Cybersecurity Requirements for Telematics Systems

May 2020
Acknowledgments

We would like to acknowledge the contributions of DOT/Volpe Center and the members of the Cybersecurity Requirements for Telematics Systems working group. At the time this report was published, named participants included Derek Held of Zonar Systems, several representatives from Geotab, Altaz Valani of Security Compass, Mark Zachos, President of DG Technologies, Bill Brown, Retired Manager of Fleet Telematics, and Richard M. Litwinczuk, Senior Cybersecurity Engineer, Land Cyber Mission Assurance Program DND. The working group benefited greatly from the contributions of several other fleet managers and telematics service providers (TSPs) who wish to remain anonymous.

The authors would also like to acknowledge the contributions of the NMFTA Request for Proposal Contract Template Language (RFPCTL) working group.
Contents

Acknowledgments .................................................................................................................................................. 2

List of Figures .................................................................................................................................................... 3
List of Tables ....................................................................................................................................................... 3
List of Abbreviations ......................................................................................................................................... 4
Foreword ............................................................................................................................................................. 5
Preface .................................................................................................................................................................. 6
Executive Summary ............................................................................................................................................... 7
Introduction ........................................................................................................................................................ 8
Requirements Matrix Description ...................................................................................................................... 11
Recommendations and Conclusions .................................................................................................................. 14
References .......................................................................................................................................................... 15
Appendix A: Telematics Cybersecurity Requirements ...................................................................................... 16

List of Figures

Figure 1. Abstracted Telematics, Fleet Management Information Systems (FMIS) and/or ELD .................... 8

List of Tables

Table 1. Sample Requirement for Reference .................................................................................................... 11
## List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASVS</td>
<td>Application Security Verification Standard</td>
</tr>
<tr>
<td>BSIMM</td>
<td>Building Security in Maturity Model</td>
</tr>
<tr>
<td>CAIQ</td>
<td>Consensus Assessment Initiative Questionnaire</td>
</tr>
<tr>
<td>CTIA</td>
<td>Cellular Telecommunications and Internet Association</td>
</tr>
<tr>
<td>Cyber ITL</td>
<td>Cyber Independent Testing Labs</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DOT</td>
<td>Department of Transportation</td>
</tr>
<tr>
<td>DOT</td>
<td>Department of Transportation</td>
</tr>
<tr>
<td>ELD</td>
<td>Electronic Logging Device</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>FM</td>
<td>Fleet Manager</td>
</tr>
<tr>
<td>FMI</td>
<td>Fleet Management Information</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IS</td>
<td>Information System</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IVG</td>
<td>Intelligent Vehicle Gateway</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Controls</td>
</tr>
<tr>
<td>MASVS</td>
<td>Mobile Application Security Verification Standard</td>
</tr>
<tr>
<td>MSTG</td>
<td>Mobile Security Testing Guide</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NMFTA</td>
<td>National Motor Freight Traffic Association, Inc.</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Proposal</td>
</tr>
<tr>
<td>RFPCTL</td>
<td>Request for Proposal Contract Template Language</td>
</tr>
</tbody>
</table>
Foreword

After the US DOT/Volpe published “Telematics Cybersecurity Primer for Agencies” in June 2017, we wanted to create resources for use by our motor freight carrier members to procure new telematics systems such as Electronic Logging Devices (ELD). Starting with the telematics cybersecurity controls and recommendations made by the Primer, a working group was assembled to complete a detailed list of testable cybersecurity requirements for all the components of a telematics system. We are fortunate to have been able to collaborate with DOT/Volpe and to see the efforts of the working group come to fruition through the publications of this report, which is a natural refinement of the security controls defined in the Primer.

Urban Jonson, CTO National Motor Freight Traffic Association, Inc. (NMFTA)
Preface

The purpose of this document is to provide government agency Fleet Managers and private industry stakeholders (e.g. TSPs, carriers, OEMs, Tier 1 suppliers, and others) responsible for the selection and procurement of Telematics, Fleet Management Information Systems (FMIS) and/or ELDs with situational awareness of potential cybersecurity risks of deploying such systems. This report also delivers a comprehensive list of cybersecurity requirements that should be satisfied by all components of a Telematics, Fleet Management Information System (FMIS) and/or Electronic Logging Devices (ELD), including validation steps for federal agencies and private industry stakeholders when deploying such systems.

The audience for this report are the agencies and private industry stakeholders responsible for the selection and procurement of Telematics, Fleet Management Information Systems (FMIS) and/or ELDs, as was the case in the previously released “Telematics Cybersecurity Primer for Agencies” report. The working group believes that any stakeholder that must procure Telematics, FMIS and/or ELDs will also find the requirements outlined in this document relevant. The complete list of requirements outlined in Appendix A will remain a living document which can respond to feedback from industry and technical experts. The requirements are hosted at https://github.com/nmfta-repo/nmfta-telematics_security_requirements and readers are encouraged to check there for updates to, and to offer feedback on, the requirements.
Executive Summary

The comprehensive list of cybersecurity requirements for Telematics, FMIS and/or ELDs presented here was developed in collaboration with a diverse working group. The requirements are prioritized and include references to public authoritative sources containing more information, should the reader require additional details. The complete listing will provide purchasers with sufficient information to prioritize the need for cybersecurity in the Telematics, FMIS and/or ELD as well as validate the presence of the controls upon delivery of a system.

It is the recommendation of the working group that agencies and private stakeholders use these cybersecurity requirements when procuring new Telematics, FMIS and/or ELDs as well as when evaluating their current systems when the need to evaluate cybersecurity arises. The working group continues to refine the requirements and the reader is encouraged to visit https://github.com/nmfta-repo/nmfta-telematics_security_requirements to obtain the most up-to-date copy of the requirements, which is also available in a supplier questionnaire format. The site should also be used to give feedback to the working group on ways that the requirements can be further refined. It is NMFTA’s recommendation that motor freight carriers use these requirements as a natural successor to “Telematics Cybersecurity Primer for Agencies.”

The complete list of cybersecurity requirements can be found in Appendix A. Requirements are prioritized for use by stakeholders via a Criticality field to encourage adoption incrementally. These requirements are presented for all the components of a Telematics, FMIS and/or ELD: Physical In-cab, Connectivity/Communications, Mobile App, and Cloud or Back-end and must be taken in their entirety for any assurances of cybersecurity to be realized.
Introduction

The deployment of Telematics, FMIS and/or ELDs in motor vehicles is pervasive today. As with any Information System (IS), it is the owner/operator of that system who bears the responsibility for managing the security of that system. This includes security of the information being collected, managed and stored, but also the security of the assets being monitored which – if not considered in procurement – could have their security posture worsened by the introduction of a Telematics, FMIS and/or ELD. In the case of agencies as the owners of an IS, their responsibility is detailed in the Federal Information Security Management Act of 2014\(^1\).

A core objective of this document is to provide information to owners of Telematics, FMIS and/or ELDs in the phases of procurement of these systems so they can manage risks to security. An additional objective is to provide comprehensive cybersecurity requirements that can be consulted by the owner and potential vendors to provide sufficient information that can prioritize the needs for cybersecurity in the Telematics, FMIS and/or ELD and validate the presence of the controls upon delivery of the system.

The approach taken to create this list included consultations with many authoritative sources of cybersecurity controls and then mapping them to the components of a Telematics, FMIS and/or ELD. To do this, the report considers a simplified model of a Telematics, FMIS and/or ELD. The four components of such a simplified system are broken down by Physical In-cab, Connectivity/Communications, Mobile App, and Cloud or Back-end and are depicted in Figure 1 below:

![Diagram of Telematics, Fleet Management Information Systems (FMIS) and/or ELD](#)

---

The Cybersecurity Requirements for Telematics Systems matrix uses the following terms for the components of a Telematics, FMIS and/or ELD:

- **Physical In-Cab Device** – The component of Telematics, FMIS and/or ELD that is connected to vehicle networks. There may also be a Human Machine Interface (HMI) aspect to this component. In cases where the HMI is a separate device from that which connects to vehicular networks, then all the requirements identified as being applicable to the ‘Mobile App’ (see below) should be considered to apply to the HMI device.

- **Connectivity/Communications** – The component of a Telematics, FMIS and/or ELD which communicates data with the Cloud or Back-end (see below). This may or may not be the same device as the Physical In-Cab Device. In cases where they are the same device, both sets of the requirements identified as being applicable to a Physical In-Cab Device and the requirements identified as being applicable to Connectivity/Communications components should be considered to apply to the device.

- **Cloud or Back-end** – The component or components of a Telematics, FMIS and/or ELD which are internet facing, where data is collected, where commands or remote control of vehicular components are possible and where monitoring of the entire fleet or subsets thereof is made possible by dashboard or operations center features. In some cases, these components will be hosted by service providers, while in others they may be hosted by the owner. In either case, all the requirements identified as being applicable to Cloud or Back-end should be considered to apply to the device.

