

Automotive Vehicle Cybersecurity Assessment Criteria

Problem Statement

Department of Homeland Security (DHS) components require an effective and validated solution for diagnosing and mitigating cybersecurity vulnerabilities in automotive vehicles used for law enforcement operations and other mission activities requiring enhanced cybersecurity. These vehicles may be DHS-owned and maintained, leased, or the property of another federal, state, local, tribal, or territorial (FSLTT) law enforcement or civilian agency. A comprehensive vehicle solution will include existing or developed, state-of-the-art technologies and processes allowing DHS law enforcement personnel to assure the cybersecurity of its automotive vehicle fleet, protect against cyber-physical attacks, and mitigate the risk of exposing sensitive data.

Capability Requirements

The solution will be used in the field to ensure operational integrity of vehicles and must be able to:

- Scan and validate ECUs.
 - Baseline the firmware of the ECUs in use on the vehicle.
 - Immediately identify a vehicle's ECU firmware is faulty before the vehicle is used.
- Scan and eliminate rogue devices CAN buses.
 - Immediately identify devices on the CAN bus that were not intended to be there by the manufacturer that could inject unwanted traffic on the vehicle's bus.
- Detect anomalies in the CAN bus traffic.
- Shut off all non-secure remote access pathways into vehicle (reduce the attack surface) to include cellular, telematics, radios, Wi-Fi and Bluetooth connectivity.
- Shield against directed RF energy attacks.
- Delete sensitive information from vehicle systems that stored them after operators paired phones or other devices with the vehicle.
- Log data for future forensics analysis.
- Restore non-DHS owned vehicles to the owner's initial configuration after the completion of operation.

Salient Characteristics and Performance Attributes

- Executable on a wide variety of makes of vehicles to include, but not limited to, General Motors, Dodge, Ford, BMW, Mercedes, and Audi.
- Executable in the field using equipment portable by 1-2 persons and transportable by commercial air cargo holds.
- Executable within an hour for temporary/non-permanent solutions and within five hours for permanent installation.