

AUTO-ISAC
AUTOMOTIVE CYBERSECURITY BEST PRACTICES

INCIDENT RESPONSE

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	10 November 2016	
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: Risk Landscape	3
2.1 NEED FOR VEHICLE CYBER INCIDENT RESPONSE	3
2.2 VEHICLE CYBER INCIDENT RESPONSE CHALLENGES.....	3
2.3 THREATS	4
3.0: Best Practices	6
3.1 PREPARE	6
3.2 FIND	9
3.3 FIX.....	12
3.3.1 Coordination	12
3.3.2 Technical Response	13
3.3.3 Business Response	14
3.4 CLOSE	16
Appendix A: Glossary of Terms	18
Appendix B: Additional References and Resources	19
Appendix C: Acronyms	21

1.0: Introduction

1.1 BEST PRACTICES OVERVIEW

This Best Practice Guide is one in a series intended to provide the automotive industry with implementation 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 “Incident Response” 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 automakers, suppliers and auto industry stakeholders as they design, mature and operate their vehicle cyber incident response capabilities.

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.** The Auto-ISAC plans to periodically update this Guide to adapt to the evolving automotive cybersecurity landscape.

1.3 SCOPE

This Guide covers vehicle cyber incident response (IR) best practices for automotive stakeholders throughout the vehicle lifecycle, including design, development, and post-production. These phases are described in Figure 1 below.

**FIGURE 1: VEHICLE LIFECYCLE PHASES**

Vehicle cyber incidents can originate in, or impact, any part of the full vehicle lifecycle, but the Post-Production phase may be where the potential for customer impact is the greatest.

Accordingly, organizations can benefit from defined processes to both identify and respond to events and incidents throughout the lifecycle. Identifying an incident in one phase may not preclude the other phases from being affected and/or considered in the incident response.

It is relevant to incidents originating across the **connected vehicle ecosystem**: The **components** and **infrastructure** on or connected to the vehicle (e.g. product hardware and software, mobile applications, customer data, vehicle data, Wi-Fi networks, Bluetooth connections, and supplier/ manufacturing networks, tooling and development environments, and applications), as well as the **processes** and **organizations** that directly or indirectly touch the vehicle, and may play a role in vehicle cybersecurity. While this Guide was not specifically developed for incidents originating in, or impacting, transportation infrastructure (TI), there is potential relevance, and organizations may wish to consider how they would coordinate response with TI owners.

The Guide does not prescribe or require specific technical or organizational solutions. Rather, this document provides a reference for each company as it develops and refines its individual processes. Please see Section 1.2 for more information.

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 for this document is individuals and teams who are responsible for preparing for, or responding to, cybersecurity incidents related to the vehicle, connected infrastructure, and services. They may represent business (e.g. legal, communications, purchasing) and technical organizations (e.g. engineering, IT) within OEMs, suppliers, and other automotive stakeholders. Example roles include: product cybersecurity managers, support staff, crisis managers, executives, legal counsel, and product managers.

1.5 AUTHORITY AND GUIDE DEVELOPMENT

This Guide was written by the Auto-ISAC Best Practices Working Group, facilitated by Booz Allen Hamilton incident response experts, in coordination with Auto-ISAC Members, including:

AT&T	FCA	Infineon	Nissan
Auto Alliance	Ford	Jaguar Land Rover	NXP
BMW Group	General Motors	Kia	Subaru
Continental	Global Automakers	Magna	Toyota



INCIDENT RESPONSE

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

Cummins
Daimler AG
Delphi
DENSO

Harman
Honda
Hyundai

Mazda
Mercedes Benz
Mitsubishi Motors

Volkswagen
Volvo
ZF

It was developed in coordination with several external stakeholders, including NHTSA, NIST, CERT-CC, and US-CERT.

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: Risk Landscape

This section describes challenges, threats, and risks associated with vehicle cyber incidents.

2.1 NEED FOR VEHICLE CYBER INCIDENT RESPONSE

Vehicle cyber incidents may put consumer safety and privacy at risk, as types of vehicle cyber incidents may include:

- Remote manipulation or control of a vehicle or vehicle ecosystem
- Disruption to operations of the vehicle or vehicle ecosystem
- Unauthorized access of data through the vehicle or vehicle ecosystem

Vehicle cyber IR helps prevent or minimize impact, damage, and costs of a vehicle cyber incident. A mature IR process, tools and capabilities help organizations minimize impact to customer safety and privacy, reduce losses, and maintain customer trust.