- **Mobile App** – The component of a Telematics, FMIS and/or ELD, which presents Human Machine Interfaces to drivers or other users of the system, has its own communications paths to the Cloud or Back-end and may or may not be hosted in a device separate from the Physical In-Cab Device, but is otherwise able to connect to and communicate with that vehicular component.

A goal of the working group was to ensure that stakeholders who procure equipment could also be capable of verifying that the equipment satisfies cybersecurity requirements. Therefore, each requirement includes a validation step which is intended to be executed by the purchaser. In some cases, the verification of the cybersecurity requirement requires more specialized knowledge than is reasonable to expect the purchaser to have. In these few cases, the validation steps recommend consulting a 3rd party report.

In recognizing that the implementing cybersecurity for systems is an ongoing process for which there are rarely enough resources, each requirement has been each assigned a ‘criticality.’ These criticalities can be used to prioritize implementation by vendors or selection of vendors by purchasers.
We have avoided any requirements that are novel or otherwise unique in favor of referencing publicly available authoritative sources. This report refers to multiple authoritative sources including:

- National Institute of Standards and Technology (NIST) 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- Cloud Security Alliance. Consensus Assessment Initiative Questionnaire (CAIQ)

Additional authoritative sources will be included in future versions of this report.
Cybersecurity Requirements for Telematics Systems Matrix Description

Each requirement captured is augmented with Criticality, Verification Steps, Public Requirements References, etc. A sample requirement is shown in Table 1 below:

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality: High, Medium, or Low</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA-010</td>
<td>Audit and Accountability</td>
<td>Medium</td>
<td>NIST 800-53 AU-2 – AUDIT EVENTS</td>
</tr>
</tbody>
</table>

The example requirement above demonstrates the form in which each requirement is presented in Appendix A.
Ref # – shows a unique value assigned to the requirement for easy reference

**Security Controls** – groups like requirements together

**Criticality** – assigns a ‘priority’: a recommendation to the purchaser for each requirement:

- **High**: the working group advises that purchasers do not accept proposals that do not meet all ‘High’ criticality requirements
- **Medium**: the working group advises that purchasers may accept proposals that do not meet ‘Medium’ criticality requirements when the failure is justifiable or mitigated by the vendor
- **Low**: the working group advises that purchasers may accept proposals that do not meet ‘Low’ criticality requirements

**Applicable Component Categories** – shows to which of the components of the Telematics, FMIS and/or ELD that this requirement applies.

**Public Requirements References / Descriptions** – shows as many external authoritative requirements as were known to the working group at the time of this draft. These references are included so that

- Purchasers can easily refer to the referenced sections of the document for further clarification on what are acceptable norms when evaluating vendor responses to RFPs AND
- Vendors can use the referenced sections of the documents for establishing common language and terms in the responses to RFPs to amortize the costs of developing detailed responses.

**Requirement** – shows the requirement as it applies to the components of a Telematics, FMIS and/or ELD. The working group made every effort to make these requirements shorter and more succinct than the authoritative external references.
**Verification** – shows the steps which can be executed by purchasers to confirm that a given Telematics, FMIS and/or ELD satisfies this requirement. There are several cases where the working group does not expect that purchasers will perform their own verification. Where it is recommended that either a third party be engaged to provide an analysis which can be used by the purchasers to verify vendor claims, or that the vendor perform a demonstration that the requirement is satisfied which can be observed and confirmed by the purchaser. In such cases, rationale will be given. Due to the costly nature of delegating to a third party or of preparing a demonstration, this will only be recommended in cases where the requirement has been listed as having high *Criticality*. Because of the high *Criticality* of these requirements, it would be ideal to verify them relying on both a third party and a demonstration; the recommendation of the working group is that one or the other is sufficient.

- In the context of verification via reports from a third party it is acceptable to either, as a purchaser, contract the third party for testing or to verify documentation provided by a third party contracted by the vendor.
- In the context of demonstration by the vendor, it is important that the purchaser ensure the demonstration covers the non-functional aspects of these requirements, (e.g. for secure boot it is not sufficient to demonstrate that valid images are bootable, but rather it is necessary to demonstrate that tampered images are not bootable.)

**Remarks** – shows comments or notes from the working group.

In the Appendix A to this report you will find a complete collection of requirements collected in the above format.
Recommendations and Conclusions

The working group has produced the comprehensive list of cybersecurity requirements for Telematics, FMIS and/or ELDs found in Appendix A. These requirements are prioritized via Criticality and assigned to one or more components in a generic Telematics, FMIS and/or ELD. They also include references to public, authoritative sources for more details on the requirement for the benefit of additional understanding on the part of the purchaser and vendor.

The working group recommends that federal agency fleet managers and private industry stakeholders use these requirements when procuring new Telematics, FMIS and/or ELDs, as well ELDs as well as when evaluating their current systems when the need to evaluate cybersecurity arises. It is NMFTA’s recommendation that motor freight carriers use these requirements as a natural successor to “Telematics Cybersecurity Primer for Agencies.” The requirements contained in this report complete several key areas which are missing in the Primer.

The working group continues to refine the requirements and the reader is encouraged to visit https://github.com/nmfta-repo/nmfta-telematics_security_requirements to obtain the most up-to-date copy of the requirements, which is also available in a supplier questionnaire format. The site should also be used to give feedback to the working group on ways that the requirements can be further refined.
References

Appendix A: Telematics Cybersecurity Requirements

In this section the reader will find all of the requirements of the v1.3 release of the Telematics Cybersecurity Requirements. The full release can be found here https://github.com/nmfta-repo/nmfta-telematics_security_requirements/releases/tag/v1.3
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA-010</td>
<td>Audit and Accountability</td>
<td>Medium</td>
<td>NIST 800-53 AU-2 – AUDIT EVENTS</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Cloud or Back-end;

**Requirement**

The vendor’s system shall record event and system logs

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documentation detailing locations where audit logs are stored and the types of events logged.

**Remarks**

Ideally the logs are immutable, backed up, and retained for a certain period of time

- The organization:
  a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];
  b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
  c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
  d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

  NIST 800-53 AU-2 (3) – AUDIT EVENTS | REVIEWS AND UPDATES

- The organization reviews and updates the audited events [Assignment: organization-defined frequency].

- CTIA ICCTP 4.7 Audit Log
### Public Requirements References/Descriptions

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
</table>
| AC-010 | Protecting Data on Devices | Medium | NIST 800-53 SI-16 - MEMORY PROTECTION  
The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution. |
|       |                   |              | NIST 800-53 AC-6 (4) - LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS  
The information system provides separate processing domains to enable finer-grained allocation of user privileges. |
|       |                   |              | NIST 800-53 SC-2 – APPLICATION PARTITIONING  
The information system separates user functionality (including user interface services) from information system management functionality. |
|       |                   |              | NIST 800-53 SC-2 (1) - APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS  
The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users. |
|       |                   |              | NIST 800-53 AC-25 – REFERENCE MONITOR  
The information system implements a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured. |

### Applicable Component Categories

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

### Verification: Inspection, Demonstration, Test, or Analysis

- Inspection of vendor-supplied design documentation detailing the privilege separation of the device.  
Ensure that 1) a Mandatory Access Control scheme is employed 2) there are separate domains/users/roles (whichever is applicable to the MAC) for dealing with the sensitive information (vendor defined, see SCP-030) and finally 3) accounts for running system tasks (e.g. crond, portmap, systemd) are not in the separate domains/users/roles for dealing with sensitive information.

### Remarks

- e.g. a Linux system with MAC configured to deny access to the processes dealing with protected data and also denying debugger access to the memory space of those processes.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-020</td>
<td>Protecting Actions on Devices</td>
<td>High</td>
<td>NIST 800-53 AC-6 – LEAST PRIVILEGE</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
All actions taken by the vendor’s telematics system that are capable of supporting access controls shall be configured such that each user account or process/service account are assigned only the minimal privileges required to perform the specific, intended, actions of the user or process/service account.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor documentation or a demonstration by the vendor that details how software privileges are assigned in vendor systems. Ensure that principles of least privilege are met.

**Remarks**
This principle underpins system security
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-030</td>
<td>Access Control</td>
<td>High</td>
<td>NIST 800-53 AC-6 – LEAST PRIVILEGE</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

The vendor’s system shall employ authentication to prevent unauthorized access to telematics systems and data.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor documentation detailing the methods used to authenticate users. Ensure that an acceptable method of authentication is available for all components which be interfaced-to by carrier staff and systems.

In the case of single-sign-on delegation, ensure that your (carrier) system requirements are met with respect to security assertions (e.g. SAML is supported).

**Remarks**

Identity management is critical

e.g. PINs, single-sign on with carrier’s identity provider (SAML or other), vendor managed identity provider (SAML or other)

NIST 800-53 AC-3 – ACCESS ENFORCEMENT

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

FMCSA GDL 32 Make sure local wireless interfaces like Bluetooth or Wi-Fi don’t provide admin access without authentication.
The vendor shall identify all instances where the telematics system includes actions that cannot support access authentication and/or execute with elevated privileges.

