Attachment A

Date: 15 March 2021	Commenter: DENSO	Document: NHTSA FRN (CySec BP) 12 Jan 2021

MB/ NC[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ $G.n_i$ (e.g. [G.2])	Type of comment[2]	Comments	Proposed change
DN-01	N / A	N / A	Ge	Generic Gap within Scope / Purpose of BP Document: NHTSA document does not provide rationale for many of the requirements. When providing references to other standards, often some requirements do not include the location (e.g. section or clause) within the specified reference.	Recommendation: NHTSA should include rationale within all of their requirements.
DN-02	Ge	N / A	Te	Missing Generic Best Practice: Process-level Traceability	Recommendation: NHTSA's document mainly views traceability under the scope of document control. Beyond that, traceability for tracking cybersecurity requirements all the way to the implementation stage is an important aspect in ensuring secure product development.
DN-03	Ge	N / A	Te	Scope description of document is unclear—it does not convey safety-oriented focus.	Recommendation: Scope of document should clarify that the best practices outlined within the document are safety-oriented. This document is not intended to include situations where safety is not impacted.
DN-04	4.0	Paragraph 1	Te	Vague description of what is considered a "successful attack": "…ensure vehicle systems take appropriate and safe actions, even when an attack is successful"	Proposal: Add clarity on scope of "successful" attack. Examples: adding acronyms or list examples of what are considered "successful attacks."
DN-05	4.0	G.9	Ed	**Original** [G.9] Clear cybersecurity standards should be specified and communicated to the suppliers that support the intended protections.18 **Comment** Not clear what cybersecurity standards means here. ISO/SAE 21434 mentions that cybersecurity requirements shall be specified and communicated to suppliers. Also, cybersecurity protections are not always standardized.	Proposal: Replace "Clear cybersecurity standards" with "cybersecurity requirements"

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Attachment A

Date: 15 March 2021	Commenter: DENSO	Document: NHTSA FRN (CySec BP) 12 Jan 2021

MB/ NC[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ $G.n_i$ (e.g. [G.2])	Type of comment[2]	Comments	Proposed change
DN-06	4.2.5	Footnote 18 for G.9	ed	Maybe Typo :1711 ***and responsibilities between customers and 1711 suppliers for cybersecurity activities.	Remove "1711"
DN-07	4.1	G.2 [c]	Te	Vehicle cybersecurity considerations should not be limited to safety-related considerations. The cybersecurity-related considerations should consider entire vehicle design process, not just vehicle safety design process. "Enabling an independent voice for vehicle cybersecurity-related considerations within the vehicle safety design process."	Proposal: Remove term "safety": "Enabling an independent voice for vehicle cybersecurity-related considerations within the vehicle design process."
DN-08	4.2.1	G.3	Te	Use of the term "unreasonable" is vague and not defined. "…systems free of unreasonable safety risks…."	Proposal: Remove "free of unreasonable" and replace with the following: "…with the goal of designing systems to mitigate potential safety risks, including those from potential…"
DN-09	4.2.1	G.3	Te	Use of the term "robust" is vague and not defined. "The automotive industry should follow a robust product development process…."	Proposal: remove "robust": "…follow a product development process…"
DN-10	4.2.11	G.23	Te	Auto-ISAC is the only entity specifically mentioned here, but other organizations such as SAE and ISO should also be mentioned. Otherwise, this can be seen as biased promotion of Auto-ISAC by NHTSA. "[G.23] Manufacturers should actively participate in automotive industry-specific best practices and standards development activities through Auto-ISAC	Recommendation: Include other organizations such as SAE and ISO. Instead of just Auto-ISAC. "[G.23] Manufacturers should actively participate in automotive industry-specific best practices and development activities through recognized industry organizations (e.g. Auto-ISAC) and standards development organizations (e.g. SAE, ISO, IEEE, NIST,

