autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

**Addendum to Auto Care's March 12 Comments RE: "Cyber Best Practices for the Safety of Modern Motor Vehicles."**

**Mapping SVI to NHTSA Best Practices 2.26.2021**

The Auto Care Association supports the implementation of a standardized interface to the vehicle utilizing ISO standards: 21177, 21185 and 21184. Unofficially, this collection of standards is referred to as Secure Vehicle Interface (SVI). Use of these international standards would provide for the establishment of a secure interface to the vehicle, while still allowing access to specific data by authenticated and authorized users for specifically identified and authorized vehicle services.

- ISO 21177 specifies access control policies and mechanisms for enforcing them, allowing different access control requirements for access to different resources. Access control is enabled by cryptographic authentication and by authorization processes associated with that authentication.
- ISO 21185 specifies a methodology to define communication profiles based on standardized communication protocols to interconnect trusted devices. These profiles enable secure information exchange between such trusted devices.
- ISO 21184 specifies methods for mapping non-standardized data into a common format in order to support the control of access to specific types of data. This allows for the access to specific data to be controlled on the bases of a confirmed need and a confirmed authorization, along with authentication and certification.

The same security standards specified in ISO 21177 along with IEEE1609.2 are being utilized for V2V, and a similar implementation is being developed for secure charging of Electric Vehicles (EV). It therefore seems extremely practical to leverage a common standardized secure interface for all access to vehicle data types based on authentication and authorization by registered, certified and authorized devices. SVI supports the ability to define data types e.g., maintenance data for access by only devices and users who have been authenticated and authorized for that specific data type. The standards also support the ability to define service IDs for mapping a particular data type to a particular service to be performed. Adoption of SVI would create a more secure interface while establishing a open interface for authorized uses.

The following table maps the technical capabilities and design considerations of the SVI as well as the role of aftermarket providers against the best practice guidelines proposed by NHTSA.

**Mapping of SVI Against NHTSA General Best Practices**

| ID | Description | SVI Support |
|---|---|---|
| G.1 | The automotive industry should follow the National Institute of Standards and Technology's (NIST's) documented | The SVI architecture is designed to support the NIST framework. The inclusion of independent repair services as members of the vehicle telematics |

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

| | | |
|---|---|---|
| | Cybersecurity Framework, which is structured around the five principal functions "Identify, Protect, Detect, Respond, and Recover," to build a comprehensive and systematic approach to developing layered cybersecurity protections for vehicles. | community will greatly increase the number of parties who can potentially identify, detect, and respond to new threats. |
| G.2 | Companies developing or integrating vehicle electronic systems or software should prioritize vehicle cybersecurity and demonstrate executive management commitment and accountability | The SVI authentication and messaging standards have been developed with a security-first perspective. These standards seek to balance the privacy and rights of vehicle owners against the prevalence of cybersecurity threats. |
| G.3 | The automotive industry should follow a robust product development process based on a systems-engineering approach with the goal of designing systems free of unreasonable safety risks, including those from potential cybersecurity threats and vulnerabilities. | AutoCare appreciates the need to increase the level of rigorous process and testing needed in future automotive systems. It is assumed that the on-board units deployed to implement the SVI telematics protocols would all be developed to rigorous automotive cybersecurity standards. |
| G.4 | This process should include a cybersecurity risk assessment step that is appropriate and reflects mitigation of risk for the full life-cycle of the vehicle. | As fully documented, thoroughly reviewed international standards, the technical components of the SVI and the process used to create them are all accessible to rigorous risk review. |
| G.5 | Safety of vehicle occupants and other road users should be of primary consideration when assessing risks. | AutoCare fully agrees that safety is paramount, followed immediately by the need to protect the privacy and data access rights of vehicle owners. |
| G.6 | Manufacturers should consider the risks associated with sensor vulnerabilities and potential sensor signal manipulation efforts such as GPS spoofing, road sign modification Lidar/Radar jamming and spoofing, camera blinding, or excitation of machine learning false positives | A key part of protecting sensors is to ensure that sensor data is properly calibrated and validated after a repair. The SVI technology allows all authorized and trained service technicians to properly calibrate and test sensors. |
| G.7 | Any unreasonable risk to safety-critical systems should be removed or mitigated to acceptable levels through design, and any functionality that presents an unavoidable and unnecessary risk should be eliminated where possible. | |
| G.8 | For remaining functionality and underlying risks, layers of protection[17] that are appropriate for the assessed risks should be designed and implemented. | The integration of SVI technology into a vehicle shall, by design and intent, follow a layered approach. The use of a secure OBU or gateway is strongly recommended as a means of isolating and protecting internal networks from the telematics interface. |