Verification: Inspection, Demonstration, Test, or Analysis

Inspection of vendor-supplied documentation listing system actions and interfaces that do not require authentication. Ensure that the list is short, that each entry in the list is acceptable to you (the carrier), and there is a justifiable reason for no-authentication on each item in the list.

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-040</td>
<td>Access Control</td>
<td>Medium</td>
<td>NIST 800-53 AC-14 – PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION</td>
</tr>
</tbody>
</table>

Applicable Component Categories

Mobile App; Physical In-Cab Device; Connectivity/Communications; Cloud or Back-end;

Requirement

The vendor shall identify all instances where the telematics system includes actions that cannot support access authentication and/or execute with elevated privileges.

Remarks

-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-041</td>
<td>Access Control</td>
<td>Medium</td>
<td>NIST 800-53 AC-14 – PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

Identifying information about the connected devices will not be made available without authentication first.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documentation listing system actions and interfaces that do not require authentication. Ensure that no information leaks are possible from these unauthenticated actions.

**Remarks**

e.g. it should not be possible to identify the device type nor firmware version by port scanning a connected device. Also, it should not be able to determine that a vehicle is operational or not via non-authorized connections.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-050</td>
<td>Access Control</td>
<td>Medium</td>
<td>NIST 800-53 AC-17 – REMOTE ACCESS</td>
</tr>
</tbody>
</table>

### Applicable Component Categories
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

### Requirement
All remote access methods and possible remote actions to/on telematics system shall be documented.

### Verification: Inspection, Demonstration, Test, or Analysis
Inspection of vendor-supplied documentation listing the methods of remote access and the actions that can be performed. Ensure that the remote access methods and actions are justifiable and also ensure that all remote methods require authentication (i.e. ensure none of them are listed in vendor documentation for AC-040)

### Remarks
-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-060</td>
<td>Access Control</td>
<td>Medium</td>
<td>NIST 800-53 AC-18 – WIRELESS ACCESS</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Physical In-Cab Device;
- Connectivity/Communications;

**The organization:**

- Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
- Authorizes wireless access to the information system prior to allowing such connections.

**Requirement**

For all components of the system, the vendor shall provide a listing of all wireless communication interfaces to the system and specify how the interfaces can be configured and/or disabled.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documentation detailing what wireless communications hardware is present, which wireless communications methods can be disabled, and how wireless communications enablement or disablement is managed.

**Remarks**

e.g. Bluetooth, cellular, satellite, Wi-Fi hotspot, Wi-Fi client, infrared, NFC, RFID
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-061</td>
<td>Access Control</td>
<td>Medium</td>
<td>(GDL 39) Only use WPA2 authentication / encryption. Never use WEP, WPS, or &quot;open&quot; Wi-Fi.</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Physical In-Cab Device;
- Connectivity/Communications;

**Requirement**
The vendor shall not use any deprecated encryption+authentication on any WiFi interface of the device. At the time of drafting this includes WEP, WPS or open/none.

**Verification: Inspection, Demonstration, Test, or Analysis**
Test that the device will not connect to WEP, WPS or open Wi-Fi hotspots.

**Remarks**
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
</table>

**Applicable Component Categories**
- Physical In-Cab Device;
- Connectivity/Communications;

**Requirement**
The vendor shall implement, for all bluetooth interfaces, pairing that must be specifically allowed by physical controls on the device and be time-limited. Furthermore, pairing will not use legacy pairing or passkey entry.

**Verification: Inspection, Demonstration, Test, or Analysis**
Test that it is not possible to pair with the device 5 minutes after enabling pairing on the device. Test that pairing does not support SSP or passkey, only numeric comparison.

**Remarks**
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-063</td>
<td>Access Control</td>
<td>Medium</td>
<td></td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Physical In-Cab Device;
- Connectivity/Communications;

**Requirement**
Any and all software or firmware implementing wireless interface encryption+authentication (those satisfying AC-061 and AC-062 above) will be prepared for future deprecation of methods. i.e. That software/firmware is upgradable.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation confirming upgradability of the software implementing encryption+authentication of wireless interfaces.

**Remarks**

Source: https://github.com/nmfta-repo/nmfta-telematics_security_requirements
NIST 800-53 AC-7 - UNSUCCESSFUL LOGON ATTEMPTS

The information system:

a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

CTIA ICCTP 5.2 Password Management Test

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-070</td>
<td>Identification and Authentication</td>
<td>Medium</td>
<td>NIST 800-53 AC-7 - UNSUCCESSFUL LOGON ATTEMPTS</td>
</tr>
</tbody>
</table>

Applicable Component Categories

Cloud or Back-end;

Verification: Inspection, Demonstration, Test, or Analysis

Inspection of vendor-supplied documentation detailing the methods used to enforce rate limiting.

Remarks

-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-080</td>
<td>Device-Local Authentication</td>
<td>Medium</td>
<td>ETSI TS 103 645 V1.1.1 Provision 4.1-1 All IoT device passwords shall be unique and shall not be resettable to any universal factory default value.</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;

**Requirement**
All authentication offered on device-local interfaces shall expect credentials which are unique to each device instance and uncorrelated to any and all public information about the device.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing the local authentication and how the unique credential is generated. Ensure that the generation of this credential cannot be guessed from public information.

**Remarks**
This requirement applies to many common facilities found on devices. e.g. local management portals, local Wi-Fi access points, Bluetooth pairing codes, local ssh servers, local serial console logins.

FMCSA GDL 32 Make sure local wireless interfaces like Bluetooth or Wi-Fi don't provide admin access without authentication.

FMCSA GDL 40 Always use a complex, unique password per device.

FMCSA GDL 43 Always use a complex, unique password per device.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-010</td>
<td>Protecting Actions on Devices</td>
<td>Medium</td>
<td>NIST 800-53 CM-7 – LEAST FUNCTIONALITY</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Physical In-Cab Device;
- Connectivity/Communications;

**Requirement**

All components of the vendor’s system shall be configured to utilize the principle of least functionality and use only the services necessary for secure operations of the system and remove unnecessary services’ executables or at least disabled such that their execution (by even superuser) is not possible in deployed systems.

**CTIA ICCTP 5.17 Design-In Features "deny all inbound and outbound network connections by default**

**FMCSA GDL 20 Give applications the least privilege they need to function**

**FMCSA GDL 21 Where possible, remove code that isn’t used**

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor documentation asserting that unnecessary software or services are not present or disabled on the device.

**Remarks**

E.g. this is particularly true of unauthenticated or unencrypted transport services (which would not satisfy protected communication requirements above) such as File Transfer Protocol, telnet, Short Messaging Service, etc.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-020</td>
<td>Configuration Management</td>
<td>High</td>
<td>NIST 800-53 CM-7 – LEAST FUNCTIONALITY</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
The vendor’s devices shall have all services used for troubleshooting disabled or properly protected from unauthorized access and use.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing all services (listening ports or outbound connections) available on deployed devices.

Ensure that none of the services available are without authentication (see AC-030) and furthermore that any troubleshooting functionality is ideally disabled, or at least the service available requires unique credentials for authorization of that feature.

**Remarks**
Deploying with test or debug facilities enabled is egregious.

**FMCSA GDL 54** Disable unnecessary debugging interfaces in production.

**FMCSA GDL 55** Authenticate debugging and diagnostic interfaces.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-030</td>
<td>Configuration Management</td>
<td>High</td>
<td>NIST 800-53 CM-7 – LEAST FUNCTIONALITY</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
Vendor ensures that any and all interfaces used for testing or debug are unavailable in production builds of the devices.

**Verification: Inspection, Demonstration, Test, or Analysis**
- Inspection of vendor-supplied documentation detailing all service (listening ports or outbound connections) available on deployed devices.
- Ensure that there are no services for test or debug active in the device. Ideally, look for assurances that any test or debug executables cannot be run on the device.

**Remarks**
Deploying with test or debug facilities enabled is egregious.

The organization:
- Configures the information system to provide only essential capabilities; and
- Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

CAIQ CCC-03.4 Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?
- FMCSA GDL 31 Make sure debugging interfaces (JTAG, serial, USB) have authentication required.
- FMCSA GDL 54 Disable unnecessary debugging interfaces in production.
- FMCSA GDL 55 Authenticate debugging and diagnostic interfaces.
### Public Requirements References/Descriptions

**NIST 800-53 IA-3 – DEVICE IDENTIFICATION AND AUTHENTICATION**

The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

### Applicable Component Categories

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

### Requirement

All remote hosts of the vendor’s system shall be configured to uniquely identify and authenticate all other remote hosts of the system and/or any other interfacing systems.

### Verification: Inspection, Demonstration, Test, or Analysis

Inspection of vendor-supplied documentation detailing how devices and components are uniquely identified.

Ensure that interfacing systems can query and/or inspect these unique identifiers.

