National Motor Freight Traffic Association, Inc.
1001 North Fairfax Street, Suite 600
Alexandria, VA 22314
(703) 838-1810

Motor Freight Carrier Industry Bulletin

Bulletin Name	Issue Date	Last Updated	Version
Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles by the FMCSA	May 13, 2020	May 13, 2020	1.0

NMFTA Bulletin: *Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles* by the FMCSA

Recent publication of the Federal Motor Carrier Safety Administration's (FMCSA) report*, Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles* [https://rosap.ntl.bts.gov/view/dot/49248] (hereafter 'the report'), represents a much needed first step towards specification of cybersecurity requirements for connected heavy vehicle systems. The ELD (Electronic Logging Device) rule was mandated in December 2015 as part of the enactment of the Moving Ahead for Progress in the 21st Century Act (MAP-21). However, MAP-21 did not effectively address cybersecurity aspect of these connected devices. The National Motor Freight Traffic Association, Inc. (NMFTA), through its Heavy Vehicle Cybersecurity (HVCS) program, has been working with heavy vehicle Original Equipment Manufacturers (OEMs), tier 1 suppliers, and Telematics Service Providers (TSPs) to advance cybersecurity requirements of connected heavy vehicle systems from the private sector side. Through these and other activities, we have a unique perspective and special expertise on this subject, which will be leveraged to offer a review of this new report.

The report is a positive move by FMCSA to raise the bar for cybersecurity in heavy vehicles. It offers succinct guidelines highlighted throughout the report body referencing **[GDL #]** designations, which are collected together in a 'checklist' contained in the appendix to the report. The topics covered by these guidelines are broad and appropriate to the subject of cybersecurity of connected heavy vehicle systems.

The guidelines offered in the report are targeted at a wide audience, including (as stated in section *2. Scope*) tractor, trailer, engine and other OEMs, telematics manufacturers and vendors for both the OEM and aftermarket, federal government, state governments, local governments, dealers, service centers, installers, fleet managers and motor freight carriers. Each GDL makes specific recommendations and not all are applicable to each audience party, nor are any of the GDLs – save GDL3 'Perform adversarial testing before a product is finalized (OEMs) or before it is deployed (TSPs/dealers/installers).' – targeted by mention of any party in the GDL description.

Our focus is on our member motor freight carriers, the equipment manufacturers, and the suppliers from whom they purchase. The following table refines the GDLs from the FMCSA report by mapping them to the parties to which they apply. In some cases, the report indicates to whom the GDL applies and we list that information below. In most cases, the association of GDL to a party is implicit and we have inferred the relationship as listed below. Motor freight carriers can use this to disambiguate the responsibility of satisfying any given best practice.

GDL	MF Carriers?	OEMs?	Tier Suppliers?	TSPs?
[GDL 1] Conduct architectural analysis and/or threat modeling during system design		X	X	X
[GDL 2] Follow secure coding best practices.			X	X
[GDL 3] Perform adversarial testing before a product is finalized (OEMs) or before it is deployed (TSPs/dealers / installers).		X	X	X
[GDL 4] Security problems will happen; fail safely.			X	X
[GDL 5] Perform a risk assessment before implementing any telematics or other sort of “connected” technology in vehicles.	X			
[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.	X	X		X
[GDL 7] Obtain [contractual] security guarantees that meet your minimum-security requirements for all products.	X	X	X	X
[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.	X	X	X	X
[GDL 9] Reset default credentials, logs, etc. as soon as the device is received.	X			
[GDL 10] Publish a vulnerability reporting and disclosure policy.		X	X	X
[GDL 11] Have a process for tracking vulnerability disclosures affecting devices being deployed in the fleet.	X			
[GDL 12] Security patches should always be deployed to fleet devices in timely manner (also see GDL 8).	X			
[GDL 13] Share cybersecurity information with heavy vehicle the industry.	X	X	X	X
[GDL 14] Employ an incident response process.	X	X	X	X
[GDL 20] Give applications the least privilege they need to function.			X	X
[GDL 21] Where possible, remove code that isn’t used.			X	X
[GDL 22] Leverage security controls built in to the operating system.			X	X
[GDL 23] Follow best practices for securing cellular or satellite interfaces.		X		X
[GDL 24] Don’t support 2G on cellular modems unless operationally necessary.		X		X
[GDL 25] Assume satellite communication channels have unknown security vulnerabilities and might become compromised at any time.		X		X
[GDL 26] Filter input to any device or interface that gets digitally processed.			X	X
[GDL 27] Limit telematics units’ access to the CAN bus, and whitelist the CAN messages they can send.		X		X
[GDL 28] Enable security monitoring of the telematics system(s) using native tools.				X

