**U.S. Department of Transportation**
Office of the Secretary of Transportation

**GENERAL COUNSEL**

1200 New Jersey Avenue, SE
Washington, DC 20590

September 9, 2015

Jacqueline C. Charlesworth
General Counsel and Associate Register of Copyrights
United States Copyright Office, Library of Congress
101 Independence Ave., S.E.
Washington, D.C. 20559-6000

Re: Section 1201 Rulemaking (Docket No. 2014-07)
Proposed Exemptions of Vehicle Software
U.S. Department of Transportation Views

Dear Ms. Charlesworth:

Thank you for your May 12, 2015 letter notifying me about the rulemaking that the U.S. Copyright Office is conducting under the Digital Millennium Copyright Act ("DMCA") and inviting the Department to submit views.

The DMCA prohibits persons from circumventing "technological protection measures" ("TPMs") that restrict access to copyrighted works. 17 U.S.C. § 1201(a). It also authorizes the Librarian of Congress, upon recommendation by the Register of Copyrights and in consultation with the Assistant Secretary for Communications and Information of the Department of Commerce, to exempt certain TPMs from this "anti-circumvention" provision in order to allow uses of the protected works that would not otherwise constitute copyright infringement. 17 U.S.C. § 1201(c). In this year's rulemaking, the latest in a series of triennial rulemakings your office conducts under section 1201(c)(1), you are considering whether there are any classes of copyrighted works for which noninfringing uses are, or in the next three years are likely to be, adversely affected by the prohibition on circumvention of TPMs that control access to copyrighted works. 79 Fed. Reg. 73856-72, Notice of proposed rulemaking (Dec. 12, 2014).

The notice of proposed rulemaking would exempt TPMs that control access to motor vehicle software for several different classes of purposes. Two of those classes are of particular interest and concern to the Department of Transportation.

Proposed Class 21

> would allow circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicle, including personal automobiles, commercial motor vehicles, and agricultural machinery, for purposes of lawful diagnosis and repair, or aftermarket personalization, modification, or other improvement.

> would allow circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicle for the purpose of researching the security or safety of such vehicles.

Exemption proponents state that the proposed exemptions would allow vehicle owners to "personalize, improve or repair" and to "tinker with" their vehicles, and researchers to discover programming errors that pose safety risks or make a vehicle vulnerable to remote hackers. Under each of these proposed exemptions, "circumvention would be allowed when undertaken by or on behalf of the lawful owner of the vehicle."

The Department understands that the DMCA and its exemption process are focused on issues relating to copyright and the "fair use" of copyright materials. Nevertheless, given this Department's statutory safety responsibilities, and given the increasing importance of the continued integrity of motor vehicle software to driving safety, we would be remiss if we did not note for the record that modifying motor vehicle software can create safety and cybersecurity risks. Modification creating these risks is contrary to the purposes of the National Traffic and Motor Vehicle Safety Act ("VSA"). Increasingly, vehicle software is being written to enable vehicle systems to detect and avoid safety risks in carefully defined circumstances. Allowing modification of such software (including its impact on other vehicle systems that may or may not be easily ascertained by the person performing the modification) in a vehicle could create significant safety risks not only to the occupants of that vehicle, but also to the occupants of other vehicles as well as to pedestrians and cyclists.

While the VSA contains a prohibition against tampering, that provision, which was enacted nearly 50 years ago, has significant limitations that prevent it from fully addressing modern risks, including the possibility of remote malicious hacking. First, the provision prohibits tampering with only those items of vehicle software and other vehicle systems, parts and components that are regulated by Federal Motor Vehicle Safety Standards ("FMVSS") issued by the Department's National Highway Traffic Safety Administration. Many of the safety critical functions and how they interact with other vehicle functions in today's motor vehicles may not be directly regulated by FMVSSs. Thus, tampering with the software that controls those functions would not violate the VSA anti-tampering provision. Second, the VSA prohibition narrowly applies to motor vehicle manufacturers, distributors, dealers and repair businesses, but not to other persons.

With respect to an exemption for circumvention of TPMs in software embedded in vehicles, for the purposes of research regarding security or safety of such vehicles, this Department has concerns over the timing and nature of the potential public disclosure of such research. The Department recognizes that enabling publication of good faith research efforts in this area presents the potential benefit of promoting collaboration in identifying security vulnerabilities or other problems. However, the Department is concerned that there may be circumstances in which security researchers may not fully appreciate the potential safety ramifications of their security circumvention acts and may not fully understand the logistical and practical limitations

associated with potential remedial actions that may become necessary. The Department's concerns potentially could be addressed with appropriate limitations on disclosures of such TPM circumvention and of the manner in which they were accomplished (*e.g.,* limiting disclosure of circumvention and its potential effects to regulators or potentially affected parties) or with the provision of adequate time for responsive actions to be formulated and executed before broader disclosures are made.

We appreciate the opportunity to share these concerns with you.

Sincerely,

Kathryn B. Thomson (KLA)

Kathryn B. Thomson
General Counsel