2.2 VEHICLE CYBER INCIDENT RESPONSE CHALLENGES

Vehicle cyber incidents can be complex since they have the potential to affect—or originate from—any facet of the connected vehicle ecosystem, including product hardware and software, network connections, mobile applications, customer data, vehicle data, and supplier/manufacturing networks and applications. Moreover, vehicle cyber incidents can impact customer safety, privacy and trust, as well as product reliability and brand reputation. As such, automakers, suppliers and other stakeholders across the connected vehicle ecosystem face a unique set of challenges around vehicle cyber incident response:

- A New Type of Incident: Vehicle cyber incidents may share some commonalities with other incidents the auto industry already faces—including those affecting enterprise IT, vehicle safety, customer privacy, and supply chain continuity—but they are inherently different. They're distinct from IT cyber incidents, as vehicle incidents generally affect products out in the field, whereas IT incidents typically affect resources within enterprise borders. While safety incidents may involve dealer service or repair, vehicle cyber incidents may be identified and fixed without ever physically touching the vehicle. Vehicle cyber IR requires a unique pace of response, managing a different risk landscape, using vehicle ecosystem data to help proactively find and fix issues, and integrating with a variety of internal and external stakeholders. Vehicle cyber IR can benefit from existing processes, but it also transcends them—requiring a new approach to stitch together these existing capabilities, while filling any gaps.
- Asset Management: While OEMs and suppliers have traditionally tracked vehicles and their as-sold parts for various reporting purposes, there's a new level of visibility needed to support vehicle cyber incident detection, triage and response. This entails an accurate asset inventory that provides insights on what's on your vehicles and in the ecosystem around it—current software versions, hardware components, third-party components, and repairs. The challenge is to calibrate a resource that can manage this complexity. Organizations may also refer to the Auto-ISAC's *Risk Assessment and Management Best Practice Guide* for additional information on asset identification and management.
- Organizational Integration: Responding to vehicle cyber incidents requires a unified, enterprise-wide approach. This may include: product cybersecurity, design and engineering, manufacturing, supply chain, safety, quality, legal, communications, public policy, and sales. Organizations should consider how to coordinate with these internal stakeholders, as well as with relevant external stakeholders (e.g. suppliers/OEMs, law enforcement, dealerships).
- Geographic Coordination: The vehicle ecosystem spans geographic regions, so global IR preparation and execution is helpful. For example, regulatory and law enforcement agencies in different countries may have different reporting requirements. Other factors that can complicate global IR include: containment options, legal agreements, legislation, decision authorities, technical/architectural differences, and servicing capabilities.
- Ownership and Consent: Uncertainty about consent to access vehicles can raise challenges around data collection for triaging, forensics, and remediation, as well as deployment of patches or other fixes. This requires careful planning around how to engage and communicate with vehicle owners.

2.3 THREATS

Vehicle cyber incidents to date have predominantly been related to “white hat” exploits publicized in media or research publications. However, threat actor capabilities, motivations, and methods seen in other industries could be repurposed in the automotive context.

The Best Practices discussed in this Guide are applicable to a range of cyber incident outcomes, threat actors, methods, and attack vectors, including the sample set provided below.

INCIDENT RESPONSE

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

Sample Adverse Events <i>What's the outcome?</i>	Sample Methods <i>How can threat actors achieve an adverse event?</i>
<ul style="list-style-type: none">• Remote control of safety-critical functions• Vehicle theft• Disruption of infotainment services• PII breach• Vulnerability exposure or exploit	<ul style="list-style-type: none">• Theft of encryption keys• Malware• Ransomware• Spoofing of vehicle sensors• DDoS
Sample Threat Actors <i>Who's interested and able to attack?</i>	Sample Attack Vectors <i>What are potential entry points into the ecosystem?</i>
<ul style="list-style-type: none">• State-sponsored organizations• Terrorists• Criminals• Malicious insiders• White hat hackers and researchers• Enthusiasts and hacktivists	<ul style="list-style-type: none">• Software• Hardware• Networks and connectivity• Supply Chain• Manufacturing• Dealerships and servicing• Third Parties (e.g. aftermarket, consumer tech)

Organizations may also refer to the Auto-ISAC's *Threat Detection, Monitoring and Analysis Best Practice Guide* for additional discussion on vehicle ecosystem threats

3.0: Best Practices

The purpose of this section is to discuss IR Best Practices and to provide implementation guidance specific to each Sub-Functional area. While some practices may overlap, the scope of this Guide does not include incident detection—this will be discussed in the Auto-ISAC's *Threat Detection, Monitoring and Analysis Best Practice Guide*. Detection is a core input into an organization's incident response capability.

