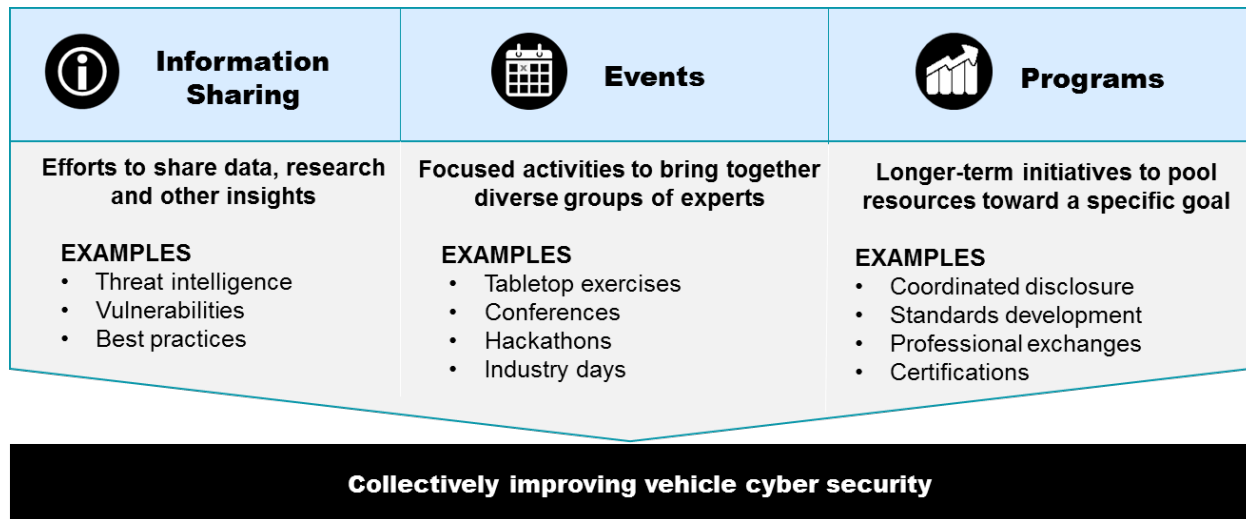


FIGURE 4: METHODS OF COLLABORATION AND ENGAGEMENT

3.2 BEST PRACTICES FOR INFORMATION SHARING

Information sharing helps organizations take swift action on potential vehicle cybersecurity incidents, threats, and vulnerabilities, keeps key stakeholders informed of vehicle cybersecurity activities, and increases the industry's collective vehicle cybersecurity knowledge.

Identify content that is helpful to share. When organizations clearly define “shareable” information, they can take more deliberate collaborative actions when appropriate. Please see the “Create processes to capture and push information to external third parties” section below for more guidance on determining what to share with various groups.

Types of information that may be helpful to share with third parties include:

- Actionable information on past and present vehicle cybersecurity incidents
- Actionable information on past and present vehicle cybersecurity threats
- Actionable information on past and present vehicle cyber vulnerabilities
- Processes for responding to vehicle cybersecurity incidents
- Processes for detecting and protecting against vehicle cybersecurity threats (see the Auto-ISAC's *Threat Detection, Monitoring and Analysis Best Practices Guide* for more information)

- Processes for finding and resolving vehicle cybersecurity vulnerabilities
- Vehicle cybersecurity organizational structure
- Research on vehicle cybersecurity
- Customer expectations and experiences regarding vehicle cybersecurity
- Industry vehicle cybersecurity trends
- Litigation trends related to vehicle cybersecurity incidents
- Future opportunities to collaborate on vehicle cybersecurity

Engage the right internal stakeholders. Vehicle cybersecurity information is often sensitive, urgent, and multi-faceted. It is important to consider timely engagement of a wide variety of internal groups to effectively exchange information with external third parties.