### Remarks

- e.g. that a remote system authenticate the other remote parties by referring to the unique identifiers using mutually authenticated TLS
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA-020</td>
<td>Identification and Authentication</td>
<td>Medium</td>
<td>NIST 800-53 IA-3 – DEVICE IDENTIFICATION AND AUTHENTICATION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Physical In-Cab Device;
Connectivity/Communications;

**Requirement**

Any authenticators (unique identification) for devices used in vendor’s systems shall be uncorrelated to any and all public information about the device, e.g. lot number, product number, serial number MAC address are all unacceptable inputs to device identifiers.

Where public information is any information that is visible (externally or internally) on the device or discoverable by searches based on that visible information.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor documentation detailing the inputs to the authenticator generation process per device. Ensure that no input is information that can be easily-guessed from simple facts about the device.

**Remarks**

-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA-030</td>
<td>Identification and Authentication</td>
<td>Medium</td>
<td>NIST 800-53 IA-7 – CRYPTOGRAPHIC MODULE AUTHENTICATION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Mobile App;  
Physical In-Cab Device;  
Connectivity/Communications;  
Cloud or Back-end;

**Requirement**

Cryptographic modules used in the vendors system shall be compliant with Federal Information Processing Standards (FIPS) 140-2: Level 1.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documentation detailing their procurement requirements for cryptographic modules.

Ensure that their procurement processes require that all cryptographic modules are FIPS 140-2 compliant.

**Remarks**

e.g.  
• For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed, or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods)  
• For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed, or a false acceptance will occur  
• Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password).  
• Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-010</td>
<td>Incidence Response</td>
<td>High</td>
<td>NIST 800-53 IR-8 - INCIDENT RESPONSE PLAN</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

The vendor shall have a documented incident response plan (IRP) in place which provides the carriers with a point of contact for components used within their telematics system.

**Verification: Inspection, Demonstration, Test, or Analysis**

- Inspection of vendor-supplied documentation detailing the vendor’s incident response process.
- Ensure that it documents the methods that can be used to notify the vendor of a security incident.

**Remarks**

- TSPs must demonstrate this level of maturity to be trusted with business critical functions.
- FMCSA GDL 14 Employ an incident response process.

**NIST 800-53 IR-8 - INCIDENT RESPONSE PLAN**

The organization:

1. Develops an incident response plan that:
   - Provides the organization with a roadmap for implementing its incident response capability;
   - Describes the structure and organization of the incident response capability;
   - Provides a high-level approach for how the incident response capability fits into the overall organization;
   - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   - Defines reportable incidents;
   - Provides metrics for measuring the incident response capability within the organization;
   - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   - Is reviewed and approved by [Assignment: organization-defined personnel or roles];
2. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];
3. Reviews the incident response plan [Assignment: organization-defined frequency];
4. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
5. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and
6. Protects the incident response plan from unauthorized disclosure and modification.
The vendor shall have procedures in place to ensure that components outside of the carrier’s direct control are not updated or modified without prior coordination and approval by an organization-defined individual or role.

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
The vendor shall have procedures in place to ensure that components outside of the carrier’s direct control are not updated or modified without prior coordination and approval by an organization-defined individual or role.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing their maintenance/release process.

Ensure that there is a process where you (the carrier) are contacted and coordinated-with before the systems upon which you rely undergo maintenance procedures.

**Remarks**
- 

**Public Requirements References/Descriptions**
NIST 800-53 MA-2 – CONTROLLED MAINTENANCE

The organization:
- a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
- b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
- d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
- e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-020</td>
<td>Maintenance</td>
<td>High</td>
<td>NIST 800-53 CP-4 - CONTINGENCY PLAN TESTING</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Cloud or Back-end;

**Requirement**

The organization:

a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

b. Reviews the contingency plan test results; and

c. Initiates corrective actions, if needed.

NIST 800-53 CP-9 (1) - SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY

Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documentation detailing backup and restore procedures.

CAIQ BCR-11.5 Do you test your backup or redundancy mechanisms at least annually?

**Remarks**

TSPs must demonstrate this level of maturity to be trusted with business critical functions.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-030</td>
<td>Disposal of Goods</td>
<td>High</td>
<td>ISO 27001 A.8.3.2 Disposal of Media</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Cloud or Back-end; NIST 800-88 R1

**Requirement**

The vendor must have a disposal of goods policy which covers the management of all computer equipment and storage media dealing with customer information including but not limited to PII and customer business operations data.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documentation detailing their disposal of goods procedures; confirm the presence of specific mention of handling of their customer’s information.

**Remarks**
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-031</td>
<td>Disposal of Goods</td>
<td>Medium</td>
<td>ISO 27001 A.8.3.2 Disposal of Media</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Cloud or Back-end:
  - NIST 800-88 R1

**Requirement**
The vendor’s disposal of goods policy must forbid disposal in skips, dumps or landfills until it has been processed to purge or clear previously stored information.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing their disposal of goods procedures; confirm that disposal of systems in skips or landfills is not allowed unless the systems have been purged or cleared.

**Remarks**
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-032</td>
<td>Disposal of Goods</td>
<td>Low</td>
<td>NIST 800-88 R1 Appendix A -- Minimum Sanitization Recommendations</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Cloud or Back-end;

**Requirement**
The vendor's processes to remove previously stored information must include acceptable processes for magnetic media, solid-state media, printers, scanners, laptops, smartphones, server and desktop computers.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing their disposal of goods procedures; confirm that there are procedures that cover all of magnetic media, solid-state media, printers, scanners, laptops, smartphones, server and desktop computers.

**Remarks**
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-010</td>
<td>Planning</td>
<td>Medium</td>
<td>NIST 800-53 PL-2 - SECURITY AND PRIVACY PLANS</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Cloud or Back-end;

---

**Requirement**

The vendor shall have a System Security Plan (SSP) which details a clear and concise understanding of authorization boundaries of the telematics system.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied SSP document that details the authorization boundaries of telematics system.

Ensure that the document details which entity has responsibility for each component of the system, the system baseline and security posture within the boundaries.

**Remarks**

-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-020</td>
<td>Planning</td>
<td>Medium</td>
<td>NIST 800-53 PL-8 - SECURITY AND PRIVACY ARCHITECTURES</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Cloud or Back-end;

**Requirement**
The vendor shall have a documented Information Security Architecture (ISA) for the telematics system.

**Verification: Inspection, Demonstration, Test, or Analysis**
- Inspection of vendor-supplied ISA documentation.

Ensure that the ISA document at a minimum includes:
- Approach to confidentiality, integrity, and availability protections
- How the telematics system’s security architecture supports the enterprise architecture’s security
- Security assumptions and dependencies on external services
- Frequency of reviews and updates to the telematics system security architecture

**Remarks**
- 

The organization:
- a. Develops an information security architecture for the information system that:
  1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
  2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
  3. Describes any information security assumptions about, and dependencies on, external services;
- b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and
- c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-030</td>
<td>Planning</td>
<td>High</td>
<td>CAIQ BCR-01.2 Do you provide tenants with infrastructure service failover capability to other providers?</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
Cloud or Back-end;

**Requirement**
The vendor shall provide interfaces to their backend using the Open Telematics API -- enabling carriers to have failover to other providers to avoid interruptions due to single point of failure in provider telematics services.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing the interfaces (APIs) offered by the vendor.
Ensure that your (carrier) systems can failover to other providers with the same interfaces (APIs).

**Remarks**
Telematics is business critical to the carriers, failover is needed for this service.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS-010</td>
<td>Personnel Security</td>
<td>Medium</td>
<td><strong>NIST 800-53 PS-1 - PERSONNEL SECURITY POLICY AND PROCEDURES</strong></td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

The vendor shall have personnel security policies & procedures, position risk categorization, personnel screening, personnel termination, personnel transfer, access agreements and third-party personnel security.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documents detailing their personal security policies & procedures.

**Remarks**

- 

**NIST 800-53 PS-7 - EXTERNAL PERSONNEL SECURITY**

The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;

c. Documents personnel security requirements;

d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and

e. Monitors provider compliance.
## Public Requirements References/Descriptions

### NIST 800-53 RA-3 – RISK ASSESSMENT

The organization:

- a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
- b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];
- c. Reviews risk assessment results [Assignment: organization-defined frequency];
- d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
- e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

### FMCSA GDL 1 Conduct architectural analysis and/or threat modeling during system design

---

### Applicable Component Categories

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

### Requirement

Vendor shall have risk assessments conducted at an industry accepted rate. Resulting risk assessment documentation should include all components and the overall system that is within the vendor’s control. The rate suggested is twice per product release, both at product design and at integration phases.

### Verification: Inspection, Demonstration, Test, or Analysis

Inspection of vendor-supplied documentation stating their previous and planned risk assessment dates and detailing the documentation requirements of their risk assessments.