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

| | | |
|---|---|---|
| G.9 | Clear cybersecurity standards should be specified and communicated to the suppliers that support the intended protections.[18] | AutoCare is an active supporter of cybersecurity standards providing extensive technical review, evaluation, and comments on open standards. Sharing of vehicle manufacturer specifications should be extended to include after-market device manufacturers. |
| G.10 | Manufacturers should maintain a database of operational software components used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime. | This database should be made available to vehicle owners and any technical representatives that they choose to share it with, so that owners can make informed decisions about the security state of their vehicles or fleets. |
| G.11 | Manufacturers should track sufficient details related to software components, such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software, manufacturers can quickly identify what ECUs and specific vehicles would be affected by it. | |
| G.12 | Manufacturers should evaluate all commercial off-the-shelf and open-source software components used in vehicle ECUs against known vulnerabilities | Agreed, the same level of scrutiny should be applied to telematics infrastructure components and diagnostic tools used to access vehicle networks. |
| G.13 | Manufacturers should also pursue product cybersecurity testing, including using penetration tests, as part of the development process. | Penetration tests are most effective when applied against open, well documented and publicly reviewed standards. AutoCare recommends that all telematics applications follow international standards. |
| G.14 | Test stages should employ qualified testers who have not been part of the development team, and who are highly incentivized to identify vulnerabilities. | It is far easier to find qualified, independent test experts when the system under test follows an approved international standard. |
| G.15 | A vulnerability analysis should be generated for each known vulnerability assessed or new vulnerability identified during cybersecurity testing. The disposition of the vulnerability and the rationale for the how the vulnerability is managed should also be documented. | |
| G.16 | In addition to design protections, the automotive industry should establish rapid vehicle cybersecurity incident detection and remediation capabilities. | Independent repair technicians who are granted access to vehicle data by the vehicle owner can provide independent support for this critical oversight and reporting role. |
| G.17 | Such capabilities should be able to mitigate safety risks to vehicle occupants | A qualified repair technician, provided with adequate access to vehicle data, is uniquely positioned to |

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

| | | |
|---|---|---|
| | and surrounding road users when a cyber-attack is detected and transition the vehicle to a minimal risk condition, as appropriate for the identified risk. | provide this service for vehicles as they age and move out of warranty support provided by the OEM. |
| G.18 | Manufacturers should collect information on potential attacks, and this information should be analyzed and shared with industry through the Auto-ISAC. | As trusted members of the automotive support community, independent repair shops will support this important detection and reporting role. |
| G.19 | Manufacturers should fully document any actions, design choices, analyses, supporting evidence, and changes related to its management of vehicle cybersecurity. | All such actions and changes should also be made available to independent repair technicians. |
| G.20 | All related work products should be traceable within a robust document version control system. | And made available to the vehicle repair and support community. |
| G.21 | Companies should use a systematic and ongoing process to periodically re-evaluate risks and make appropriate updates to processes and designs due to changes in the vehicle cybersecurity landscape, as appropriate. | |
| G.22 | Best practices for secure software development should be followed, for example as outlined in NIST 8151[3]and ISO/SAE 21434. | |
| G.23 | Manufacturers should actively participate in automotive industry-specific best practices and standards development activities through Auto-ISAC and other recognized standards development organizations. | Automotive tool vendors should be included in this community and follow the same standards, also reporting their findings to the Auto-ISAC. |
| G.24 | Members of the extended automotive industry (including, but not limited to, vehicle manufacturers, automotive equipment suppliers, software developers, communication services providers, aftermarket system suppliers, and fleet managers) are strongly encouraged to join Auto-ISAC and share information. | AutCare encourages tool vendors and independent repair organization to be active members of Auto-ISAC. |
| G.25 | Members of the Auto-ISAC are strongly encouraged to collaborate in expeditiously exploring containment options and countermeasures to reported | The inclusion of the after-market community will greatly diversify and expand the breadth of insight available to this community. |