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ G.n$_i$ (e.g. [G.2])	Type of comment[2]	Comments	Proposed change
				and other recognized standards development organizations."	etc.)."
DN-11	4.2.4	G.7	Te	Section title "Unnecessary Risk Removal" does not align with G.7's usage of "removed" or "mitigated." "4.2.4 Unnecessary Risk Removal"	Proposal: Change subsection title to "Risk Modification" or "Removal or Mitigation of Safety-Critical Risks."
DN-12	4.2.6	G.11	Ed	Requirement should be stricter and wording should be modified to reflect that. "Footnote 21: These details could include: the licenses that govern those components, the versions of the components used in the codebase, and their patch status."	Proposal: Change wording from "could" → "should." "Footnote 21: These details should include: the licenses…"
DN-13	4.2.7	G.14	Ed	Wording can be improved: "who are highly incentivized to identify vulnerabilities"→"whose purpose is to identify vulnerabilities in the system." "…and who are highly incentivized to identify vulnerabilities."	Proposal: Change "who are highly incentivized to identify vulnerabilities" → "whose purpose is to identify vulnerabilities within the system."
DN-14	4.2.7	Subsection Title	Te	"Penetration Testing and Documentation" implies that the only type of testing to be performed is penetration testing within this section	Proposal: Rephrase title to be more inclusive: "Product Cybersecurity Testing and Documentation"
DN-15	4.6.1	G.34	Te	"expected life span" Not commonly utilized industry term	Proposal: change "expected life span" to "end of cybersecurity support" Reason: alignment with ISO/SAE 21434 Clause 14
DN-16	4.6.1	G.35	Te	"robust version control protocol" is unclear.	Recommend: [G.35] Documents should follow a strict policy for both configuration management and documentation management, and should be maintained accordingly. EXAMPLE: revisions, new information, new data, new research results, etc. * add footnote reference to: ISO/SAE 21434 [RQ-05-11], [RQ-06-12]
DN-17	4.6.2	G.37	Te	"…audits annually." ISO/SAE 21434 does not specify frequency of audits – only that they can be done periodically ISO/SAE 21434 [RQ-05-17]	Proposal: Rephrase "annually" → "periodically": "…audits periodically."

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Attachment A

Date: 15 March 2021	Commenter: DENSO	Document: NHTSA FRN (CySec BP) 12 Jan 2021

MB/ NC[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ $G.n_i$ (e.g. [G.2])	Type of comment[2]	Comments	Proposed change
DN-18	4.6.2	Final Paragraph	Te	"A public version of audit reports…can assist in demonstrating the organization's commitment to product cybersecurity." There is no existing requirement (e.g. ISO/SAE 21434) for publishing audit reports.	Proposal: Remove this statement from FRN. Alternative Proposal: clarify this is meant for governmental/public agencies (add appropriate reference)
DN-19	6.2	G.41	Ed	All aftermarket device manufacturers should be held to similar standards. The word "strong" can leave this open to misinterpretation. "[G.41] Aftermarket device manufacturers should employ strong cybersecurity protections on their products."	Proposal: Change "strong" → "reasonable" "…should employ reasonable cybersecurity protections…"
DN-20	6.2	First paragraph	Te	Unclear phrasing related to "safety-of-life" "…connect with cyber-physical systems that may impact the safety-of-life…"	Proposal: "…that may impact the physical safety of vehicle occupants and pedestrians…"
DN-21	7.0	G.42	Te	Missing reference to "right to repair" laws "[G.42] The automotive industry should consider the serviceability of vehicle components and systems by individuals and third parties."	Recommendation: Add footnote/reference to "right to repair" laws as example of what should be serviceable
DN-22	7.0	G.43	Te	Unclear phrasing: "…industry should provide strong vehicle cybersecurity protections that do not unduly…"	Proposal: Replace "strong" with "reasonable" "…industry should provide reasonable cybersecurity protections that do not unduly…
DN-23	7.0	Final Paragraph	Te	Unclear phrasing: "However, cybersecurity should not become a reason to justify limiting serviceability. Similarly, serviceability should not limit strong cybersecurity controls."	Proposal: Replace "strong" with "reasonable" Utilize consistent phrasing throughout FRN "However, cybersecurity should not become a reason to justify limiting serviceability. Similarly, serviceability should not limit reasonable cybersecurity controls."
DN-24	8.2	T.3	Te	Lack of references to cryptography standards. "[T.3] Cryptographic credentials that provide an authorized, elevated level of access to vehicle computing platforms should be protected from disclosure."	Recommendation: This requirement [T.3] should include references to some of NIST best cryptography practices.
DN-25	8.7.3	T.18	Te	Technical Best Practice can be expanded to reference other best practices or standards. "[T.18] Appropriately protecting services over such ports to limit use to authorized parties."	Include reference to other best practices or standards, such as NIST 800 175B.