Internal stakeholders that may play a role when sharing vehicle cybersecurity information with third parties include:

- Executive leadership and Board of Directors – for situational awareness and approvals
- Vehicle and enterprise IT cybersecurity analysts – for technical analysis, triage, and remediation
- Engineering and Design – for supplier and customer coordination and developing and implementing solutions
- Safety experts – for awareness of safety-critical issues
- Quality assurance experts – for differentiation between mechanical and cyber issues
- Communications experts – for internal and external messaging
- Public policy experts – for coordination with government liaisons
- Legal counsel – for risk mitigation and decision insights
- Supply chain experts – for coordination with suppliers and dealers
- Manufacturing plant operators – for issues affecting the assembly line
- Purchasing – for issues related to outsourced parts and services
- Customer service and warranty representatives – for communication with end customers

Create processes to take in and act on shared information. Once an organization receives information from a third party, the next step is to ensure that the information goes to the right person(s) for the appropriate action to be taken. Creating and documenting how different types of information is managed and used allows individuals operating within an organization to maintain clear lines of responsibility and authority.

Best Practices for collecting and using information shared by a third party include:

- Documented processes govern how to manage vulnerabilities, respond to incidents, and protect against threats (See the Auto-ISAC's *Incident Response*, *Risk Assessment and Management*, and *Threat Detection, Monitoring and Analysis Best Practice Guides* for more information)
- An established protocol is shared with external third parties to enable consistent sharing of information
- Consistent guidelines are used to assess third party information, including validity and trustworthiness of external information
- An established process is used for consistent, secure dissemination and storage of information within the organization

This Guide does not prescribe or require specific technical or organizational practices. These are voluntary and aspirational practices, which may evolve over time. Please see Section 1.2 for more information.

- A clear taxonomy enables common understanding internally and with third parties
- Legal and regulatory obligations are clearly understood
- An accurate vehicle asset inventory—including hardware, software, and code versions and origins—provides rapid insights into production and post-production vehicles
- Internal stakeholders understand the organizational structure, including roles and responsibilities of business units, POCs for external groups, and approval requirements
- When applicable, there is an ability to take in information through common, standardized formats (e.g. CVE, STIX, TAXII) and via industry-wide forums (e.g. Auto-ISAC Portal)

Create processes to push information to external third parties. Before vehicle cybersecurity information can be shared externally, organizations will want to determine how, what, and to whom information is sent. Creating processes to capture and push information will enable timely sharing and limit disclosure risks.

Best Practices for pushing vehicle cybersecurity information to third parties include:

- Processes for reviewing and approving the information reflect technical, business, and legal perspectives
- A common approach and criteria define which third parties would benefit from the information, timeframes for dissemination, mechanisms to share, and roles and responsibilities to develop, review, approve and send the information
- Internal documentation and storage policies are based on the type of information and the destination, and align with regulatory requirements
- Defined metrics rank information by priority and sensitivity, including an assessment of the information's impact on vehicle safety and personal privacy
- Organizations and third parties have non-disclosure agreements or other confidentiality agreements in place, if necessary, to safeguard information
- Organizations are able to push out information through standardized formats (e.g. CVE, STIX, TAXII) and through industry-wide platforms (e.g. Auto-ISAC Portal) as appropriate

Acquire appropriate tools and technologies. At times, organizations will want to share information with a very limited number of external parties, while at others, they will want to widely broadcast the information. Some information will need to be kept anonymous, confidential, or secure when it is shared. A suite of information sharing tools will help to accommodate these requirements and allow organizations to engage third parties efficiently and reliably. Sample tools and technologies that may be used to share or receive vehicle cybersecurity information include:

- Secure web portals (e.g. Auto-ISAC Portal)
- Secure file sharing and transfer applications
- Audio and visual conferencing platforms
- Press releases
- Social media
- Contact relationship management software
- Shared email accounts or "Contact Us" webpages to provide a single entry-point for third parties to contact an organization's cyber team(s)

3.3 BEST PRACTICES FOR EVENTS

Events allow organizations to collaborate and engage with third parties on vehicle cybersecurity in a broader, more inclusive setting. Events often include a variety of experts on a particular topic, giving the discussion credibility and leading to productive idea exchange.

Identify the types of events to design or attend. Participating in a variety of events can help organizations build specific capabilities, particularly when they prioritize those that meet specific internal needs and are feasible based on available resources. Characteristics of successful events can be found below under the section titled “Design and execute 3PCE events.”