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

| | | |
|---|---|---|
| | vulnerabilities, regardless of an impact on their own systems. | |
| G.26 | Automotive industry members should create their own vulnerability reporting policies and mechanisms | |
| G.27 | Members of the automotive industry should develop a product cybersecurity incident response process | This process should include communications channels where authorized technicians can report evidence of potential threats and get a rapid response to security questions or concerns. |
| G.28 | Organizations should develop metrics to periodically assess the effectiveness of their response process | Repair tool vendors are encouraged to follow the same best practice. |
| G.29 | Organizations should document the details of each identified and reported vulnerability, exploit, or incident applicable to their products. These documents should include information from onset to disposition with sufficient granularity to support response assessment. | Repair tool vendors are encouraged to follow the same best practice. |
| G.30 | Commensurate to assessed risks, organizations should have a plan for addressing newly identified vulnerabilities on consumer-owned vehicles in the field, inventories of vehicles built but not yet distributed to dealers, vehicles delivered to dealerships but not yet sold to consumers, as well as future products and vehicles | This recommendation would be stronger if it explicitly declared older, out of warranty vehicles as part of the fleet that must be monitored and managed. |
| G.31 | Any incidents should also be reported to CISA/United States Computer Emergency Readiness Team (US-CERT) in accordance with the US-CERT Federal Incident Notification Guidelines | |
| G.32 | Industry members should periodically conduct and participate in organized, cyber incident response exercises. | These exorcises should periodically include dealer networks and independent repair technicians. |
| G.33 | The automotive industry should document the details related to their vehicle cybersecurity risk management process to facilitate auditing and accountability. | A subset of the risk management process should be made available to independent repair shops with a clear definition o their role. |
| G.34 | Further, such documents should be retained through the expected life span of the associated product. | And access to these documents, procedures, and interfaces must be maintained through the life of the vehicle. |

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

| | | |
|---|---|---|
| G.35 | Documents should follow a robust version control protocol, and should be revised regularly as new information, data, and research results become available. | |
| G.36 | The automotive industry should establish procedures for internal review of its management and documentation of cybersecurity-related activities. | |
| G.37 | The automotive industry should consider carrying out organizational and product cybersecurity audits annually. | Similarly, tool vendors and independent repair facilities (or networks of facilities) should be encouraged to self-audit their practices and preparedness. |
| G.38 | Vehicle manufacturers, suppliers, universities, and other stakeholders should work together to help support educational efforts targeted at workforce development in the field of automotive cybersecurity | Qualified independent repair technicians and tool vendors should be included in this community. |
| G.39 | The automotive industry should consider the incremental risks that could be presented by these devices when connected with vehicle systems and provide reasonable protections. | The adoption of a standards-compliant telematics interface will greatly diminish the need for the deployment of unregulated, ad-hoc aftermarket devices and greatly reduce the potential threat to vehicle safety. |
| G.40 | Any connection to a third-party device should be authenticated and provided with appropriate limited access. | The SVI architecture provides a common, standards-compliant mechanism for authentication and enforcement of fine-grain access control. |
| G.41 | Aftermarket device manufacturers should employ strong cybersecurity protections on their products. | Adoption of the SVI approach would bring strict enforcement of international standards and best practices for all access to telematics data from vehicles. |
| G.42 | The automotive industry should consider the serviceability of vehicle components and systems by individuals and third parties. | Adoption of the SVI will greatly expand the service and repair options available to vehicle and fleet owners. This is particularly true for vehicles that are in use beyond the warranty period. |
| G.43 | The automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by alternative third-party repair services authorized by the vehicle owner. | The SVI has been designed specifically to address this need by applying international standards and rigorous security and safety requirements. |

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

**Appendix B: Mapping of SVI Against NHTSA Technical Best Practices**

| ID | Description | SVI Support |
|---|---|---|
| T.1 | Developer-level access should be limited or eliminated if there is no foreseeable operational reason for the continued access to an ECU for deployed units. | Post-production diagnostic and repair of vehicles should be performed through a standards-compliant, authenticated interface such as the SVI. |
| T.2 | If continued developer-level access is necessary, any developer-level debugging interfaces should be appropriately protected to limit access to authorized privileged users. | Fine-grain access control should be applied to sensitive vehicle diagnostic data and procedures, vehicle owners should be able to enable authorized independent technicians and tool vendors to access data and interfaces in their vehicle. |
| T.3 | Cryptographic credentials that provide an authorized, elevated level of access to vehicle computing platforms should be protected from disclosure. | When proper authorization and authentication infrastructure is available, there is no need to expose or share credentials in order to grant access to vehicle systems. |
| T.4 | Any credential obtained from a single vehicle's computing platform should not provide access to multiple vehicles. | The SVI architecture ensures that every vehicle and repair tool must have a unique and authenticated identity validated using secure credentials. |
| T.5 | Diagnostic features should be limited, as much as possible, to a specific mode of vehicle operation which accomplishes the intended purpose of the associated feature. | An SVI implementation may restrict repair procedures using very fine-grain controls. Access can be restricted to a limited period of time, or to only a select set of repair procedures. |
| T.6 | Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they were misused or abused outside of their intended purposes | This principle is reinforced by the elimination of secret or proprietary access and repair protocols. An explicit requirement to enable access by third party providers reduces any temptation to overlook internal security threats. |
| T.7 | The use of global symmetric keys and ad-hoc cryptographic techniques for diagnostic access should be minimized. | A saleable infrastructure is needed to issue security credentials to vehicles and to authorize access by independent technicians. |
| T.8 | Vehicle and diagnostic tool manufacturers should control tools' access to vehicle systems that can perform diagnostic operations and reprogramming by providing for appropriate authentication and access control | As trusted members of the vehicle cybersecurity community, tool vendors should work closely with manufacturers to create and implement secure an reliable repair procedures. |
| T.9 | When possible, critical safety signals should be transported in a manner inaccessible through external vehicle interfaces. | This is consistent with the SVI's gateway architecture. In this design, critical internal networks and signals can only be accessed using a secure proxy application. |
| T.10 | Critical safety messages, particularly those passed across non-segmented | The SVI architecture does not impose any restrictions on in-vehicle networks. Strong |

