Comment from Norman Field

It might be worthwhile creating a single point-of-secure-entry to a vehicle that would implement specific standard, which can be used by all components and aftermarket devices.

For example, just as the UNIX/Linux systems have the internet daemon (inetd) that was designed to allow anyone to create a service for a computer and "advertise" the ports that were available for communication over remote procedure calls (see rpcinfo), the NHTSA could create an industry standard, lock it down with the kind of security we have in the Tellaro, and then allow vehicle and aftermarket product/service manufacturers to build on that standard communications/security interface.

This could take a couple of years to define, but once defined, the industry could come up with products that implement the standard and pitch it to vehicle manufacturers. Once standardized, anyone can then build products/services that could work globally on all cars. Securely.

Comment on [G.40].
I believe it is worth including a specific recommendation against using passwords, symmetric keys or any other form of shared secret for authentication. Vehicle manufacturers should only rely on public key cryptography or other technologies with similar security properties.

Comment on section 6.2.
Aftermarket devices specifically designed to interface with vehicles should have the capability to assert their manufacturing origin to the vehicle, so that the vehicle can evaluate the trustworthiness of the device.

Comment on section 8.1
If it is necessary to warn manufacturers that hiding connectors is not proper security, then perhaps recommending some options that can be used to control access is warranted.

Comment on section 8.2
I believe it is worth including a specific recommendation against using passwords, symmetric keys or any other form of shared secret for authentication. Vehicle manufacturers should only rely on public key cryptography or other technologies with similar security properties.

Comment on section 8.3
Enabling diagnostics and access to diagnostic interfaces should be appropriately protected to limit access to authorized privileged users.