



TRANSMITTED ELECTRONICALLY THROUGH REGULATIONS.GOV

March 15, 2021

Docket Management Facility M-30
US Department of Transportation
National Highway Traffic Safety Administration
West Building, Ground Floor, Room W12-140,
1200 New Jersey Avenue SE,
Washington, DC 20590

Subject: Cybersecurity Best Practices for the Safety of Modern Vehicles [NHTSA–2020–0087]

UL appreciates the opportunity to comment on the National Highway Traffic Safety Administration's (NHTSA) *Cybersecurity Best Practices for the Safety of Modern Vehicles*. UL supports NHTSA seeking information on the Agency's updates to the initial (2016) edition of this document.

Since its inception in 1894, UL serves a mission of promoting safe living and working environments for people everywhere and fulfills a promise of facilitating the flow of goods across borders. Grounded in science and collaboration, UL's work empowers trust in pioneering technologies, from electricity to the internet. We help innovators deliver safer, more secure products and technologies through a wide range of research, standards development, and testing and certification services.

In a world of increasingly connected infrastructure, safety cannot exist without cybersecurity. UL agrees with NHTSA that given the proliferation of computer-based control systems, software, connectivity, and onboard digital data communication networks, modern vehicles need to consider additional failure modes, vulnerabilities, and threats that could jeopardize benefits if new safety risks are not appropriately addressed. UL values the partnership on vehicle cybersecurity we have with NHTSA by virtue of the memorandum of understanding (MOU) established between UL and NHTSA in May 2019. Given the inextricable linkages between safety and security in modern vehicles, this MOU allows for examination of methodologies, tools, and metrics associated with the testing and evaluations of vehicle cybersecurity and serves as a basis for UL and NHTSA to share related test data.

UL supports the holistic approach NHTSA takes towards addressing cybersecurity and privacy risks, both in terms of the principles, and in the recognition that cyber resilience requires continuous attention. Security is a continuous process. Assisting the industry to adopt a systematic and continuous process to evaluate risks would indeed enhance awareness of cyber resilient measures to be implemented.

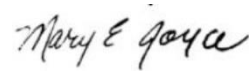
Please find below a list of suggested clarifications to best practices documents. As NHTSA and the US Department of Transportation move forward with efforts to update the *Cybersecurity Best Practices for the Safety of Modern Vehicles* and contemplate other actions to pave the way for safe deployment of such modes of transportation, UL stands ready to assist. If you have any questions regarding this submission or would like to discuss UL's comments, please do not hesitate to contact Thomas Daley, UL Global Government Affairs, at thomas.daley@ul.com. Thank you for your attention to these comments.

Sincerely Yours,



Isabelle Noblanc
VP&GM, Identity Management & Security
UL LLC

Sincerely Yours,



Mary Joyce
VP&GM – New Mobility
UL LLC

Suggested Clarifications and Comments

Page 3: The bottom section lists a number of criteria and conditions that the approach of G.1 should fulfill, but the measure of success is not quantified. What constitutes a timely response is open for interpretation; this ambiguity appears in several places throughout the document.

G.2.c: An independent voice is not the same as an individual empowered with sufficient authority to influence/steer the processes that impact cybersecurity. As currently phrased, it can be an individual who issues advice, which can be disregarded. The same goes for the last paragraph; it should be an officer who is responsible, accountable and additionally authorized and empowered to make decisions that impact security.

G.3: A robust development process is not defined; UL proposes that NHTSA define a process aligned with recommendations outlined by the National Institute of Standards and Technology (NIST). No system can be designed such that it will be free of potential cybersecurity threats, so this should perhaps be phrased differently to reflect that reality (i.e., minimize potential cybersecurity threats and maximize proactive responses).

G.6: This is a specific case of the generic risk assessment that should be performed, which makes it a bit superfluous as a requirement. The first paragraph of 4.2.3 phrases that it should be prudent to consider sensor data tampering, and then the requirement proceeds to enumerate a list of required items (via use of the word “should”). UL recommends avoiding a specific list of requirements, and instead provide an example of sensor tampering with the statement that vendors should review and identify all of these types of risks.

G.7/G.8: It is inconsistent with frequently used practices to provide a blank statement that any avoidable risks due to unnecessary functionality should be eliminated. As an example does that mean that a video screen for the front seat passenger should not be allowed as it could distract the driver? The requirement itself is not the issue, but what constitutes as “unnecessarily” in this context is ambiguous/subjective. UL recommends clarifying this requirement.

G.21: UL recommends defining “periodic” as the term will need a minimum period clause or at least require that the manufacturer has a written justification for the period length. Periodically also can mean every 10 years which may not be the intention here.

G.22: This is a duplication of G.3 which already states that a development system should be designed such that it ensures minimal safety risks including those stemming from cybersecurity. The standards referenced here would therefore be appropriate to reference in G.3 as well. For consistency this could be grouped together with G.3

G.24(b): Timely sharing of information has been mentioned a few times in previous clauses, but no quantification of “timely” is provided. We know, for example, that OEMs eventually publish to Auto-ISAC, but not before they have mitigated their risks. Note that publishing vulnerabilities to Auto-ISAC may create a risk if this has not been managed by the OEM already.

G.29: “Disposition” in this context is an odd choice of words. UL recommends to rephrase the sentence as “The nature of the vulnerability and the rationale for how the vulnerability is managed should also be documented”

Page 10: In this instance, reporting to Auto-ISAC is phrased such “as soon as possible.” Is there a legal definition that quantifies how “as soon as possible” would be interpreted in this context? To wit, does “as soon as possible” equate to when the manufacturer becomes aware of the problem, or when they resolved or otherwise mitigated the problem? UL recommends defining “as soon as possible.”

G.34: Expected life span of a vehicle is vague; this also can be defined as end of support by the manufacturer. At this point the manufacturer can make sure any remaining vehicles are in a safe state, and terminate support. It may otherwise be the case that vehicles are still supported because they exceed the average expected lifetime, but the process to support these vehicles no longer exists. UL recommends defining “expected life span.”

G.39/G.40: Without some minimum conditions/requirements for third party systems to access the vehicle these provisions effectively would kill access by third party devices and their market.

G.41: “Strong cybersecurity protections” is a very ambiguous phrase. A default operating system distribution will use strong cybersecurity protections; however, how such systems are configured and used is what affects security. UL recommends that NHTSA phrase this as: “Aftermarket manufacturers should perform a thorough risk assessment and apply appropriate security protections as needed to mitigate risks identified.”

G.42: “Considering serviceability” is ambiguous and lacks any requirement for action, i.e., someone can consider something and still say no. The paragraph following this clause explains the balance to be struck much better and makes it more explicit that this balance must be found. UL recommends aligning “considering serviceability” with the subsequent paragraph.

T.7: What does “ad-hoc” mean in this instance? It appears to refer to non-industry standard crypto systems. UL recommends clarifying or defining what is meant by “ad-hoc.”

T.21: “State of the art” is ambiguous phrasing. AES encryption is (still) state of the art, but it should not be used for everything. UL believes the requirement should suggest that manufacturers have a plan, a (written) risk analysis, and a set of measures that are suitable for dealing with these risks.