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

| | | |
|---|---|---|
| | communication buses, should employ a message authentication method to limit the possibility of message spoofing. | authentication and validation of internal messages is encouraged and is fully compliant with the gateway design. |
| T.11 | A log of events sufficient to reveal the nature of a cybersecurity attack or successful breach and support event reconstruction should be created and maintained. | It is further recommended that a durable copy of this log be maintained within the vehicle for examination by multiple authorized parties. While it is encouraged that security alerts be delivered through a remote telematics interface, this should not eliminate or replace on-board logging. |
| T.12 | Such logs that can be aggregated across vehicles should be periodically reviewed to assess potential trends of cyber-attacks. | Independent repair tools and shops can support collection and reporting of in-vehicle log data, provide that an appropriate interface is made available for delivering logs. |
| T.13 | Manufacturers should treat all networks and systems external to a vehicle's wireless interfaces as untrusted and use appropriate techniques to mitigate potential threats | This is consistent with the SVI design. The gateway architecture places a security layer in-between the remote telematics interface and all internal networks. The telematics interface is always treated until a request can be validated and authorized. |
| T.14 | Network segmentation and isolation techniques should be used to limit connections between wireless-connected ECUs and low-level vehicle control systems, particularly those controlling safety critical functions, such as braking, steering, propulsion, and power management. | This is consistent with the SVI design. |
| T.15 | Gateways with strong boundary controls, such as strict whitelist-based filtering of message flows between different network segments, should be used to secure interfaces between networks. | The SVI architecture provides a standards-based method of implementing this best practice. |
| T.16 | Eliminating unnecessary internet protocol services from production vehicles. | The SVI architecture places a secure gateway between any telematics interface and the internal vehicle networks, clearly separating in-vehicle systems from external protocols. |
| T.17 | Limiting the use of network services on vehicle ECUs to essential functionality only | The SVI gateway handles complex external protocols and requests on behalf of the vehicle. This allows internal ECUs to be restricted to robust, reliable communications protocols and restricted functions. |
| T.18 | Appropriately protecting services over such ports to limit use to authorized parties | The use of authorization and fine-grain access controls ensure that only authorize requests will be granted access to vehicle data and procedures. |
| T.19 | Manufacturers should use appropriate encryption and authentication methods in | The SVI design applies international standards for authentication and authorization. |

autocare ASSOCIATION
Independence drives us.

7101 Wisconsin Avenue
Suite 1300
Bethesda, MD 20814
www.autocare.org

T: 301.654.6664
F: 301.654.3299
info@autocare.org

| | | |
|---|---|---|
| | any operational communication between external servers and the vehicle | |
| T.20 | Manufacturers should plan for and create processes that could allow for quickly propagating and applying changes in network routing rules to a single vehicle, subsets of vehicles, or all vehicles connected to the network. | The certificate-based approach recommended by the SVI architecture encourages the use and rapid deployment of certificate revocation lists (CRLs). This is a well-known mechanism to dynamically reduce or eliminate access from systems that are suspected to be compromised. |
| T.21 | Automotive manufacturers should employ state-of-the-art techniques for limiting the ability to modify firmware to authorized and appropriately authenticated parties. | The SVI architecture can enable independent technicians to deliver factory authorized, digitally signed software updates to vehicle systems. |
| T.22 | Maintain the integrity of OTA updates, update servers, the transmission mechanism and the updating process in general | The SVI design is fully supportive of and consistent with OTA update mechanisms provided that direct deployment of updated or patched software can be initiated and prioritized over the OTA update in cases where the OTA system is delayed. |
| T.23 | Take into account, when designing security measures, the risks associated with compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities. | The international standards-based mechanisms employed in the SVI are designed to account for all of these considerations. |