**Comment from Sandia National Laboratories**

Section 1: Purpose of This Document: Prioritizing vehicle cybersecurity also means establishing internal processes and strategies to ensure systems will be safe under expected real-world conditions, including in the presence of potential vehicle cybersecurity threats.
Comments: Identifying that processes and strategies need to address real-world conditions is critical. Planning only for the “sunny day scenario” is likely to leave vulnerabilities when real-world usage deviates from the perfect scenario.

Section 2: Scope: The security of a system is measured by its weakest link.
Comments: Also a critical point. It doesn’t help if you harden a few areas of the system if others are left unprotected. As an analogy, it doesn’t matter if you have a steel door on the front of your house if the patio door is made of glass – or unlocked.

Section 4: General Cybersecurity Best Practices: Eliminate sources of risks to safety-critical vehicle control systems where possible and feasible.
Comments: Calls out the fact that not every risk can be addressed – and definitely not in a practical manner. Allows for organizations to identify things that can’t be addressed under these best practices without having to disregard the entire set of practices since they are unable to apply them everywhere.

Section 4.2: Vehicle Development Process with Explicit Cybersecurity Considerations: Cybersecurity considerations encompass the full lifecycle of the vehicle, which includes conception, design, manufacture, sale, use, maintenance, resale, and decommissioning.
Comments: Considering the entire lifecycle is critical. Not only can vulnerabilities introduced in design affect things downstream, but vulnerabilities found later in the cycle can affect vehicles still in the earlier stages. For example, if a vehicle is in an accident and is no longer usable, it may be possible for an attacker to pull out components and extract private keys or other critical information that could be used to compromise vehicles that are still on the road.

Section 6.2: Aftermarket device manufacturers: Aftermarket device manufacturers should consider that their devices connect with cyber-physical systems that may impact the safety-of-life.
Comments: This is a good reminder to these manufacturers that, while their specific aftermarket device may not be critical to life safety features, it may be able to interact or disrupt them. Calls out the serious nature of being in this ecosystem.

Section 8.1: Developer/Debugging Access in Production Devices: Merely physically hiding connectors, traces, or pins intended for developer debugging access should not be considered a sufficient form of protection.
Comments: Excellent reminder to not rely on security through obscurity.

Section 8.7: Wireless Paths into Vehicles: Privilege separation with boundary controls is important to improving the security of systems.
Comments: Ideally communication between components or systems should only be between systems that need to communicate. This prevents a malicious or malfunctioning component from impacting normal vehicle operation or life safety systems.

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