### Remarks

- 

---

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-010</td>
<td>Risk Assessment</td>
<td>Medium</td>
<td>NIST 800-53 RA-3 – RISK ASSESSMENT</td>
</tr>
</tbody>
</table>

The organization:

- a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
- b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];
- c. Reviews risk assessment results [Assignment: organization-defined frequency];
- d. Disseminates risk assessment results to [ Assignment: organization-defined personnel or roles]; and
- e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

FMCSA GDL 1 Conduct architectural analysis and/or threat modeling during system design
### Public Requirements References/Descriptions

**NIST 800-53 RA-3 – RISK ASSESSMENT**

The organization:

- a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

- b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];

- c. Reviews risk assessment results [Assignment: organization-defined frequency];

- d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and

- e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

**CAIQ GRM-08.1 Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?**

**FMCSA GDL 1 Conduct architectural analysis and/or threat modeling during system design**

### Applicable Component Categories

- Mobile App
- Physical In-Cab Device
- Connectivity/Communications
- Cloud or Back-end

### Requirement

The vendor shall use the results of risk assessments to influence systems development and processes.

### Verification: Inspection, Demonstration, Test, or Analysis

Inspection of vendor-supplied statement of the use of risk assessments in influencing the ongoing development of their products.

### Remarks

- "
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAA-010</td>
<td>Security Management</td>
<td>High</td>
<td>NIST 800-53 CA-2 - ASSESSMENTS</td>
</tr>
</tbody>
</table>

### Applicable Component Categories

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

### Requirement

The vendor shall have an Information Security Management Plan (ISMP).

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documentation detailing their ISMP/ISMS.

Note that an ISMP is broad and includes aspects which are covered by other requirements in this document. In cases where there is both a requirement here and in the ISMP, ensure that the requirement in this document is satisfied over what is stated in an ISMP.

**Remarks**
Sometimes referred to as ISMS as in ISO/IEC 27001.

May include any of the following:
- System interconnections, System monitoring plan,
- Vulnerability management plan, Incident response plan (see IR-010 for authoritative requirement),
- System Security Plan (SSP) or System Security Authorization Agreement (SSAA), Contingency Plan,
- Contingency Plan Test Results, Federal Information Processing Standards (FIPS) 199 Categorization,
- Privacy Threshold Analysis (PTA), E-Authentication, Security Test and Evaluation (ST&E) Plan, Plan of Action and Milestones (POAM), Annual Self-Assessments

a. Develops, documents, and disseminates to (assignment: organization-defined personnel or roles):
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Reviews and updates the current:
   1. Contingency planning policy (assignment: organization-defined frequency); and
   2. Contingency planning procedures (assignment: organization-defined frequency).

CAIQ GRM-04.1 Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

CAIQ GRM-04.2 Do you review your Information Security Management Program (ISMP) at least once a year?

ISO/IEC 27001 ISMS
### Public Requirements References/Descriptions

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAA-020</td>
<td>Security Assessment and Authorization</td>
<td>High</td>
<td>NIST 800-115 Technical Guide to Information Security Testing and Assessment – All sections</td>
</tr>
</tbody>
</table>

### Applicable Component Categories

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

### Requirement

The vendor shall have penetration testing performed, to an industry accepted best practice, at an industry accepted pace.

Penetration testing can be performed by teams internal to the TSP; industry best practice is to have external pentesting performed periodically also.

### Verification: Inspection, Demonstration, Test, or Analysis

Inspection of 3rd party documentation or a demonstration by the vendor that asserts the dates of penetration tests.

Note that due to the sensitive nature of these reports, you (carriers) should be prepared to enter into NDAs to review these documents.

### Remarks

Periodic pentesting keeps everyone honest

### NIST 800-53 CA-8 – PENETRATION TESTING

The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].

### CAlQ AIS-01.5 Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?

### CAlQ AAC-02.2 Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?

### CAlQ AAC-02.3 Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?

### FMCSA GDL 3 Perform adversarial testing before a product is finalized
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAA-030</td>
<td>System and Service Acquisition</td>
<td>Medium</td>
<td>NIST 800-53 SA-11 – DEVELOPER TESTING AND EVALUATION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
Vendor shall have Security Testing and Evaluation (ST&E) of the system and/or components that includes all results of the security testing and evaluation, including discovered vulnerabilities and a plan/process to mitigate discovered vulnerabilities or weaknesses in the system.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing their product release and quality controls.

Ensure that the product release process includes ST&E steps and that these feed-back into product development.

**Remarks**
- 

The organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;

b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];

c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during security testing/evaluation.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
</table>
| SAA-040 | System and Service Acquisition           | Low          | NIST 800-53 SA-12 (2) - SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS | The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.  
FMCSA GDL 6 Perform your own security due diligence, which involves but is not limited to ensuring that third-party devices in the supply chain meet your basic security requirements. |

**Applicable Component Categories**
Mobile App;  
Physical In-Cab Device;  
Connectivity/Communications;  
Cloud or Back-end;  

**Requirement**
The vendor shall perform due diligence to ensure its suppliers also meet the vendor’s security requirements.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor documentation detailing supplier review and acceptance processes and criteria.

**Remarks**
-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-010</td>
<td>Protecting Communications paths for</td>
<td>High</td>
<td>NIST 800-53 SC-8 (1) - TRANSMISSION CONFIDENTIALITY AND INTEGRITY</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

Communication paths that traverse outside controlled boundaries must protect confidentiality and integrity of data

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of a 3rd party implementation review report or a demonstration by the vendor that asserts the use of cryptographic protections for the confidentiality and integrity of all external communications channels. The cryptographic protections must be industry standard.

(rationale: cryptography must be validated by experts in the subject)

**Remarks**

Underpins device functionality and security
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-011</td>
<td>Protecting Communication paths for</td>
<td>Medium</td>
<td>NIST Special Publication 800-133 - Recommendation for Cryptographic Key Generation</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
Communication path cryptographic protections must not use identities, keys or shared secrets which are common across multiple deployed devices.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor design documentation detailing the creation use and distribution of identities, keys and shared secrets. Ensure that these are segmented in deployed systems such that a compromise of one piece of information in turn compromises a limited number of deployed devices.

**Remarks**
-
**Applicable Component Categories**

Mobile App;
Physical In-Cab Device;
Connectivity/Communications;
Cloud or Back-end;

**Requirement**

Measures will be taken by vendors to protect the confidentiality of any information at rest on the devices that could be interpreted as Sensitive and/or Personally Identifiable Information. This sensitive information is defined in SCP-030 where ‘at rest’ is understood to mean any state where the data is in a non-volatile storage medium, e.g. eMMC not RAM.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of a 3rd party implementation review report or a demonstration by the vendor that asserts the use of cryptographic confidentiality protections on storage of sensitive data (class defined by vendor, see SCP-030). The protections must be industry standard and keys must be managed to protect them from leaks as well. (rationale: cryptography must be validated by experts in the subject)

**Remarks**

Failing to adequately protect PII can incur large fines

E.g. this applies also to apps on mobile where data is cached until it can be synced to other vehicle-connected devices. This data must be encrypted as per this requirement.

NB: ideally these systems should be designed to minimize the collection of PII.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-030</td>
<td>Protecting Data on Devices</td>
<td>Medium</td>
<td></td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Mobile App; Physical In-Cab Device; Connectivity/Communications; Cloud or Back-end;

**Requirement**

Vendors will supply documentation detailing what data is and is not protected at rest by cryptography.

Vendors are encouraged to expand the list of categories of data which will be protected on-device.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documentation describing what data is protected at rest by cryptography. Ensure that the types of data that put your business at risk are protected.

**Remarks**

-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-040</td>
<td>Protecting Data on Devices</td>
<td>Medium</td>
<td>NIST 800-53 SC-12 - CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST 800-53 SC-12 (1) - CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The organization maintains availability of information in the event of the loss of cryptographic keys by users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST 800-53 SC-12 (2) - CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST 800-53 SC-12 (3) - CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key].</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST Special Publication 800-133 - Recommendation for Cryptographic Key Generation</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
Data of the categories above will be protected using cryptographic keys which are not correlated to any public information about the devices.

Public information is any information that is visible (externally or internally) on the device or discoverable by searches based on that visible information.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor documentation detailing the inputs to the cryptographic key generation process per device. Ensure that no input is information that can be easily-guessed from simple facts about the device.

**Remarks**
-
### Applicable Component Categories

Cloud or Back-end

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
</table>
| SCP-050 | Protecting Data in the Backend | High | NIST 800-53 SC-4 - INFORMATION IN SHARED SYSTEM RESOURCES  
The information system prevents unauthorized and unintended information transfer via shared system resources.  
NIST 800-53 SC-4 (2) - INFORMATION IN SHARED SYSTEM RESOURCES | MULTILEVEL OR PERIODS PROCESSING  
The information system prevents unauthorized information transfer via shared resources in accordance with [Assignment: organization-defined procedures] when system processing explicitly switches between different information classification levels or security categories.  
CAIQ AAC-03.1 Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant’s data? |

### Requirement

All customer-related data will be logically segmented (e.g. encrypted with segmented keys) such that it is possible to produce all data related to one customer without inadvertently exposing any data of any others.