[GDL 29] Treat components that connect to both a mobile device and the vehicle as part of the system attack surface, securing accordingly.	X	X		
[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.			X	X
[GDL 31] Make sure debugging interfaces (JTAG, serial, USB) have authentication required.			X	X
[GDL 32] Make sure local wireless interfaces like Bluetooth or Wi-Fi don't provide admin access without authentication.			X	X
[GDL 33] Make sure that the update has not been altered during transit (integrity).			X	X
[GDL 34] Make sure the update comes from a legitimate source (authenticity).		X	X	X
[GDL 35] Prevent the attacker from reinstalling a legitimate but known-vulnerable version (rollback attack).		X	X	X
[GDL 36] Make sure you can revoke and replace cryptographic keys.		X		X
[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.		X		
[GDL 38] Consider adoption of authenticated J1939 components, particularly in safety- and security-critical components.		X	X	
[GDL 39] Only use WPA2 authentication / encryption. Never use WEP, WPS, or "open" Wi-Fi.	X	X	X	
[GDL 40] Always use a complex, unique password per device.	X	X	X	X
[GDL 41] Don't allow a telematics unit to pair to Wi-Fi access points unless they're trusted (e.g., in your depot or motor pool).	X			
[GDL 42] Only allow pairing during device boot.			X	X
[GDL 43] Always use a complex, unique password per device.	X	X	X	X
[GDL 44] Make sure Bluetooth devices support and use Secure Simple Pairing (SSP) rather than legacy pairing.			X	X
[GDL 45] Numeric Comparison is preferred to Passkey Entry for pairing.			X	X
[GDL 46] Use encryption on all wireless communication interfaces.			X	X
[GDL 47] Use authentication on all wireless interfaces.			X	X
[GDL 48] Use a unique, complex password on each device, vehicle, or application.	X	X	X	X
[GDL 49] Change passwords from the manufacturer's default, and change them when personnel leave or change jobs (see GDL 9).	X			
[GDL 50] Have a third party check the implementation of any cryptography your security model depends on.			X	X
[GDL 51] Check whether keys have expired or been revoked.		X		X
[GDL 52] Ensure the ability to remove a Root CA's certificate.	X	X		X

[GDL 53] Consider using hardware security modules if your threat model includes high levels of risk.			X	X
[GDL 54] Disable unnecessary debugging interfaces in production.			X	X
[GDL 55] Authenticate debugging and diagnostic interfaces.			X	X
[GDL 56] Log security-relevant events.	X	X	X	X

Table 1: Association of responsible parties to the GDLs of the report.

The report states that the guidelines serve the purpose of enabling motor freight carriers to obtain "legal security guarantees" from their equipment suppliers. We believe the more comprehensive set of best practices is captured in the NMFTA *Telematics Cybersecurity Requirements Matrix* (hereafter 'the matrix') would form a better a basis for a contractual relationship between a motor freight carrier and an equipment supplier. This matrix was developed in conjunction with producing contract language templates for use by motor freight carriers in procurement of equipment that satisfies cybersecurity requirements, which can be independently verified by the motor freight carrier following the steps in the matrix. The matrix also includes a questionnaire format, which is suitable for motor freight carriers to distribute to their potential and current suppliers. We believe that these questionnaires are better suited for our member motor freight carriers to use in obtaining contractual security guarantees, both because they are designed to be verifiable by the carriers and because they are more thorough. The *Telematics Cybersecurity Requirements Matrix* covers a greater breadth of topics, in greater depth, than the report does. The matrix is being updated concurrently with this bulletin to include the topics covered by the report that were missed in the last release.

