Before the
U.S. Copyright Office
Library of Congress
Washington, DC

In the Matter of

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies	**)** **)** **)** **)**	**Docket No. 2014-07**

Short Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201

Item 1. Commenter Information

This comment is submitted on behalf of the SAE Vehicle Electrical System Security (VESS) Committee, and any questions can be addressed to:
William Gouse, Director, Federal Program Development, SAE International, 202-434-8944, wgouse@sae.org

Item 2. Proposed Class Addressed

Proposed Class 22 – Vehicle Software – security and safety research

Item 3. Statement Regarding Proposed Exemption

As publicly discussed during several SAE VESS Committee meetings, we recommend that The Librarian keep the following five technical points in mind while considering an exemption under the Proposed Class 22 for vehicle software:

1. The TPMs in question serve not only to protect copyright interests but also are an integral part of the overall security strategy that protects safety-critical vehicle software, operations, etc. against modification by those with malicious intent. For example, code signing software, secure boot loaders, software that performs access control, watchdog timer software, and supervisory control systems would be affected by the following disclosures described below and have an overall impact on vehicle security. Cryptographic keys and random number generation algorithms used for symmetric and asymmetric encryption techniques may be vulnerable to this class of exemption, causing irreparable damage to systems protected by such TPMs.
2. The code that governs the systems responsible for vehicle operation is highly complex and inter-related. Modification for the purpose of safety/security research on one system may have unintended results on other closely interdependent vehicle systems.
3. Irresponsible disclosure of discovered vulnerabilities in vehicle hardware/software may lead to malicious entities utilizing such vulnerabilities to mount zero-day attacks on vehicle systems/back-end infrastructure. There is nothing in the proposed exemptions that requires researchers to disclose their findings responsibly.
4. It is a common practice in the automotive industry to proactively identify such researchers/ organizations and conduct joint safety/security research under Non-Disclosure Agreements/Responsible disclosure agreements.

5. It is our understanding that in addition to having public discussions during SAE meetings, the automotive industry and its partners are developing the framework necessary to establish an 'Auto-ISAC' in the very near future. It is anticipated that this forum will enable confidential dialog regarding vehicle security and safety research issues.

The SAE VESS Committee stands ready to assist the Copyright Office in providing and sharing its technical expertise with respect to any future issue discussed within Proposed Class 22.