This section is organized to provide best practices aligned to four key phases of the incident response lifecycle: prepare, find, fix, and close.



Organizations may augment these Best Practices and accompanying narrative with the References listed in Appendix B.

3.1 PREPARE

Incident response preparation helps an organization efficiently and effectively react to an incident. Preparing entails planning, training, testing and ongoing improvement.

Document a plan: An organization will benefit from an Incident Response Plan (“IR Plan”) that can be followed when an incident occurs. A comprehensive IR Plan considers several topics and actions, which are described in detail throughout this Guide:

- A process, roles and responsibilities, and resources to guide response (Section 3.1)
- Processes to identify, triage and escalate an incident (Section 3.2)
- Incident coordination, technical and business response activities to contain, remediate and recover from an incident (Section 3.3)
- Processes to close out response activities (Section 3.4)

Best Practices for documenting an IR Plan include:

- The IR Plan defines a vehicle cyber incident

- The IR Plan is easily accessible to response-relevant internal stakeholders; this may include making the Plan and any associated resources available through a central IR Information Sharing Platform
- The IR Plan is coordinated with response-relevant external stakeholders
- The IR Plan documents clear processes to manage the incident response lifecycle, from identification through close out
- The IR Plan is actionable, and provides the guidance necessary to execute
- The IR Plan includes clear decision authority (i.e. levels of approvals and actions)
- The IR Plan reflects regional reporting and regulatory requirements
- There is a process to periodically update and refine the IR Plan
- A Lessons Learned Database captures insights from prior incidents and exercises to help inform periodic updates to the IR Plan

What to Prepare: Sample vehicle cyber IR resources

- ① **IR Plan.** Documents the organization's approach to incident response
- ① **Incident Definition.** Articulates program scope
- ① **Roles and Responsibilities.** Sets expectations for response team roles
- ① **Trigger Criteria.** Helps determine whether an identified event merits escalation to IR
- ① **Severity Matrix.** Creates a standard taxonomy for talking about incident criticality
- ① **Call Sheet.** Specifies primary and back-up members of the IRT, criteria and methods to engage them
- ① **Incident Response Log.** Provides a central platform to document response activities / decisions
- ① **Containment Options Chart.** Details options and processes for containment mechanisms
- ① **Incident Communications Toolkit.** Prepositions templates and processes for external communications
- ① **Success Criteria.** Specifies metrics that indicate successful completion of IR

Establish roles and responsibilities, including decision authorities: An Incident Response Team (IRT) is a cross-functional group of personnel trained to execute the IR Plan. Generally, this team is comprised of internal stakeholders—including those who are the conduits to key external stakeholders (e.g. NHTSA, suppliers, OEMs) and will serve as coordinator to these partners during response. Some organizations, however, may opt to directly include external players in their IRT. In this Guide, engaging external stakeholders is addressed in Section 3.3.3.

An IRT consists of points of contact (POCs) that align to three core functions:

- **Coordination** (includes activities like: administrative management, notification and communications, meeting facilitation, logistics, and documentation of response activities)
- **Technical response** (includes activities like: incident monitoring, analysis, containment, forensics, and remediation)

- **Business response** (managing corporate risk through business activities including: legal, communications, law enforcement/public policy, purchasing, sales, etc.)

Designing an IRT

A vehicle cyber IRT represents a variety of business units and global counterparts to effectively manage business and technical risk. Organizations may include:

- | | |
|--|---------------------------------------|
| ❖ Customer service | ❖ Privacy |
| ❖ Design (systems, networks, hardware, software) | ❖ Product cybersecurity |
| ❖ Engineering | ❖ Public relations and communications |
| ❖ Executive leadership | ❖ Public policy |
| ❖ Human resources | ❖ Purchasing and supply chain |
| ❖ IT security and/or cyber defense | ❖ Quality |
| ❖ Legal counsel | ❖ Safety |
| ❖ Manufacturing | ❖ Sales |

Best Practices for establishing an IRT include:

- There is a single leader identified with ultimate authority for response activities
- The IR Plan articulates roles for all team members (contingent on the type of incident) through the response lifecycle
- The IR Plan includes decision trees and organizational charts to assign team members with decision-making authority; the levels and team members with decision authorities may vary depending on incident severity and type
- Alternates (who are approved to have the same responsibilities and decision authority as their respective primary POCs) are identified and informed of their responsibilities
- The IR Plan appropriately assigns responsibilities and maps key stakeholders to responsibilities
- The IR Plan specifies Success Criteria for each team or response role (e.g. Assessment Team promptly reports potential incidents to appropriate leaders; Business Response Team regularly coordinates and communicates actions to the IR Coordinator, per timelines established in Severity Matrix)

Document a Call Sheet: A Call Sheet enables rapid engagement of appropriate stakeholders across the organization. It also provides a process to facilitate communications with and engage response-relevant stakeholders in the IRT.

Best Practices for documenting a Call Sheet include:

- Primary and secondary POCs for response-relevant business units (including those listed above) are documented in a Call Sheet
- Additionally, the Call Sheet specifies roles and organizations for these POCs, to help find the right person in case identified POCs change positions or are otherwise unavailable
- POCs for each global region are identified
- The Call Sheet documents clear criteria to engage various POCs and in what capacity (e.g. informed, responsible)

- The Call Sheet includes multiple forms of communication (e.g. email, desk phone, cell) in case of failure of any mechanism
- There is a process to periodically review and update this resource

Train and test: Training IRT members on their specific roles and responsibilities may include traditional classroom, web-based, and job experience training, in addition to simulated exercises. Organizations can also consider enterprise-wide training to inform all employees of their role in identifying and reporting incidents.

Best Practices for training and testing the organization include:

- A vehicle IR program ensures the IRT and other response-relevant stakeholders (internal and external) are properly trained and aware of their specific roles and responsibilities
- An organization-wide awareness campaign helps staff understand what a vehicle cyber incident might look like, and how/where to report potential issues
- A vehicle IR program promotes IR preparation through comprehensive testing of the response plan through regular exercises, such as tabletops, drills and wargames
- The frequency, content and focus of exercises and trainings are aligned to program risk
- Training and exercises include periodic review of previous lessons learned

Understand baseline state: Incident assessment requires an understanding of expected vehicle, system, network, and application behaviors to help identify anomalous activity. This includes an understanding on the setup and interactions of the respective components of the vehicle ecosystem to better understand potential attack vectors, root causes, propagation, and attack flow of incidents.

Best Practices for understanding baseline functionality and behavior include:

- A vehicle IR program maintains a profile of characteristics of expected vehicle, system, network, and application behaviors to provide a baseline of normal operations for comparison and restoration during an incident
- A vehicle IR program maintains vehicle, system, network and applications logs to document normal trends and changes over time

3.2 FIND

While some practices may overlap, the scope of this Guide does not include incident detection—this will be discussed in the Auto-ISAC's *Threat Detection, Monitoring and Analysis Best Practice Guide*. The goal of this “Find” phase is to rapidly, consistently, and effectively triage and escalate potential issues that were detected.

Processes for incident evaluation and confirmation help to promote coordinated responses among business and technical stakeholders. This includes engaging legal counsel early to determine a plan to preserve attorney-client privilege during the investigation.

Identify an incident: Organizations can identify potential incidents through a variety of internal (e.g. threat monitoring, perimeter monitoring) and external (e.g. Auto-ISAC intelligence) mechanisms. Symptoms that may indicate a potential cyber incident include:

- Attempts to gain unauthorized access to a system or its data

- Misuse or falsification of systems or data
- Disruption or denial of service (DoS)
- Unauthorized access to vehicle components, computers, networks, servers, routers, firewalls, cloud applications, etc.
- Changes to system hardware or software without approval
- Detection of virus or worm infection, spyware, malware, and ransomware

Best Practices for identifying potential incidents to route through the IR process include:

- There is a documented list (e.g. Collection Matrix) of channels through which a vehicle cyber incident may be detected, including ownership of these sources, as well as sample indicators/thresholds to monitor
- Confirmed and potential incident indicators are logged and monitored in relevant systems across the ecosystem (e.g. vehicle logs, network logs)
- Owners and managers of intel sources and detection mechanisms are educated and familiar with vehicle cyber incident signs and symptoms
- Clear Trigger Criteria help initial assessors determine whether to route the potential issue through the vehicle cyber IR Plan, and who to engage
- Analytics help automate the triage, identification and notification process

Organizations may also refer to the Auto-ISAC's *Threat Detection, Monitoring and Analysis Best Practice Guide* to support incident identification across the vehicle ecosystem.