Types of events that support vehicle cybersecurity capabilities include:

- **Incident Response (IR) Exercises.** Opportunities to build relationships with response-relevant third-parties through a variety of exercises—including tabletops, wargames, drills, and threat scenario workshops—where participants simulate vehicle cyber incident response processes through a scenario
- **Cyber Challenges.** Challenge-based events—including hackathons and code-athons—in which software developers and/or engineers collaborate to produce a prototype, proof of concept, or cybersecurity solution
- **Conferences.** Formal meetings designed to promote information sharing through presentations, networking, and discussion panels.
- **Webinars.** Remote information sharing sessions led by subject matter experts on a specific topic
- **Workshops.** Collaborative working group sessions that bring together diverse experts to produce specific content (e.g. Best Practices Workshops)
- **Press Events.** Media events designed to share news or announcements

As illustrated in Figure 5, each type of event has its own set of potential benefits and value proposition. Some events (e.g. Exercises) provide more value when performed on a regular schedule, while others may be done on a more ad-hoc basis. Organizations may consider an appropriate cadence based on their risk landscape and resources to maximize value and avoid event fatigue or overinvestment.

Benefits	Exercises	Cyber Challenges	Conferences	Webinars	Workshops	Press Events
Networking		X	X		X	
Capability Improvement	X	X	X	X	X	
Process Improvement	X			X	X	
External Communication			X		X	X
Recruitment		X	X			X
Industry Alignment	X		X		X	

FIGURE 5: BENEFITS OF EVENTS

Design and execute 3PCE events. Designing and executing events allows automotive industry organizations to better align events to their specific needs. It may also help to establish the organization as an industry leader in vehicle cybersecurity, improving brand image and recruiting. Sometimes, cybersecurity events can be incorporated into existing events or working relationships to avoid duplication of efforts.

Best Practices for designing and executing 3PCE events related to vehicle cybersecurity include:

- Invitations are distributed within and across industries to bring together expertise and foster collaboration
- Guidelines for participant behavior and use of information controls (e.g. confidentiality, ownership agreements) are clearly articulated and documented
- Appropriate legal and ethical oversight is on-hand
- Anti-trust statements are read aloud before commencing the event
- Consideration is given to relevant international concerns (e.g. policy variations, language barriers, etc.)
- Logistics and scheduling enable widespread participation by avoiding conflicting events and largely inconvenient locations
- A specific focus of the event is determined and articulated at the beginning of event planning
- Appropriate staffing and resources are in place to accommodate the event's scale
- Recognized subject matter experts are invited and able to attend

Participate in 3PCE events designed by third parties. Participating in other organizations' events allows automotive industry organizations to benefit from events without committing significant time and resources. It also may help build new capabilities and explore areas outside of an organization's core competencies.

Best Practices for participating in 3PCE events pertaining to vehicle cybersecurity designed by third parties include:

- Participants' roles and responsibilities are aligned with the event's topic of interest
- Participants are aware of anti-trust guidelines
- Participants are aware of what they are (and are not) permitted to share with event attendees
- Participants are prepared to capture insights from the event and provide a recap to the organization

3.4 BEST PRACTICES FOR PROGRAMS

Vehicle cybersecurity programs offer an opportunity to engage in longer term initiatives around a specific goal with third parties.

Identify relevant 3PCE programs. Engaging in vehicle cybersecurity programs can help all facets of vehicle cybersecurity and provide a seat at the table for collective industry decisions. In some cases, resource constraints may limit the number of programs in which an organization can participate, requiring an internal prioritization methodology. Where funding and resources are limited, weighing program requirements, benefits, and relevance will help determine which programs to prioritize.