Comparing the report and the matrix more closely, we can see that there is a great deal of overlap where the two agree and this overlap is listed below. However, the matrix is a living document, which we are constantly working to improve and, as such, the matrix is presently being updated to increase this overlap. The following GDLs from the FMCSA report are also covered in the most recent release of the matrix:

- [GDL 1] Do architectural analysis and/or threat modeling during system design.
- [GDL 2] Follow secure coding best practices.
- [GDL 3] Perform adversarial testing before a product is finalized (OEMs) or before it is deployed (dealers / installers).
- [GDL 4] Security problems will happen; fail safely.
- [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.
- [GDL 10] Publish a vulnerability reporting and disclosure policy.
- [GDL 14] Employ an incident response process.
- [GDL 20] Give applications the least privilege they need to function.
- [GDL 22] Leverage security controls built in to the operating system.
- [GDL 27] Limit telematics units' access to the CAN bus, and whitelist the CAN messages they can send.
- [GDL 28] Enable security monitoring of the telematics system(s) using native tools.
- [GDL 21] Where possible, remove code that isn't used.
- [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.
- [GDL 31] Make sure debugging interfaces (JTAG, serial, USB) have authentication required.
- [GDL 32] Make sure local wireless interfaces like Bluetooth or Wi-Fi don't provide admin access without authentication.
- [GDL 40] Always use a complex, unique password per device.

- [GDL 43] Always use a complex, unique password per device.
- [GDL 46] Use encryption on all wireless communication interfaces.
- [GDL 47] Use authentication on all wireless interfaces.
- [GDL 48] Use a unique, complex password on each device, vehicle, or application.
- [GDL 54] Disable unnecessary debugging interfaces in production.
- [GDL 55] Authenticate debugging and diagnostic interfaces.
- [GDL 56] Log security-relevant events.

The FMCSA report is a step in the right direction. However, it is lacking may aspects of cybersecurity that are required for connected heavy vehicle systems, in particular telematics. The following security requirements from the NMFTA *Telematics Cybersecurity Requirements Matrix* do not have corresponding guidelines in the report:

- AC-010 Vendor devices will implement least privilege for the memory spaces of processes handling protected data. i.e. data in-use, of the categories of sensitive protected data above, shall be segmented from software components which do not handle such data. Acceptable segmentations include Mandatory Filesystem Access Controls and Mandatory Volatile Memory Access Controls.
- AC-020 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 only are assigned the minimal privileges required to perform the specific, intended, actions of the user or process/service account.
- AC-040 The vendor shall identify all instances where the telematics system includes actions that cannot support access authentication and/or execute with elevated privileges
- AC-041 Identifying information about the connected devices will not be made available without authentication first.
- AC-050 All remote access methods and possible remote actions to/on telematics system shall be documented.
- AC-060 For all components of the system, the vendor shall provide a listing of all wireless communications interfaces of the system and specify how the interfaces can be configured and/or disabled.
- AC-070 Authentication attempts to the vendor’s devices and backends shall be rate-limited to an industry accepted rate.
- IA-010 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.
- IA-020 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."
- IA-030 Cryptographic modules used in the vendors system shall be compliant with Federal Information Processing Standards (FIPS) 140-2: Level 1.
- M-010 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
- M-020 The vendor shall have procedures in place to test backup restoration processes of their own systems and their own facilities on at least an annual basis.
- P-010 The vendor shall have a System Security Plan (SSP) which details a clear and concise understanding of authorization boundaries of your telematics system;
- P-020 The vendor shall have a documented Information Security Architecture (ISA) for the telematics system.
- P-030 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.

- PS-010 The vendor shall have personnel security policies & procedures, position risk categorization, personnel screening, personnel termination, personnel transfer, access agreements & third party personnel security.
- SAA-010 The vendor shall have an Information Security Management Plan (ISMP)
- SAA-030 Vendor shall have Security Testing and Evaluation (ST&E) of the system and/or components which includes all results of the security testing & evaluation, including discovered vulnerabilities and a plan/process to mitigate the discovered vulnerabilities or weaknesses in the system
- SCP-011 Communication path cryptographic protections must not use identities, keys or shared secrets which are common across multiple deployed devices
- SCP-020 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."
- SCP-030 Vendors will supply documentation detailing both what data is protected at rest by cryptography and what is not protected at rest by cryptography. Vendors are encouraged to expand the list of categories of data which will be protected on-device."
- SCP-040 Data, of the categories above, being protected will be so-protected using cryptographic keys which are not correlated to any public information about the devices. Where public information is any information that is visible (externally or internally) on the device or discoverable by searches based on that visible information.
- SCP-050 All customer-related data 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
- SCP-090 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."
- SCP-100 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)
- SCP-110 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.
- SII-010 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."
- SII-040 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.
- SII-060 The vendor shall provide a means (and document the process) for customers to verify the firmware in their devices.
- SII-081 The vendor shall utilize protective mechanisms to protect components from unauthorized runtime/volatile modification of code.
- SII-110 The vendor conducts regular vulnerability scans of operating environment to verify software components in use have been patched according to remediation SLAs.
- SII-180 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

- SII-190 The vendor’s software will have software resiliency measures included that will slow the progress of tampering and reverse engineering efforts.