### Verification: Inspection, Demonstration, Test, or Analysis

Inspection of vendor-supplied design documentation or a demonstration by the vendor that details backend data storage and access. Ensure that either design aspects such as storage instances are per-customer or the cryptographic confidentiality protections are used to ensure one customer instance cannot read data from another. NB: Some or multiple may apply.

### Remarks

Otherwise could cause PII breaches and incur strong penalties
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-060</td>
<td>Protecting Vehicle Network Escalation</td>
<td>High</td>
<td>NIST 800-53 SI-10 – INPUT INFORMATION VALIDATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The information system checks the validity of [Assignment: organization-defined information inputs].</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST 800-53 SC-7 (21) - (21) BOUNDARY PROTECTION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined missions and/or business functions].</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FMCSA GDL 27 Limit telematics units’ access to the CAN bus, and whitelist the CAN messages they can send</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FMCSA GDL 37 It is recommended to isolate safety-critical ECUs on their own CAN bus, with some sort of gateway between them and other ECUs</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Physical In-Cab Device;
- Connectivity/Communications;

**Requirement**

The vendor shall enforce controls integrated into the telematics device to limit the possible commands and data transmitted to the vehicle network.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of 3rd party implementation review or a demonstration by the vendor that asserts that there are protections in place which limit what data can be sent from the telematics device to the vehicle network. Ensure that the protections are ‘layered’ (follow defense-in-depth) so that the compromise of software leading to sending vehicle network data cannot also bypass the protections.

**Remarks**

Vehicle network protection is paramount
### Public Requirements References/Descriptions

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>NIST 800-53 SC-23 – SESSION AUTHENTICITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-090</td>
<td>System and Communication Protocols</td>
<td>High</td>
<td><em>The information system protects the authenticity of communications sessions.</em></td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

The vendor’s system shall implement protection of communications sessions against attacks including session hijacking and traffic manipulation. Where a session is understood to mean a time-limited authenticated login with the cloud/back-end.

- Sessions shall be invalidated at logout.
- Sessions must be randomized and uniquely identified.
- Protections must be implemented to restrict certificate authorities to a short (maximum 3) list of those expected by the vendor, i.e. secure communications must implement certificate pinning to a short whitelist of certificate authorities.

Certificate pinning shall be implemented on all telematics device to server communications (e.g. telematics gateways or IVGs). Administrative ‘backend’ systems may be exempt from this requirement to allow for stream inspection by enterprise intrusion detection systems.

**Verification: Inspection, Demonstration, Test, or Analysis**

- Inspection of vendor-supplied documentation detailing the session management mechanism employed in vendor systems.
- Ensure that certificate pinning is in use in communication path between telematics device and vendor’s infrastructure.
- Ensure compliance with NIST 800-53 control SC-23.

**Remarks**

Confidentiality and integrity of communication underpins the security of the system

Certificate pinning in clients – when combined with the other requirement for e.g. fail-over – could result in extra complications and so functional testing of fail over should be performed.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-091</td>
<td>System and Communication Protocols</td>
<td>Medium</td>
<td>[GDL 51] Check whether keys have expired or been revoked.</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Mobile App; Connectivity/Communications; Cloud or Back-end;

**Requirement**

The vendor shall implement checks for expired certificates and ensure the ability to remove trust in any given root certificate authority from their systems and devices PKI implementations.

**Verification: Inspection, Demonstration, Test, or Analysis**

Test that root certificate trust can be removed. This should result in failure to establish communications or a failure to validate updates, depending on which system is being tested.

**Remarks**
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-100</td>
<td>System and Communication Protocols</td>
<td>Medium</td>
<td>NIST 800-53 SC-39 - PROCESS ISOLATION The information system maintains a separate execution domain for each executing process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST 800-53 SC-39 (2) - PROCESS ISOLATION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Physical In-Cab Device;

**Requirement**
The vendor's system shall separate execution domains and/or processes (i.e. process isolation within both the telematics device and back-end system and between the serial communications in the telematics device and the interface to the vehicle network)

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing the software architecture.

**Remarks**

-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-110</td>
<td>System and Communication Protocols</td>
<td>High</td>
<td>CAIQ IPY-02.1 Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

Cloud or Back-end;

**Requirement**

The vendor’s system shall provide a means to download unstructured customer data in an industry-standard format (Open Telematics API). This download will occur over secured communication protocols.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor-supplied documentation detailing the interfaces (APIs) offered by the vendor.

Ensure that there is an interface (API) such that you (carrier) can download all data in an unstructured format.

**Remarks**

Telematics is business critical and failover is required

e.g. csv, txt, json formats
### Public Requirements References/Descriptions

**Security Controls**

**SCP-120**

<table>
<thead>
<tr>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique API Keys and API Passwords</td>
<td>Medium</td>
<td>OWASP ASVS Service Authentication Requirements 2.10.4</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

The vendor’s software shall not contain any credentials that are shared among other copies of software; e.g. the software cannot contain hardcoded API keys or API passwords.

**Verification: Inspection, Demonstration, Test, or Analysis**

- FMCSA GDL 40 Always use a complex, unique password per device
- FMCSA GDL 43 Always use a complex, unique password per device
- FMCSA GDL 48 Use a unique, complex password on each device, vehicle, or application

**Remarks**

- Inspection of 3rd party documentation or a demonstration by the vendor that asserts the absence of any hard-coded API keys in the client software. E.g. proof that any and all information from the backend is inaccessible without both valid user credentials and any client identifiers such as API keys.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP-130</td>
<td>System and Communication Protocols</td>
<td>Medium</td>
<td>FMCSA GDL 23 Follow best practices for securing cellular or satellite interfaces.</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

Vendors shall limit hardware support for deprecated or insecure communications protocols. This includes those with known vulnerabilities.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor documentation confirming secured configuration of any wireless and or satellite interfaces. Confirm especially that there are no downgrades of communications protocols possible.

**Remarks**
The vendor shall have a process for remediating flaws in deployed telematics devices and backend systems. In the case of telematics devices, firmware update capabilities are important to be able to remediate all flaws that could be located in the device.

Verification: Inspection, Demonstration, Test, or Analysis

Inspection of vendor-supplied documentation detailing their flaw remediation process for backend systems.

Requirements

c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process.

NIST 800-53 SI-2 (5) - FLAW REMEDIATION | AUTOMATIC SOFTWARE AND FIRMWARE UPDATES

The organization installs [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined information system components].

Remarks

This is a leniently-worded requirement that a process to update device firmware exists.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-011</td>
<td>Protecting Firmware on Devices</td>
<td>Medium</td>
<td>FASTR Connectivity and Cloud Work Group, 2018, SOTA recommendations</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App
- Physical In-Cab Device
- Connectivity/Communications
- Cloud or Back-end

**Requirement**
The vendor shall implement/deploy secure over the air update systems including assurances of integrity & authenticity. Also rollback protections and a means of denying the use of old potentially compromised signing keys.

**Verification: Inspection, Demonstration, Test, or Analysis**
Test that a) a modified update is rejected b) a modified update signed by any key other than the manufacturer is rejected c) a previous version cannot be reinstalled.

If this facility is not in motor freight carrier control; then inspection of a report from the vendor showing tests of the above.

**Remarks**
The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process.

The organization installs [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined information system components].

CAIQ TVM-02.5 Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?

CTIA ICCTP 3.5 Patch Management

CTIA ICCTP 5.5 Patch Management

FMCSA GDL 8 Decide early who is in charge of creating, implementing and maintaining software/firmware updates for a device when a vulnerability emerges and ensure these guidelines are met.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-021</td>
<td>Protecting Firmware on Devices</td>
<td>Medium</td>
<td>NIST 800-53 SI-2 - FLAW REMEDIATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The organization:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a. Identifies, reports, and corrects information system flaws;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>b. [...]</td>
</tr>
<tr>
<td>Applicable Component Categories</td>
<td></td>
<td></td>
<td>NIST 800-53 SI-2 (5) - FLAW REMEDIATION</td>
</tr>
<tr>
<td></td>
<td>Mobile App;</td>
<td></td>
<td>The organization installs [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined information system components].</td>
</tr>
<tr>
<td></td>
<td>Physical In-Cab Device;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connectivity/Communications;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cloud or Back-end;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement</td>
<td>Identified vulnerabilities are remediated or mitigated using suitable compensating controls on a timeline predicated by the severity of the vulnerability identified. Taking no longer than the following elapsed times: high in 30d, moderate in 90d and low in 180d.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification: Inspection, Demonstration, Test, or Analysis</td>
<td>Vendors shall provide a document that defines vulnerabilities severities (e.g. CVSS). Negotiation of mutually aggregable exceptions to the remediation timelines is acceptable to compensate for cases where the complexity of remediation or mitigations of the vulnerability is prohibitively expensive to execute in the prescribed timeline. In general, the timelines of remediation can be agreed -to in a SLA.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remarks</td>
<td>Inspection of vendor supplied documentation detailing the methods used to update software components across vendor’s infrastructure. Ensure that it is possible to remediate a vulnerability with an identified high severity (30d).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAIQ TVM-02.5 Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTIA ICCP 3.5 Patch Management</td>
<td>FedRAMP CSP CMSG B Row 10 – Vulnerability Scanning CSPs must mitigate all discovered high-risk vulnerabilities within 30 days, mitigate moderate vulnerability risks in 90 days, and mitigate low vulnerability risks in 180 days. CSPs must send their Reviewer updated artifacts every 30 days to show evidence that outstanding high-risk vulnerabilities have been mitigated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMCSA GDL 8 Decide early who is in charge of creating, implementing and maintaining software/firmware updates for a device when a vulnerability emerges and ensure these guidelines are met.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref #</td>
<td>Security Controls</td>
<td>Criticality:</td>
<td>Public Requirements References/Descriptions</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------</td>
<td>--------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>SII-030</td>
<td>Protecting Firmware on Devices</td>
<td>Medium</td>
<td>NIST 800-53 SI-3 - MALICIOUS CODE PROTECTION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor documentation demonstrating that only cryptographically signed software is allowed to be executed/run on telematics devices. Ensure that signature verification is performed before load/execute/run and not solely at time of installation.