Types of 3PCE programs pertaining to vehicle cybersecurity include:

- **Intelligence Sharing Programs:** Organizational or industry-wide programs to encourage the disclosure, triage, and remediation of vehicle cybersecurity vulnerabilities
 - Examples include: Auto-ISAC, US-CERT, and the National Vulnerability Database (NVD)
- **Vulnerability Disclosure Programs:** Programs that encourage third parties to report vulnerabilities they find directly to the producer of the product. These programs may be incentivized by monetary payments or other rewards. They may be run in-house or be operated by a third-party vendor.
 - Examples include: individual company coordinated disclosure programs and third party-operated coordinated disclosure programs.
- **Standards Development.** Collaborative efforts to develop vehicle and product cybersecurity standards
 - Examples include: SAE J3061A: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, ISO/AWI 21434: Road Vehicles -- Automotive Security Engineering, and OASIS STIX/TAXII
- **Research Projects.** Joint research ventures regarding a specific vehicle cybersecurity topic
 - Examples include: University partnerships, SAE J3061 Table 35, government-sponsored research (e.g. NHTSA's Vehicle Research and Test Center (VRTC), Automotive Cybersecurity Industry Consortium (ACIC), and Transportation Research Board (TRB))
- **Strategic Talent Development.** Ongoing activities designed to train, educate, and recruit individuals with roles and responsibilities pertaining to vehicle cybersecurity
 - Examples include: Mentorship programs, certifications, and continuing education

Figure 6 outlines the potential benefits and outputs that automotive industry organizations can expect from each program type.

Type of Program	Benefits and Outputs
Intelligence Sharing	<ul style="list-style-type: none"> • Awareness of threat and vulnerability information • Improved cybersecurity processes • Customer protection • Reduced repair requirements • Insight into past solutions and prevention techniques
Vulnerability Disclosure	<ul style="list-style-type: none"> • Awareness of threat and vulnerability information • Improved vulnerability management • Customer protection • Reduced repair requirements • Brand protection and enhancement • Recruiting opportunities
Standards Development	<ul style="list-style-type: none"> • Technical standards, guidelines, and reports • Inform regulatory policy • Insight into past solutions and prevention techniques
Research Projects	<ul style="list-style-type: none"> • In-depth research reports • Information that aids security decision making processes • Guidance on resource allocation and activity prioritization
Strategic Talent Development	<ul style="list-style-type: none"> • Skills development • Exchange of ideas • Recruiting opportunities

FIGURE 6: BENEFITS AND OUTPUTS OF PROGRAMS

Design and execute 3PCE programs. Designing and executing programs allows automotive industry organizations to better align programs to their needs. It also helps to establish the organization as an industry leader in vehicle cybersecurity, improving brand image and recruiting.

Best Practices for designing and executing 3PCE programs with third parties related to vehicle cybersecurity include:

- Planning teams are aware of internal confidentiality and privacy requirements and able to communicate them to third parties
- There is a process to assess participating third parties' value proposition and reputation
- Programs are designed to acquire different perspectives and additional knowledge within a defined group of organizations
- Appropriate business, technical, and legal resources are provided for the program
- The program has a defined scope that is unique and relevant to all parties
- Organizers consider appropriate incentives and motivations to encourage sufficient participation in the program
- Organizers take ownership of the program's outcomes

Participate in 3PCE programs designed by third parties. Participating in other organizations' programs allows automotive industry organizations to benefit from programs without committing significant time and resources. It also may help build new capabilities and explore areas outside of an organization's core competencies.

Best Practices for participating in 3PCE programs with third parties dedicated to vehicle cybersecurity include:

- Participants' roles and responsibilities are aligned with the program's topic of interest
- Participants are aware of anti-trust guidelines
- Participants are aware of what they are (and are not) permitted to share with other program participants
- Participants have an ability to document and publish program findings either internally or publicly, as appropriate
- Participants have defined a process to review program results prior to sharing findings

Appendix A: Glossary of Terms

3PCE terms used in this Guide are defined below.

TERM	DEFINITION
Black Hat	Malicious and/or criminal cyber threat actors
Collaboration and Engagement	Voluntary information sharing activities, events and programs that auto industry stakeholders may pursue with external stakeholders to enhance their vehicle cyber security
Events	Focused, short-term activities to bring together diverse groups of experts
Information Sharing	Efforts to share data, research and other insights
Mitigation Strategy	Potential approach to minimize risks and roadblocks
Programs	Longer-term initiatives to pool resources toward a specific goal
Roadblock	Potential issue that could impede 3PCE initiatives
Third Party	An organization or individual outside of one's organization, that may contribute to vehicle cybersecurity
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 cyber 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
White Hat	Researchers and/or ethical hackers who act to promote and/or enhance vehicle cybersecurity

Appendix B: Additional References and Resources

The following References and Resources provide additional content and expertise for organizations to consider in conjunction with the Best Practices discussed in this Guide.