In summary, the gaps in cybersecurity requirements contained in the FMCSA report include requiring that vendors use runtime code protections, boot verification that uses asymmetric cryptography, a vulnerability remediation process, communications protections to the backend and ensuring no authenticators used are predictable. Additionally, the requirements highlighted above – and all of the other requirements in the Matrix –include verification steps which ideally can be performed by motor freight carriers for their own assurance purposes.

FMCSA’s recent report is a step in the right direction for the industry. NMFTA will integrate the guidelines that were not already covered in the matrix as additional requirements and include references to guidelines from the report for those requirements that were already covered. We recommend that motor freight carriers, when working to satisfy the report’s supply chain guideline GDL7 “Obtain legal security guarantees that meet your minimum-security requirements […]”, refer to the matrix, its questionnaires and the associated contract template language project to better realize contractual security guarantees through its detailed requirements with external references and verification steps that can be performed by the motor freight carriers.

As previously stated, the matrix is a living document that NMFTA and its working group members contribute to on an ongoing basis. We have identified guidelines from the FMCSA report that were not addressed in the matrix including disabling 2G on cellular modems, filtering all inputs to digital processes, integrity detection on transfers, preventing rollback of firmware, including the ability to revoke and replace cryptographic keys and the ability to remove a root certificate authority from devices. We will collaborate with our working group and create updates to the matrix that incorporate the complete set of topics that can be derived from the report’s guidelines. See the pull request *https://github.com/nmfta-repo/nmfta-telematics_security_requirements/pull/8* for more details. The matrix will also be updated to include references to the guideline GDLs from the report in the ‘external references’ column where cybersecurity requirements overlap, as noted above.

Appendix A: Detailed Review Feedback

In reviewing the FMCSA report*, Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles* [https://rosap.ntl.bts.gov/view/dot/49248] (hereafter 'the report') we made extensive notes on ways that it could be improved for motor freight carriers and for the industry. We offer the following review feedback as a resource to our motor freight carrier members who are also reviewing the report and to the FMCSA for their consideration in future revisions of the report.

1. The guideline "[GDL 23] Follow best practices for securing cellular or satellite interfaces" is too ambiguous to be actionable by any reader. Being that the report **is a** guidelines doc, more detail is needed, such as more external references, to define what constitutes best practices for securing cellular or satellite interfaces. It is possible that GDL 24, 25 & 26 are the details. In which case, delete this GDL 23.
2. The report uses the term "purchasing vendor" (pp 17-18) without introduction or context. It is not clear to which party in the heavy vehicle supply chain that this term is referring.
3. The report offers the guidance to carriers (it is assumed) "[GDL 41] Don't allow a telematics unit to pair to Wi-Fi access points unless they're trusted (e.g., in your depot or motor pool)." This omits that devices should only be allowed to 'pair' **when necessary** but also conflates *trusting* a device with the device being *trustworthy*. We recommend this guideline be re-worded to '[GDL 41] Don't allow a telematics unit to pair to Wi-Fi access points unless it is necessary and the device is trustworthy (i.e. it satisfies all of the relevant guidelines that your organization has set forth for equipment supplier cybersecurity quality).'
4. The report suggests that "[GDL 53] Consider using hardware security modules if your threat model includes high levels of risk." This suggestion is hedging too heavily to result in adoption the modules and hence the purported increase in security which they should bring. The report is a guidelines document which can recommend a course of action and it should do so. The introduction of the report established that heavy vehicle equipment and telematics systems do pose high levels of risk. In our estimation, the level of maturity needed to add hardware security modules (HSMs/TEEs/TPMs etc.) is not present in the industry yet.
If and when these guidelines are adopted, the second-order problem OEMs and suppliers will inherit will be how to securely provision these additional secure hardware subsystems? The recent paper by the NMFTA and NCC Group http://www.nmfta.org/documents/hvcs/Secure_Device_Provisioning_Best_Practices.pdf prepares suppliers for this next-order problem. Should hardware security be included in a guideline then the reader should be directed to appropriate resources on how to securely provision hardware security.
5. The report recommends "[GDL 40] Always use a complex, unique password per device." This recommendation is duplicated in GDL 43 and GDL 58. However, it is not sufficient to require that a password be unique and complex to result in an improvement in access control to the devices and applications that use these passwords. e.g. the device MAC would satisfy this recommendation, but it would not be a good password because it is a publicly obtainable piece of information. We believe that the report should further recommend that the password be uncorrelated to any and all public information about the device.
6. In the context of recommendation "[GDL 28] Enable security monitoring of the telematics system(s) using native tools" the report notes that deploying anti-virus into head units will become common practice in the future. This suggests that these technologies are, in fact, what is being recommended by the term "native tools." This recommendation is ignoring the well-established deleterious effects of these technologies to system security in PC – with the important exception of rapidly updating sample databases. The nature of antivirus SW is to parse attacker controlled data and to also have sufficient privileges to create and edit executables in the system. The exception noted is the case where the antivirus software and its signature databases can be updated rapidly in response to events distributed across global PC populations; however, that level of connectivity in vehicles is not now nor in our immediate future for all of the motor freight carriers who must deal with connectivity issues across the continent on a daily basis.

