1. Please explain whether the requested exemption would or could impact non-software copyrighted content that is offered through vehicle telemetry and/or entertainment systems. Could an exemption be crafted that would preserve protection of such content?

There isn't any risk in pirating content or OSes from automotive components. These components are so specific to the vehicle that you could not copy them to any other vehicle other than what they were intended to be used for. Firmware is specifically compiled to match the chips they run on and unless the boards are laid out the exact same way, it would be impossible to successfully copy software from one telematics unit to another.

2. Please explain whether and/or how the purchaser of a used vehicle would be able to identify and assess modifications to vehicle software by the previous owner. What would be the process, as well as the cost and burden, of identifying such changes? What type of equipment would be necessary?

There are several companies that are working towards similar goals for general Internet of Thing devices. One method of doing this is for the OEMs or Tier 1 suppliers to release a series of checksums ("hashes") that reflect a "known good" state.

Computing this hash requires copying the software from the device and computing a checksum, then comparing that against "known good" checksums from the OEM. This will not require expensive specialized equipment or processing power.

If the systems are open then anyone can simply verify those checksums. If the OEMs lock down systems so a consumer cannot look into them then these exemptions are required in order to get into the system and for some 3rd party company or consumer to make this list of checksums. It is possible that malicious parties could be bypass TPMs and install software that harms the purchaser — by modifying the odometer, for example. Granting this exemption would provide a legal path for vehicle purchasers to verify the software prior to purchase.

Most manufacturers already have these firmware checksums but currently they do not publish them. Known-good checksums could be crowdsourced in lieu of manufacturer's publication.

3. The Office is interested in additional information concerning the costs and availability of manufacturing information and data to create diagnostic techniques and tools for the automobile "aftermarket," as well as the costs and availability of such information for persons who seek to create tools for individual use.

The diagnostics in question are purely informational. These are the CAN packet descriptions (typically stored in DBC files, see http://vector.com/vi_candb_en.html) and proprietary diagnostic codes (codes they are not explicitly forced to tell you about) that work over Unified Diagnostic Services (UDS). For the first one there are usually just a few files per car and every car needs them to be manufactured. Over time these files are only given out to partners and typically for the cost of $25,000-$50,000 per make/model and year of vehicle. Most mechanics work on many models of vehicles, so this cost is prohibitive to local mechanics. Even wealthy hobbyists can't afford these if they want to work on more than one car.

The tool manufacturers that have an agreement with the OEMs and purchase these files will strip out a lot of the information and wrap it into their own tool with their own limited functionality and typically sell each tool for $2,000-10,000. While it is possible to get cheaper diagnostics such as a $20 3 day subscriptions to where wires are in your vehicle or a $200 tool that does basic non-proprietary diagnostics, these are not useful for advanced diagnostics and modifications. These DBC files are created during the vehicle design, so granting access to them would not incur additional cost to create.

There are also undocumented features that can be find while reversing the firmware. Information on these features are not available through purchase of the DBC files but can be triggered by manufacturer specific tools. Having the full knowledge on how a vehicle works can improve 3rd party tools for modifications and repairs.

Restricting access to network details and relying on TPMs are integral parts of the process to design an artificial system to lock in repairs only to themselves and to close partners. The contents of these DBC files can be reverse engineered, but most people fear sharing this information in public will incur the wrath of large companies, who may cut them off further from the information that they need to perform repairs.