REFERENCES – DOCUMENTS THAT MAY OFFER ADDITIONAL IMPLEMENTATION GUIDANCE

ABA - What To Do When Your Data is Breached <[link](#)>

AT&T - Hackathon Best Practices <[link](#)>

FTC/DOJ - Memo on Anti-Trust Policy Related to Information Sharing <[link](#)>

ISO/IEC 29147 - Information technology - Security Techniques - Vulnerability Disclosure <[link](#)>

Naval War College - Using Wargames for Command and Control Experimentation <[link](#)>

NTIA - Coordinated Vulnerability Disclosure “Early Stage” Template and Discussion <[link](#)>

NTIA - Vulnerability Disclosures Attitudes and Actions <[link](#)>

NIST – 800 Series <[link](#)>

Open Group –Leveraging Open Trusted Technology Partners in the Supply Chain <[link](#)>

PAXSims - Teaching Professional Wargaming <[link](#)>

SAE International - Cyber Talent Development Events <[link](#)>

Tech Crunch - Hackathon Planning in Less Than 10 Steps <[link](#)>

University of Minnesota - Guidance on Setting up Tabletop Exercises <[link](#)>

US-CERT - External Dependencies Management – US-CERT <[link](#)>

RESOURCES – ORGANIZATIONS THAT MAY OFFER ADDITIONAL INSIGHTS

Auto-ISAC <[link](#)> (For sharing potential vulnerabilities, threats and other information. You are not required to be a Member to share information with Auto-ISAC. Membership eligibility information is also available on the link provided.)

Consumer Technology Association (CTA) <[link](#)>

CERT-CC <[link](#)>

DHS – ICS-CERT <[link](#)>

FCC Communications Security, Reliability, and Interoperability Council <[link](#)>

RESOURCES – ORGANIZATIONS THAT MAY OFFER ADDITIONAL INSIGHTS

Federal Emergency Management Agency (FEMA) <[link](#)>

First.org <[link](#)>

Food and Drug Administration (FDA) <[link](#)>

DHS, Science and Technology <[link](#)>

DHS, Cyber Information Sharing and Collaboration Program <[link](#)>

Institute of Electrical and Electronics Engineers (IEEE) <[link](#)>

International Organization for Standardization (ISO) <[link](#)>

National Cybersecurity and Communications Integration Center (NCCIC) <[link](#)>

National Telecommunications and Information Administration (NTIA) <[link](#)>

National Vulnerability Database (NVD) <[link](#)>

NIST Computer Security Division <[link](#)>

Ready.gov <[link](#)>

SAE International <[link](#)>

US-CERT <[link](#)>

Volpe <[link](#)>

Appendix C: Acronyms

3PCE	Third Party Collaboration and Engagement
ABA	American Bar Association
ACIC	Automotive Cybersecurity Industry Consortium
Auto-ISAC	Automotive Information Sharing and Analysis Center
CERT-CC	Computer Emergency Readiness Team Coordination Center
CTA	Consumer Technology Association
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
DoT	Department of Transportation
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IEEE	Institute of Electrical and Electronics Engineers
IR	Incident Response
ISO	International Organization for Standardization
IT	Information Technology
MOU	Memorandum of Understanding
MTC	Mobility Transformation Center
NCCIC	National Cybersecurity and Communications Integration Center
NDA	Non-Disclosure Agreement
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
OEM	Original Equipment Manufacturer
POC	Point of Contact
SME	Subject Matter Expert

TLP	Traffic Light Protocol
TRB	Transportation Research Board
US-CERT	United States Computer Emergency Readiness Team
VRTC	Vehicle Research and Test Center
V2X	Vehicle-to-Everything Communications