Log the incident: An Incident Log documents response activities. The purpose of an Incident Log is to document incident details, actions, and to ensure response teams have timely access to information. The Incident Log also helps meet requirements around reporting and evidence collection, and aids in the preparation of an effective after-action report.

Best Practices for creating and maintaining an Incident Log include:

- A process initiates timely analysis of all incoming information to develop the initial assessment
- Access to the Incident Log is monitored and is closely held
- The Severity score is continuously monitored and logged throughout the incident
- Any changes and additions to the Log (including content, time and user) are documented

Validate the incident: Validating incident occurrence and associated information helps an organization evaluate whether IR action is needed. Key questions to consider include:

- Was the incident identified/reported by a credible source?
- Are there sufficient details available to analyze the incident?

Best Practices for validating incident information include:

- Standard validation processes, standards and considerations help ensure potential incidents are appropriately routed for incident response
- When information is deemed to have come from an unreliable source, contain incorrect information, or other issues emerge, the potential issue undergoes additional investigation prior to dismissal

- The IRT provides guidance for next-step actions when a potential incident cannot be validated
- False positives are recorded for historical purposes

Classify and escalate the incident: Assessing the incident's impact and scope helps inform response activities. Incident type, impact and severity may affect the composition of the IRT, expectations around timing of response, and notification procedures. Questions to consider during this assessment include:

- What is the impact?
- What vehicle make(s), model(s), and model year(s) are affected?
- Where is the vehicle in its lifecycle (e.g. pre-production, production, post-production)?
- What sub-systems were affected? What avenue appears to have been exploited to affect the sub-system?
- What is the scope? How many vehicles are affected? Where are the vehicles located?
- How long have the affected controls been affected?

Organizations may also categorize the incident by impact type, defining discrete event categories, such as:

- Unauthorized vehicle control
- Disruption of vehicle functions or services
- Unauthorized access of vehicle, company, or customer data

An incident may also be classified based on its severity level. A cyber Severity Matrix standardizes incident severity scoring based on pre-determined metrics. These scores help standardize expectations for decision authority, level of engagement, timeframes for containment and communications, etc. in line with the risk associated with each particular incident

A Severity Matrix includes factors like:

- Incident timeframe
 - Is the impact ongoing, imminent or concluded?
- Incident impact
 - What is the impact to customer/consumer safety?
 - What types of data were breached?
 - What is the impact to non-safety functions?
 - How could this incident impact brand reputation?
 - How quickly could it spread?

Best Practices for analyzing and classifying an incident include:

- An incident is classified based on severity, likelihood, timeframe, impact, and other metrics as appropriate
- A standard Severity Matrix in the IR Plan creates a taxonomy to quickly classify incidents based on scale, impact and severity
- After severity is determined, the incident is escalated appropriately through pre-defined channels
- Escalation procedures are clearly documented, and may align with incident severity scores and/or incident type

3.3 Fix

This phase focuses on technically fixing the incident (e.g. root cause analysis, containment, remediation), as well as managing business risk through complementary corporate activities (e.g. communications). The foundation of effective technical and business response is coordination: to get the right team in place, notify appropriate stakeholders, and maintain incident coordination throughout.

This section describes best practices around coordination (3.3.1), technical (3.3.2), and business (3.3.3) response.

3.3.1 Coordination

Activate the team: Relevant internal stakeholders across the organization are promptly notified, and the appropriate set of representatives from response-relevant organizations are brought in as part of the IRT. This group may evolve depending on incident type and/or severity, and affected systems.

Effective activation and notification procedures facilitate communications with response-relevant stakeholders in the IRT, which may include:

Sample IRT Members

Stakeholder organizations may include:

- | | |
|--|---------------------------------------|
| ❖ Customer service | ❖ Privacy |
| ❖ Design (systems, networks, hardware, software) | ❖ Product cybersecurity |
| ❖ Engineering | ❖ Public relations and communications |
| ❖ Executive leadership | ❖ Public policy |
| ❖ Human resources | ❖ Purchasing and supply chain |
| ❖ IT security and/or cyber defense | ❖ Quality |
| ❖ Legal counsel | ❖ Safety |
| ❖ Manufacturing | ❖ Sales |

Responsible POCs for the above business units are documented in a call sheet. A call sheet enables rapid engagement of appropriate stakeholders across the organization. The call sheet should consider POCs for each global region.

