The California Highway Patrol (CHP) thanks NHTSA for soliciting public comment on cybersecurity best practices that have safety implications for motor vehicles and motor vehicle equipment. The CHP concurs with NHTSA's current focus on providing guidance on best practices which allows for future development and improvements in these processes, while also aligning with industry cybersecurity-related initiatives and efforts by organizations, such as SAE International (SAE), the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and the Automotive Information Sharing and Analysis Center (Auto-ISAC).

(1) General Cybersecurity Best Practices:
Referenced source materials, such as those under Standards G.22 and G.33, serve as a valuable reference to companies involved in development and testing. Furthermore, allowing for the industry itself to identify many of its own best practices is a stimulus towards advancement. Aligning with Standard T.22 and in light of the recent supply-chain attack (AKA Solar Winds) in which malicious actor(s) compromised a software company and inserted malware into the programming code, manufacturers should take all cybersecurity precautions to secure the network at their businesses and perform exhaustive testing of any updates prior to being deployed to vehicles.

(2) Education:
Documentation and sharing of resources, such as those referenced under Standards G.12, G.22, and G.23, allow for industry efforts to collectively progress by leveraging accomplishments and recognizing vulnerabilities discovered by other contributors. The CHP concurs with the guidance and supports collaboration to help support educational efforts.

(3) Aftermarket/User Owned Devices:
Modern vehicles continue to have increased use of and dependence upon software-based systems to control basic vehicle functions, Advanced Driver Assistance Systems (ADAS), and Automated Driving Systems (ADS). As software-based systems increase, the prevalence of aftermarket devices and applications capable of accessing those systems will also continue to increase. These aftermarket devices may range in function from basic data and systems analysis related to use tracking, performance, and diagnostics, or could include temporary or permanent reprogramming or bypassing of certain parameters or software components. This reprogramming or bypassing could be done for gains of performance or economy, for falsifying compliance or function, or potentially, for malicious purposes. Even if not malicious in nature or design, any software changes that might have any impact on ADAS or even ADS systems as they are developed could result in safety reductions. As vehicle systems increasingly employ technology for basic functions, such as throttle and braking being applied entirely by electronics with no physical component interaction between a driver and their intended action, the public becomes increasingly dependent upon the security and reliability of these systems.

From an investigative perspective, these advancements constitute a forensic need to retroactively be able to identify time, device, and actions performed by aftermarket devices or even by wireless-access applications. The ability to acquisition post-crash data from involved vehicles remains a critical component of crash investigation. Data recorded from vehicle sensors can be invaluable in determining the human contributions to a crash. Currently, this data can illustrate

vehicle status, such as velocity, safety restraint use and seat occupancy, and driving inputs associated to its accelerator pedal, brake pedal, and steering. As software systems begin to increasingly perform some of those functions, there is a correlating increase in the potential for a vehicle-based system to have contributed to an action or crash. There will be an investigative need to determine what processes, and vehicle or software-originated inputs were being applied by software systems. In the case of a failure, it then becomes necessary to identify the source of that software-based process, including the determination if the software system is original and unaltered from the manufacturer's design, or if it has been deliberately or unknowingly altered by after-market software modification.

These determinations are necessary not only for purpose of liability and culpability, but also for the improvement of safety. The improvement of software systems depends greatly upon identification of failures when they occur and will require proper attribution to the software and systems involved. In addition to the benefits of data logs referenced in Standard T.12, modern vehicles utilizing combined ADAS, ADS, or even teleoperation systems create a need to preemptively address forensic data-retrieval needs. This includes potential considerations for what data shall be recorded and available, what retrieval methods are necessary, and what assurances are needed to ensure that the data retrieved can be readily interpreted for use. Preventative measures towards reducing crashes and improving safety are most effectively made after causational factors can be determined and evaluated. As modern vehicles increase the capacity at which their systems provide driving assistance or even perform driving actions in place of a driver, the burden of post-incident investigation and safety evaluation shifts increasingly towards the software systems of involved vehicles.

(4) Serviceability:
The CHP concurs with the guidance provided by NHTSA as it relates to vehicle serviceability and cybersecurity.

(5) Technical Vehicle Cybersecurity Best Practices:
In the event a cybersecurity incident has occurred, manufacturers should consider logging connection data, and any activities performed by network or physically connected devices. This data should also include any unique identifiers, such as International Mobile Equipment Identifiers (IMEI), Internet Protocol (IP) addresses, Media Access Control (MAC) addresses, serial numbers, etc. In the event the incident is determined to be a crime, manufacturers should consider providing a pathway to allow for investigative steps in the gathering and subsequent processing of data (including proprietary data).

Thank you again for the opportunity to provide comments on this topic. The CHP is committed to addressing public safety during the testing and subsequent deployment of ADS-equipped vehicles and looks forward to future opportunities to work with our traffic safety partners and stakeholders.