Comment from Rik Farrow

There is much to like about this update to cybersecurity best practices, and I applaud most of what I read in the summary of this document.

I have two concerns, though. First, these are merely best practices, and failure to properly test vehicle software for correctness and robustness while under attack could easily lead to injuries and deaths. I'd rather have read that some level of due diligence is required, just as the Requests for Comments (RFCs) used to regulate the proper working of the Internet have been shown to work. Requirements also mean that a vendor not meeting requirements cannot argue that the regulation only provides suggestions for best practices.

My second concern is that vehicle cybersecurity should not unduly restrict access by alternative third-party repair services authorized by the vehicle owner. I've read about the plight of farmers who cannot diagnose and perform simple repairs on their modern farm machinery. Simply replacing a sensor, as indicated by a diagnostic, can be done without the intervention of the vehicle dealer, for example. But if access to diagnostics is limited to a small set of dealers, then the dealers have a monopoly that harms their customers, especially those living in rural areas.

[G.40] Any connection to a third-party device should be authenticated and provided with appropriate limited access.

This statement could be clearer if it defined "appropriate limited access". It is one thing to have access to system diagnoses, and quite another to be able to change the state of the system, for example, by rewriting firmware. The ability to replace a sensor discovered to be faulty doesn't need to involve changing the state of the system, other than having the system "notice" that the sensor had been replaced or repaired, in the case of a bad electrical connection.

Vehicle vendors are preparing to build electric vehicles, ones that generally need much less maintenance that ICE. Allowing vendors to limit access to diagnostic systems is a way to limit the repairability of new vehicles, and I suggest you consider wording that allows the use of diagnostics, as opposed to allowing unauthenticated or authorized changes to system software and settings. Computer systems have been designed to allow diagnostics, but not alteration, by unauthorized users since about 1970. It shouldn't be too much to expect from vehicle vendors.