Best Practices for notifying and engaging internal stakeholders in incident response include:

- There is a consistent process to engage internal stakeholders, including the types of information to share, timeframes for engagement, and methods to notify them
- The composition of the IRT may be different depending on incident severity level, type or other classification features
- An automated alert and notification system instantly and simultaneously contacts all members of the IR Team on multiple devices (e.g. cell, email, text, home phone)
- Back-up communications mechanisms ensure communications are available in case of failure due to power outages, cyber-attacks, or other events
- Secondary POCs are defined for each role or person on the list, so that there is a clear contact in case the primary is unavailable

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.

Communicate response activities: The incident coordination function provides the mechanism to coordinate technical and business response activities, to ensure that they remain in alignment throughout the response. This includes capturing and managing an Incident Log, facilitating information sharing, and overseeing regular status updates.

Best Practices for communicating activities include:

- Incident response activities and decisions are documented through the course of the response in an Incident Log
- There are regular status updates and information sharing meetings to ensure alignment and coordination between relevant technical and business response functions
- A centralized information sharing portal provides a forum where IRT members can readily access status updates, the Incident Log, and other response-relevant information
- Retention, information governance, and data classification policies govern the handling of incident response data and communications
- Technical and business response functions provide regular updates on activities and outcomes with response coordinators or team members as appropriate (e.g. containment is validated and complete, specific messages were shared with customers and/or dealers)

3.3.2 Technical Response

This function fixes the incident from a technical perspective. Activities include: containment, root cause analysis, monitoring, remediation and recovery. The team necessary to fill this role may change depending on incident type, scope, geographic region, and affected vehicle product/service/platform.

Contain the incident: Containment is a critical step to help ensure the incident effects do not continue to spread across the vehicle ecosystem, and may help to remediate its impact. This activity may help limit the risk to the organization and keep critical systems functional, provided they have not been seriously impaired. Incident containment may also provide valuable time for developing a tailored remediation strategy.

A Containment Options Chart documents available containment solutions and actions (e.g. software update, service disconnection, recall). The Chart includes decision guidelines for selecting appropriate containment solutions. Each containment option may have a dedicated playbook to drive appropriate actions.

Best Practices for incident containment include:

- A clear set of containment strategies are pre-defined, for efficient review, approval and execution during incident response
- The containment process includes clear guidelines to confirm containment: eliminating factors that caused the event to be a cyber incident
- Final determination of containment is tested and validated before successful containment is announced to appropriate stakeholders

Develop and communicate a Remediation Plan: After an incident is contained, vulnerability remediation may be necessary. A first step is developing and communicating a plan to provide clear guidance for the IRT to eradicate the source of the incident.

Best Practices for developing an incident remediation plan include:

- Ongoing monitoring and root causing activities help inform the development of the remediation plan
- An incident-specific timeframe, with clear milestones, informs the remediation process
- Previous similar incidents and the associated activities to mitigate those incidents are considered in developing the remediation plan
- Potential remediations are evaluated and tested to determine the appropriate technical fix(es) and their effectiveness
- The Remediation Plan is shared with the full IRT to help align technical and corporate response activities
- There is a clear approval chain that must be processed before deploying any solutions

Implement remediation: Executing the remediation plan entails delivering solutions to eradicate the source of the incident.

Best Practices for implementing an incident remediation include:

- Incident remediation is documented to ensure all steps are completed
- The appropriate incident response tools are used
- The appropriate system owners and experts are engaged to eradicate the incident

Validate remediation: The IRT will perform validation efforts on the affected systems to ensure success of the eradication activities.

Best Practices for validating incident remediation include (as applicable):

- All known instances of malicious code are removed from the network, vehicles, applications, and/or connected infrastructure
- All known communication channels used by the adversary are blocked and monitored
- Integrity of critical components is fully re-established and critical components and systems functioning properly
- Longer term remediation activities may be identified (see Section 3.4)

Validate steady-state recovery: Recovery activities focus on restoring normal operations, and confirm that affected vehicles, services and connected infrastructure are functioning normally. This includes reviewing snapshots of the affected systems prior to the event to compare current and baseline operations. The goal of this process is to ensure recovery took place properly and steady state operations are in effect.

