**Comment from Sandia National Laboratories**

Section 4.2.2: Risk Assessment and [G.4]
Comments: Risk assessments should also consider the insider threat, which includes vehicle technicians, or others who may have unrestricted – and potentially privileged – access to the vehicle. This is mentioned in Section 8.9 [T.23] but also applies in this section.
In addition, the risk assessment should be ongoing and not just be a single step in the entire development process. For example, ideally it should be included as a step in each of the phases of the development process.

Section 4.2.3: Sensor Vulnerability Risks [G.6]
Comments: The list could also include road sign spoofing, like that accomplished with the "Tesla projector attack."
https://arstechnica.com/cars/2020/01/how-a-300-projector-can-fool-teslas-autopilot/

Section 4.2.7: Penetration Testing and Documentation
Comments: It would be beneficial to also include Design Assurance Assessments to the process. This approach allows the requirements documentation, business use cases, and design information to be assessed, allowing vulnerabilities to be eliminated or mitigated prior to moving forward in the development process.

Section 4.5: Organizational Incident Response Process [G.27[d]]
Comments: Typo since [G.26] does not have sections a-c.

Section 8.2: Cryptographic Credentials
Comments: We recommend this section includes additional references – government or industry – on cryptographic standards and processes. These could include;
•NIST SP 800-175B Rev. 1 Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies
•NIST SP 800-175A Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
•NIST also has a page for Cryptographic Standards and Guidelines, located at: https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

Section 8.3: Vehicle Diagnostic Functionality
Comments: The claim the Public key cryptography techniques are more secure than symmetric key systems should be caveated with “properly implemented techniques” are “generally” more secure…

Section 8.5: Vehicle Internal Communications
Comments: In addition to being inaccessible through external interfaces, internal messages should be encrypted where possible and feasible, and where it won't interfere with safety-critical systems. This will prevent replay attacks and other forms of malicious activity.

Section 8.6: Event Logs
Comments: If the vehicle is connected to a network (ex. cellular modem), logs for critical events - like updating the firmware - should be uploaded immediately to ensure they are not deleted by a malicious actor.

SAND Number: SAND2021-2600 O
SNL is managed and operated by NTESS under DOE NNSA contract DE-NA0003525