7. The report recommends "[GDL 7] Obtain legal security guarantees that meet your minimum-security requirements for all products.". We believe that 'contractual' would be a better term than 'legal'. Assurances of the cybersecurity posture of procured equipment should be sought in the form of contractual agreements between carriers and their suppliers: OEMs and TSPs. Including a checklist/questionnaire in the RFP provided by the carrier to the OEM/TSP that include requirements for cybersecurity is an appropriate place to gain assurances contractually. At the RFP stage of engagement all expectations of security requirements can be made clear for the supplier relationship going forward.

   This single recommendation seems like it is covering too many aspects and should be broken up into further GDLs: 1) that OEMs/TSPs/Suppliers have vulnerability management programs 2) that OEMs/TSPs/suppliers have vulnerability monitoring and disclosure programs; and this *in addition to* the guideline that carriers 'obtain contractual security guarantees [...].' Much like the statement made by the report in context of "[GDL2] Follow secure coding best practices" , "Manufacturers of telematics systems should take positive steps to implement and enforce secure coding practices, while their customers should ask potential vendors what practices they follow." The requirement is two-fold, on both the carriers procurements methods and the suppliers development and production methods.

   Such a pair of guidelines would help move the industry have minimum security requirements for the equipment that they procure and furthermore that the security requirements that they should have in contract language are all of those guidelines which are targeted at OEMs/TSPs.
   For motor freight carriers, it would be beneficial to recommend that they require a complete set of cybersecurity requirements from the OEMs or TSPs. Because security is an emergent property of systems, the motor freight carriers will not realize a cybersecurity posture increase unless the equipment they procure satisfies complete sets of requirements, rather than cherry-picked subsets.

8. In the context of "[GDL 56] Log security-relevant events" the report asserts that these logs should be "digitally signed to be tamper-evident." This is a valid recommendation in and of itself; however, it is not capture in either the GDL56 text, nor in any other guidelines in the report.

9. In the context of "[GDL 26] Filter input to any device or interface that gets digitally processed," the report recognizes that a common pattern of compromise follows attacker-controlled inputs being provided to target processes. Then further discusses 'filtering' of these inputs along with "Where possible, external input should be cryptographically protected and verified (e.g. Transport Layer Security (TLS) protocol or other accepted authentication and encryption mechanisms)." Ultimately, the report is only recommending that inputs to processes get filtered. It then conflates filtering with cryptographic authentication and misses the more important security requirement that the software handling potentially attacker-controlled data should be itself robust against these inputs. Cryptographic authentication is very different from sanitizing/filtering inputs and both filtering or authentication are not a substitute for segmenting memory spaces of input parsers from other execution and/or using provably correct or memory safe languages for input processing. We are concerned that putting this recommendation here will mislead the reader into thinking that adding encryption will mitigate the risks of unsafe input handling.