Best Practices for incident recovery include:

- System snap shots are reviewed from a time prior to the incident
- There is a mechanism and standard set of criteria to gauge whether vehicles have been restored to normal steady-state operations
- Targeted monitoring for possible reinfection and attack are in place
- Vulnerability management process is in effect, and includes systematic patching and updates

3.3.3 Business Response

The business response function is responsible for reducing business risk through corporate processes. Activities include: external engagement, external communications, reporting and

notifications, legal and privacy. The team necessary to fill this role may change depending on incident type, scope, geographic region, affected vehicle product/service/platform, and applicable laws and regulations.

Communicate with customers: When an incident affects the customer, proactive, transparent, and responsive communications help maintain their trust.

Best Practices for incident communications include:

- An established process informs review and approval of information used to engage customers, and key customer interfaces (e.g. dealerships, customer service)
- An Incident Communications Tool Kit—including pre-positioned talking points, press releases, and other communications templates—is in place and approved ahead of an incident to expedite any external communications

Engage external stakeholders: Organizations are responsible for informing appropriate external stakeholders of an incident, and sometimes may need to engage these stakeholders in response. For example, this may include owners of TI in case an incident has potential to impact, or originates in, TI. Engaging the media may also help control messaging.

External stakeholders may include:

- OEMs/Suppliers
- Service providers
 - Telecom provider
 - Application service providers
 - Insurance providers
 - Identity management and authentication service providers
- Customers interfaces
 - Call centers
 - Dealerships
 - Website submission
 - Social media
- Government
 - DHS
 - ICS-CERT
 - NCCIC
 - US-CERT
 - DOT
 - Crisis Management Center
 - NHTSA
 - DOJ
 - FBI – Office of Technology Division
 - FBI – National Cyber Investigative Joint Task Force
 - FCC
 - FTC
 - State Government (e.g. State DOT, local law enforcement)
- Other third parties
 - Auto-ISAC

- Security researchers

Best Practices for engaging external stakeholders in incident response include:

- An established process informs review and approval of information used to engage external stakeholders, and internal staff beyond the IRT
- Primary and secondary POCs for each organization are documented, and regularly updated
- Exercises include internal and external stakeholders, to test these relationships and roles and responsibilities

Address reporting requirements: Some incidents may require the intervention of the authorities. Proper reporting protocols help the IRT to report the incident to relevant authorities. Sample conditions for reporting cybersecurity incidents include:

- Private information has been (or might have been) breached
- There is (or might be) a public safety risk
- There is (or might be) physical harm to employees

Best Practices to report incidents include:

- Working in conjunction with Legal Counsel helps ensure the company is within the scope of legal boundaries and requirements
- Escalating the incident information to the corporate regulatory function (e.g. legal, public policy, public relations, crisis management teams) helps ensure the incident is properly reported
- Standard procedures for communicating with external stakeholders, such as the FBI, local police, or government agencies, helps ensure the incident is appropriately routed through and coordinated with local law enforcement
- These standard operating procedures (SOPs) are regularly tested, reviewed and revised

Oversee legal requirements: There are times where an incident may require legal action (including prosecution of threat actors, or managing liability claims associated with the incident).

Best Practices to handle legal proceedings associated with an incident include:

- The Incident Log captures the necessary information (e.g. decisions and timing, key actors) to enable legal proceedings
- Technical response activities and forensics are coordinated with Legal Counsel to ensure compliance with information storage and reporting, chain of evidence, eDiscovery and other similar requirements
- Retention, information governance, and data classification policies govern the handling of incident response data and communications

3.4 CLOSE

Post incident, it is important to reflect on the response process to assess strengths and weaknesses, and consider and implement any longer-term remediation controls. This includes evaluating the IR Plan to continuously evolve it to reflect new threats, improved technology, and lessons learned.

Conduct a debrief: An incident debriefing reviews the effectiveness of the response procedures to determine necessary procedure or policy changes. Discussion questions may include:

- Did the IR Plan sufficiently guide the response?
- Was the IRT adequately trained and prepared?
- Do additional POCs need to be added to the call list?
- Did the incident response work? What, if anything, did not work?
- Is the organization still vulnerable from the incident?

Best Practices for debriefing incident response include:

- An assessment collects feedback from IRT members and other appropriate stakeholders
- This debrief brings clarity to the root cause of the incident, and informs retroactive analysis
- This assessment is captured in an after action report, which is made available to relevant stakeholders
- Lessons learned described in the after action report help inform future plan updates

Implement long-term remediation controls: A plan for longer-term remediation controls helps minimize recurrence of the incident by improving design and test stages of the product lifecycle, as well as detection and incident response activities. The IRT or other stakeholders may be assigned to execute this plan. Depending on the scope and complexity, this plan may incorporate technical and/or business remediation activities.