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Attachment A

Date: 15 March 2021	Commenter: DENSO	Document: NHTSA FRN (CySec BP) 12 Jan 2021

MB/ NC[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ $G.n_i$ (e.g. [G.2])	Type of comment[2]	Comments	Proposed change
DN-26	4.2.11	N / A	Ge	Missing General Best Practice related to: Secure Coding Practices - Developers of ECU software should follow secure and safe coding best practices and standards such as MISRA C and CERT C	Recommendation: Add new General BP within section 4.2.11 Industry Best Practices.
DN-27	4.2.4	G.7	Te	"Unavoidable and Unnecessary" terminology is also unclear and vague. Ambiguity creates potential for future challenges. "4.2.4 Unnecessary Risk Removal [G.7] Any unreasonable risk to safety-critical systems should be removed or mitigated to acceptable levels through design, and any functionality that presents an unavoidable and unnecessary risk should be eliminated where possible."	Proposal: Modify G.7 "unavoidable and unnecessary risk should be eliminated where possible." to **"**reasonable & foreseeable risk should be eliminated where possible." Recommendation: move G.7 into G.4 as an example or note or sub-requirement.
DN-28	4.2.6	[T.x] after [T.14]	Te	Missing Generic Best Practice: Network based intrusion detection systems (NIDS) to implement "Identify, Detect, Protect, Respond, Recover" from the NIST Cybersecurity framework referenced in [G.1] for Vehicle network systems and ECU network components such as CAN, LIN, FlexRay, Ethernet etc.	Proposal: Add a new technical comment [T.x] after [T.14] for NIDS as a best practice. Include footnote to reference NIST SP 800-94.
DN-29	4.2.9	G.18	Ge	Manufacturers should not be forced to join the Auto-ISAC in order to be in compliance with this best practice. Instead, information should be shared with all affected parties and supplier should consider sharing relevant information with entities such as the Auto-ISAC. "…this information should be analysed and shared with industry through the Auto-ISAC."	Proposal: Remove requirement to be part of Auto-ISAC from [G.18]. Option 1: Change to: "Information should be shared with all affected parties and supplier should consider sharing this information with entities such as Auto-ISAC." Option 2: "information should be shared with all affected parties. NOTE: Supplier may consider sharing this information with external entities such as Auto-ISAC."
DN-30	4.3	G.25	Te	Unclear on what "an impact on their own systems" is referring to – Auto-ISAC community standards already encourage collaboration. "…collaborate in expeditiously exploring containment options and countermeasures to reported vulnerabilities, regardless of an impact on their own systems."	Recommendation: Clarify (1) collaboration; (2) remove final phrase "regardless of an impact on their own systems": "Members of the Auto-ISAC community should collaborate to expeditiously explore containment options and countermeasures to reported vulnerabilities."