**Requirement**
The vendor shall use digitally signed software on telematics devices and prohibit execution of unsigned or invalidly signed software.

**Remarks**
Note may just want to make this one vendor shall utilize digitally signed firmware

**The organization:**

- a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
- b. […]

- NIST 800-53 SI-7 (1) - SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS […]
- NIST 800-53 SI-7 (6) - SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION […]
- NIST 800-53 SI-7 (15) - SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION […]

- CAIQ CCC-04.1 Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?
- CTIA ICCTP 3.6 Software Upgrades CTIA ICCTP 5.6 Software Upgrades
- FMCSA GDL 30 If the device can be updated from local media (USB, SD cards, etc.), make sure the updates are digitally-signed and authorization is required
**Public Requirements References/Descriptions**

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
</table>
| SI-040 | Protecting Firmware on Devices | High | NIST 800-53 SI-7 (5) - SOFTWARE, Firmware, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS  
The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered.  
NIST 800-53 SI-7 (6) - SOFTWARE, Firmware, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION  
The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.  
NIST 800-53 SI-7 (9) - SOFTWARE, Firmware, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS  
The information system verifies the integrity of the boot process of [Assignment: organization-defined devices].  
NIST 800-53 SI-7 (10) - SOFTWARE, Firmware, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE  
The information system implements [Assignment: organization-defined security safeguards] to protect the integrity of boot firmware in [Assignment: organization-defined devices].  
NIST 800-53 SI-7 (15) - SOFTWARE, Firmware, AND INFORMATION INTEGRITY | CODE AUTHENTICATION  
The information system implements cryptographic mechanisms to authenticate [Assignment: organization-defined software or firmware components] prior to installation. |

**Applicable Component Categories**

| Physical In-Cab Device;  
Connectivity/Communications; |

**Requirement**

The vendor shall utilize a boot verification process built with (asymmetric) cryptographic digital signatures and implemented such that the public key used for verification or the hash of the public key used for verification is protected from being tampered on the device.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of a 3rd party implementation review report or a demonstration by the vendor that asserts the use of cryptographic protections for the integrity of the boot process. The cryptographic protections must employ asymmetric industry standard algorithms. (rationale: cryptography must be validated by experts in the subject)

**Remarks**

Secure boot underpins the access control which protects the vehicle networks.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-060</td>
<td>Protecting Firmware on Devices</td>
<td>Low</td>
<td>NIST 800-53 SI-7 (12) - SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The organization requires that the integrity of [Assignment: organization-defined user-installed software] be verified prior to execution.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST 800-53 SI-7 (15) - SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The information system implements cryptographic mechanisms to authenticate [Assignment: organization-defined software or firmware components] prior to installation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST 800-53 SC-3 - SECURITY FUNCTION ISOLATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The information system isolates security functions from nonsecurity functions.</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Physical In-Cab Device;
- Connectivity/Communications;

**Requirement**
The vendor shall provide a means (and document the process) for customers to verify the firmware in their devices.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor documentation detailing the process of verifying the firmware on a device. Ensure that these steps can be executed by your (carrier) staff to gain your own assurance of device firmware state.

**Remarks**
Is a rare feature to find deployed and is nice-to-have over and above secure boot
The vendor shall utilize an array of code safety features across the entire collection of executables in its devices: ASLR, DEP, CFI, Stack Guards, Fortification, and RELRO. Unless that code safety feature is not applicable on the system architecture, in which case it should be noted.

### Verification: Inspection, Demonstration, Test, or Analysis

Inspection of a 3rd party implementation review report or a demonstration by the vendor that asserts the presence of an array of code safety features (such as those listed in the requirement SII-070 or at the CITL safety features list).

(rationale: measuring the presence of these mitigations requires binary analysis by experts in the subject)

### Remarks

Without any of these, exploitation is trivial
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-071</td>
<td>Protecting Firmware on Devices</td>
<td>Medium</td>
<td>(GDL 26) Filter input to any device or interface that gets digitally processed.</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

The vendor shall use the techniques of sanitizing/filtering inputs, segmenting memory spaces of input parsers from other execution and/or using provably correct or memory safe languages for input processing.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of vendor documentation detailing the filtering performed on inputs to the software.

**Remarks**
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
</table>
| SI-080| Protecting Firmware on Devices        | Medium       | NIST 800-53 SI-17 - FAIL-SAFE PROCEDURES  
The information system implements [Assignment: organization-defined fail-safe procedures] when [Assignment: organization-defined failure conditions occur].  
NIST 800-53 SC-24 – FAIL IN KNOWN STATE  
CTIA ICCTP 5.17 Design-In Features “Fail Secure”  
FMCSA GDL 4 Security problems will happen; fail safely |

### Applicable Component Categories
- Mobile App;  
- Physical In-Cab Device;  
- Connectivity/Communications;  
- Cloud or Back-end;  

### Requirement
The vendor shall design security components that fail-secure to protect integrity of systems and data.

### Verification: Inspection, Demonstration, Test, or Analysis
Inspection of vendor documentation detailing how software components and the systems are designed to fail-secure.

### Remarks
-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-081</td>
<td>Protecting Firmware on Devices</td>
<td>Low</td>
<td>NIST 800-53 SI-3 - MALICIOUS CODE PROTECTION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
The vendor shall utilize protective mechanisms to protect components from unauthorized runtime/volatile modification of code.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor documentation detailing the operation of software protections for prevent the runtime modification of code.

**Remarks**
Not well defined enough to make this of critical importance to TSPs or carriers
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-090</td>
<td>Vulnerability Management</td>
<td>Medium</td>
<td>NIST 800-53 SI-5 - SECURITY ALERTS, ADVISORIES, AND DIRECTIVES</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

| Mobile App; Physical In-Cab Device; Connectivity/Communications; Cloud or Back-end; |

**Requirement**

The vendor shall maintain a responsible disclosure program that allows for vulnerabilities discovered in the system (device, mobile app or backend) by researchers, and other external entities to be reported, tracked and mitigated.

Vulnerability programs should include sufficient legal provisions to provide for a “Legal Safe Harbor” for researchers.

**Verification: Inspection, Demonstration, Test, or Analysis**

Demonstration, by vendor, that disclosure instructions are published on their public website and are readily accessible.

Demonstration, by vendor, of an active security@[vendor domain] email, that will provide a known contact point for disclosure.

**Remarks**

FMCSA GDL 8 Decide early who is in charge of creating, implementing, and maintaining software/firmware updates for a device when a vulnerability emerges, and ensure these guidelines are met.

FMCSA GDL 10 Publish a vulnerability reporting and disclosure policy.
### Public Requirements References/Descriptions

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>NIST 800-53 SI-4 – SYSTEM MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-100</td>
<td>Incident Response</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

#### Applicable Component Categories
- Cloud or Back-end;

#### Requirement
The organization:
- a. Monitors the information system to detect: [...]
  - FMCSA GDL 28 Enable security monitoring of the telematics system(s) using native tools.

#### Verification: Inspection, Demonstration, Test, or Analysis
Inspection of vendor-supplied documentation which asserts the use and active monitoring of their systems for intrusion.

#### Remarks
Regardless of how secure a system might be it will eventually be breached; therefore monitoring is of high criticality
- e.g. SIEM, IDS, WAF, Application monitoring
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-110</td>
<td>Vulnerability Management</td>
<td>Medium</td>
<td>NIST 800-53 RA-5 – VULNERABILITY SCANNING</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
The organization:

- a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

- b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
  1. Enumerating platforms, software flaws, and improper configurations;
  2. Formatting checklists and test procedures; and
  3. Measuring vulnerability impact;

- c. Analyzes vulnerability scan reports and results from security control assessments;

- d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and

- e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documents stating the frequency, method, and scope of vulnerability scans.

d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and

- e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-120</td>
<td>Vulnerability Management</td>
<td>Low</td>
<td>NIST 800-53 SI-2 - FLAW REMEDIATION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App
- Physical In-Cab Device
- Connectivity/Communications
- Cloud or Back-end

**Requirement**
The vendor shall have a vulnerability management process that includes steps to triage any found vulnerabilities and plan remediation.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation describing their triage process.

**Remarks**
This requirement, if satisfied, shows process maturity but is nice-to-have over and above the previous requirements in this category.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-130</td>
<td>Vulnerability Management</td>
<td>Medium</td>
<td>NIST 800-53 SA-11 (1) - DEVELOPER TESTING AND EVALUATION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
The vendor shall verify code and best practice standards prior to deployment including:

- Static Code Analysis / Static Application Security Testing (SCA/SAST)
- Dependency Scanning for known vulnerabilities in third party components

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing their release process and quality controls.

Ensure that the process ensures that code is subject to static analysis prior to production release.

**Remarks**
-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-140</td>
<td>Vulnerability Management</td>
<td>Medium</td>
<td>NIST 800-53 SI-3 – MALICIOUS CODE PROTECTION</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**

- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

**Verification: Inspection, Demonstration, Test, or Analysis**

- Inspection of vendor-supplied documentation detailing the methods used to protect systems and devices from malicious code.

**Remarks**

- e.g. whitelisting, anti-malware scanning, cryptographic protections

**FMCSA GDL 28 Enable security monitoring of the telematics system(s) using native tools**
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-150</td>
<td>Vulnerability Management</td>
<td>Medium</td>
<td>NIST 800-53 SA-15 (7) - DEVELOPMENT PROCESS, STANDARDS, AND TOOLS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The organization requires the developer of the information system, system component, or information system service to: (a) Perform an automated vulnerability analysis using [Assignment: organization-defined tools]; (b) Determine the exploitation potential for discovered vulnerabilities; (c) Determine potential risk mitigations for delivered vulnerabilities; and (d) Deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles].</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
The vendor shall verify code according to best-practice coding standards

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor-supplied documentation detailing the software development processes of the vendor.

Ensure that the vendor has coding standards that encourage secure code development.

**Remarks**
-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-170</td>
<td>System and Information Integrity</td>
<td>Medium</td>
<td>NIST 800-53 SI-5 - SECURITY ALERTS, ADVISORIES, AND DIRECTIVES</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
The vendor shall actively monitor resources such as NIST Common Vulnerabilities and Exposures (CVE), Bugtraq, for security alerts and advisories related to the telematics system's components.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor process documentation detailing whether alerts, advisories, and directives are monitored and how these items are consumed e.g. email, ticketing system.

**Remarks**
- 

FMCSA GDL 8 Decide early who is in charge of creating, implementing, and maintaining software/firmware updates for a device when a vulnerability emerges, and ensure these guidelines are met.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-171</td>
<td>System and Information Integrity</td>
<td>Medium</td>
<td>NIST 800-53 SI-5 - SECURITY ALERTS, ADVISORIES, AND DIRECTIVES</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
The vendor shall notify their customers of any vulnerabilities discovered in the telematics systems components via monitoring or vulnerability disclosure programs. The notification to customers will happen in a timely manner.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor process documentation detailing how customers are notified. Confirm that the timelines stated in the vendors notification procedures are acceptable.

**Remarks**
-
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-180</td>
<td>Secure Software Development Lifecycle</td>
<td>Medium</td>
<td>NIST 800-53 SA-3 - SYSTEM DEVELOPMENT LIFE CYCLE</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
- Remediation SLA or objectives are defined and are adhered to by the security and development teams.
- Identified vulnerabilities are remediated or mitigated using suitable compensating controls

**Verification: Inspection, Demonstration, Test, or Analysis**
- Inspection of vendor documentation detailing:
  - System Development Lifecycle
  - Remediation process
  - Security, Risk, and Privacy controls along with sample reports

**Remarks**
- BHIMM [SM1.4: 101] IDENTIFY GATE LOCATIONS, GATHER NECESSARY ARTIFACTS
  - a. Establish security-specific release gates necessary for go/no-go decisions prior to deployment.
- BHIMM [SM2.2: 42] ENFORCE GATES WITH MEASUREMENTS AND TRACK EXCEPTIONS
  - a. Deployment package must meet measured acceptance criteria for remediation or obtain a waiver.
- BHIMM [SM2.6: 39] REQUIRE SECURITY SIGN-OFF
  - a. Risk acceptor signs off on release package.
- BHIMM [CP1.3: 66] CREATE POLICY
  - a. Create a security policy that satisfies internal, regulatory, and customer-driven security requirements.
- SAMM [COMPLIANCE MANAGEMENT MATURITY 3]
  - a. Develop a program for measuring and reporting on the status of compliance between different applications
  - b. Compliance should be periodically assessed by the QA, Internal Audit, or Information Security teams through a combination of manual testing and interview
  - c. Compliance remediation activities should be periodically reviewed to ensure teams are making appropriate progress, as well as assuring remediation strategies will be effective in achieving compliance.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
</table>

**Applicable Component Categories**

Mobile App;

**Requirement**

The vendor’s software will have software resiliency measures included that will slow the progress of tampering and reverse engineering efforts.

**Verification: Inspection, Demonstration, Test, or Analysis**

Inspection of 3rd party documentation or a demonstration by the vendor that asserts the presence of anti-reverse-engineering in the vendor software. Ideally executed following the testing steps detailed in the OWASP MSTG ‘Android Anti-Reversing Defenses’ or ‘iOS Anti-Reversing Defenses’ sections

- OWASP MASVS MSTG-RESILIENCE-1
  a. The app detects, and responds to, the presence of a rooted or jailbroken device either by alerting the user or terminating the app.

- OWASP MASVS MSTG-RESILIENCE-2
  a. The app prevents debugging and/or detects, and responds to, a debugger being attached. All available debugging protocols must be covered.

- OWASP MASVS MSTG-RESILIENCE-3
  a. The app detects, and responds to, tampering with executable files and critical data within its own sandbox.

- OWASP MASVS MSTG-RESILIENCE-4
  a. The app detects, and responds to, the presence of widely used reverse engineering tools and frameworks on the device.

- OWASP MASVS MSTG-RESILIENCE-5
  a. The app detects, and responds to, being run in an emulator.

- OWASP MASVS MSTG-RESILIENCE-6
  a. The app detects, and responds to, tampering the code and data in its own memory space.

- OWASP MASVS MSTG-RESILIENCE-7
  a. The app implements multiple mechanisms in each defense category (8.1 to 8.6). Note that resiliency scales with the amount, diversity of the originality of the mechanisms used.

- OWASP MASVS MSTG-RESILIENCE-8
  a. The detection mechanisms trigger responses of different types, including delayed and stealthy responses.

- OWASP MASVS MSTG-RESILIENCE-9
  a. Obfuscation is applied to programmatic defenses, which in turn impede de-obfuscation via dynamic analysis.

- OWASP MASVS MSTG-RESILIENCE-10
  a. The app implements a ‘device binding’ functionality using a device fingerprint derived from multiple properties unique to the device.

**Remarks**
This is a nice-to-have. Mature solutions that process sensitive information in devices that could be in the hands of attackers are expected to have these protections; however, allowances should be made for products to focus on the necessary security controls first, for which these resiliency requirements are not a substitute.

**OWASP MASVS MSTG-RESILIENCE-11**

a. All executable files and libraries belonging to the app are either encrypted on the file level and/or important code and data segments inside the executables are encrypted or packed. Trivial static analysis does not reveal important code or data.

**OWASP MASVS MSTG-RESILIENCE-12**

a. If the goal of obfuscation is to protect sensitive computations, an obfuscation scheme is used that is both appropriate for the particular task and robust against manual and automated de-obfuscation methods, considering currently published research. The effectiveness of the obfuscation scheme must be verified through manual testing. Note that hardware-based isolation features are preferred over obfuscation whenever possible.

**OWASP MASVS MSTG-RESILIENCE-13**

a. As a defense in depth, next to having solid hardening of the communicating parties, application level payload encryption can be applied to further impede eavesdropping.
<table>
<thead>
<tr>
<th>Ref #</th>
<th>Security Controls</th>
<th>Criticality:</th>
<th>Public Requirements References/Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SII-200</td>
<td>System and Information Integrity</td>
<td>Low</td>
<td>FMCSA GDL 13 Share cybersecurity information with heavy vehicle the industry.</td>
</tr>
</tbody>
</table>

**Applicable Component Categories**
- Mobile App;
- Physical In-Cab Device;
- Connectivity/Communications;
- Cloud or Back-end;

**Requirement**
The vendor shall participate in a cybersecurity information sharing and analysis group in the heavy vehicle industry.

**Verification: Inspection, Demonstration, Test, or Analysis**
Inspection of vendor process documentation confirming participation in information sharing group.

**Remarks**
-