Best Practices for implementing long-term remediation controls include:

- There is a documented process and mandate to identify industry leading tools and technologies to help address and fix identified areas for improvement
- Remediation measures are reusable and repeatable for long-term use
- A clear tracking and accountability system is in place to monitor rebuilding and adjustments to system tools which are found to be misaligned after an assessment.

Update the plan: The results of the debrief help identify potential areas to revise the IR Plan to expedite and improve incident response. Additional information is provided in Section 3.1.

Best Practices to continuously improve the IR Plan include:

- Lessons learned from the incident response assessment are extracted and shared with the IRT (e.g. through a Lessons Learned Database)
- Lessons learned are incorporated into periodic IR Plan updates
- Implementation of these lessons learned is tested through exercises
- The Call Sheet is periodically updated to reflect any changes to POCs

Appendix A: Glossary of Terms

Incident Response terms used in this Guide are defined below.

TERM	DEFINITION
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability or confidentiality
Exercise	A planned event during which an organization simulates a cyber incident to develop or test capabilities
Threat	Any circumstance or event with the potential to adversely impact the vehicle ecosystem through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
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
Vehicle Cyber Incident	An occurrence that actually or potentially results in adverse consequences to a vehicle, connected infrastructure, or information that the vehicle processes, stores, or transmits and that may require a response action to mitigate the consequences
Vehicle Cyber Incident Response Plan	A predetermined and documented process, tools/resources, and roles and responsibilities to identify and respond to a vehicle cyber incident
Vehicle Cyber Incident Response	A capability to identify and respond to a vehicle cyber incident
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.
White Hat	Researchers and/or ethical hackers who act to promote and/or enhance vehicle cybersecurity

Appendix B: Additional References and Resources

Best Practices included in this Guide leverage content from established incident response best practices and standards.

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

CIS: Security Controls

NHTSA: Cybersecurity Best Practices for Modern Vehicles

NIST: Cyber Security Framework

NIST 800-61: Security Incident Handling Guide

NIST SP 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

ISO/IEC FDIS 27035-2: Part 2: Guidelines to Plan and Prepare for Incident Response

ISO/IEC 27035:2011: Information Security Incident Management

ISO/IEC 29147: Vulnerability Disclosure

ISO/IEC 30111: Vulnerability Handling Process

PPD 41: US Cyber Incident Coordination

SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

US-CERT NCIRP: National Cyber Incident Response Plan

US-CERT: Federal Incident Notification Guidelines

RESOURCES

CERT® Coordination Center, Carnegie Mellon University (CERT®/CC) [<link>](#)

FBI / National Cyber Investigative Joint Task Force [<link>](#)

Forum of Incident Response and Security Teams (FIRST) [<link>](#)

Government Forum of Incident Response and Security Teams (GFIRST) [<link>](#)

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [<link>](#)



INCIDENT RESPONSE

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

National Initiative for Cybersecurity Careers and Studies (NICCS) <[link](#)>

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

SysAdmin, Audit, Network, Security (SANS) Institute <[link](#)>

United States Computer Emergency Readiness Team (US-CERT) <[link](#)>

U.S. Department of Transportation / Crisis Management Center (CMC) <[link](#)>

Appendix C: Acronyms

Auto-ISAC	Automotive Information Sharing and Analysis Center
CERT-CC	Computer Emergency Response Teams Coordination Center
CIS	Center for Internet Security
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DOJ	Department of Justice
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FIRST	Forum of Incident Response and Security Teams
FTC	Federal Trade Commission
G-FIRST	Government Forum of Incident Response and Security Teams
ICS-CERT	Industrial Control System Computer Emergency Response Teams
IR	Incident Response
IRT	Incident Response Team
ISO	International Organization for Standardization
IT	Information Technology
NCCIC	National Cybersecurity and Communications Integration Center
NHTSA	National Highway Traffic Safety Administration
NICCS	National Initiative for Cybersecurity Careers and Studies
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
PII	Personally Identifiable Information
POC	Point of Contact
SAE	Society of Automotive Engineers
SANS	System Administration, Networking, and Security Institute
SOP	Standard Operating Procedure



INCIDENT RESPONSE

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

TI	Transportation Infrastructure
TLP	Traffic Light Protocol
US-CERT	United States Computer Emergency Readiness Team