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Attachment A

Date: 15 March 2021	Commenter: DENSO	Document: NHTSA FRN (CySec BP) 12 Jan 2021

MB/ NC[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ $G.n_i$ (e.g. [G.2])	Type of comment[2]	Comments	Proposed change
DN-31	6.1	G.39	Te	"Reasonable" is vague. If an issue arises, it may be challenged. "[G.39] The automotive industry should consider the incremental risks that could be presented by these devices when connected with vehicle systems and provide reasonable protections."	Proposal: Change document structure of G.40 → move [G.40] to become an EXAMPLE under G.39 in order to provide sufficient explanation of what is meant by "reasonable protections" "[G.39] The automotive industry….reasonable protections. EXAMPLE: Any connection to…appropriate limited access."
DN-32	8.1	T.1	Ed	Wording change from "should" to "must" in order to change from weak to strong requirement. "…Developer-level access should be limited or eliminated…"	Proposal: Change "should" to stronger word such as "must" or "shall". "…Developer-level access must be limited or eliminated…"
DN-33	8.1	T.2	Ed	Wording change from "should" to "must" in order to change from weak to strong requirement. "…developer-level debugging interfaces should be appropriately protected to limit…"	Proposal: Change "should" to stronger word such as "must" or "shall "…developer-level debugging interfaces must be appropriately protected to limit…"
DN-34	8.2	T.4	Ed	Unclear phrasing: "…should not provide access to multiple vehicles."	Proposal: change "multiple" to "other." "…should not provide access to other vehicles."
DN-35	8.2	T.4	Ed	Unclear phrasing: "should not provide access"	Proposal: replace "should not provide access" to "should not provide fleet-wide access."
DN-36	8.7	T.14	Te	Unclear if inclusive of non-network isolation techniques such as hypervisors. [T.14] Network segmentation and isolation techniques should be used to limit connections between wireless-connected ECUs and low-level vehicle control systems, particularly those controlling safety critical functions, such as braking, steering, propulsion, and power management.	Recommendation to move [T.14] into G.8. With revised [G.8], Modify wording to be more broad and include both network-based and host-based techniques.
DN-37	8.7	T.n	Te	Missing Technical Best Practice: Host based intrusion detection systems (HIDS) to implement "Identify, Detect, Protect, Respond, Recover" from the NIST Cybersecurity framework referenced in [G.1] for Vehicle and ECU software components.	New section [8.x] Technical BP to be added into section 8. Include footnote to reference NIST SP 800-94. Proposal: 8.x - Runtime Software & System Integrity

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Attachment A

Date: 15 March 2021	Commenter: DENSO	Document: NHTSA FRN (CySec BP) 12 Jan 2021

MB/ NC[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ $G.n_i$ (e.g. [G.2])	Type of comment[2]	Comments	Proposed change
					Vehicle software may have residual risk in the form of software vulnerabilities. Memory corruption attacks like buffer overflow [CWE 120] can allow an attacker to achieve RCE and arbitrary memory access in vehicle systems. In order to detect and prevent exploitation of such vulnerabilities, [T.x] Host based intrusion detection systems (HIDS) should be implemented to "Identify, Detect, Protect, Respond, Recover" from memory corruption attacks. Note: Add CWE (Common Weakness Enumeration) to list of terms and abbreviations appendix
DN-38	8.7.5	T.20	Te	Not clear where this requirement is to be applied. "[T.20] Manufacturers should plan for and create processes that could allow for quickly propagating and applying changes in network routing rules to a single vehicle, subsets of vehicles, or all vehicles connected to the network.	Add clarification to where to apply requirement. For example, cell network.
DN-39	8.9	T.21, T.22, T.23	Te	Sections [T.21, T.22, and T.23] are similar and not enough distinction between the two to be separate sections.	Recommendation to merge section 8.9 → 8.8.
DN-40	8.9	T.23	Te	List appears incomplete and does not state examples. "[T.23] Take into account, when designing security measures, the risks associated with compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities."	Recommendation to add examples or include footnote reference to additional examples.

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial