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

[ ] Check here if multimedia evidence is being provided in connection with this comment

Item 1. Commenter Information

This Comment is submitted on behalf of BSA | The Software Alliance ("BSA"), the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, D.C., and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

Item 2. Proposed Class Addressed

Proposed class 25: Software—Security Research.

The December 12, 2014 Notice of Proposed Rulemaking ("NPRM") described this proposed class as permitting "researchers to circumvent access controls in relation to computer programs, databases, and devices for purposes of good-faith testing, identifying, disclosing, and fixing of malfunctions, security flaws, or vulnerabilities." 79 Fed. Reg. 73,856, 73,870 (Dec. 12, 2014). "Petitioners seek to circumvent TPMs in medical devices, car components, supervisory control and data acquisition ("SCADA") systems; and other critical infrastructure, such as the computer code that controls nuclear power plants, smart grids, and industrial control systems; smartphones that operate critical applications, such as pacemaker applications; internet-enabled consumer goods in the home; and transit systems." *Id.* at 73,870-71.

The actual class of works proposed by Professor Steven M. Bellovin, et al. ("Security Researchers"), would be defined as follows:

> "Literary works, including computer programs and databases, protected by access control mechanisms that potentially expose the public to risk of harm due to malfunction, security flaws or vulnerabilities when[:]
>
> (a) circumvention is accomplished for the purpose of good faith testing for, investigating, or correcting such malfunction, security flaws or vulnerabilities in a technological protection measure or the underlying work it protects; OR
>
> (b) circumvention was part of the testing or investigation into a malfunction, security flaw or vulnerability that resulted in the public dissemination of security research when (1) a copyright holder fails to comply with the standards set forth in ISO 29147 and 30111; or (2) the finder of the malfunction, security flaw or

> vulnerability reports the malfunction, security flaw or vulnerability to the copyright holder … in advance of or concurrently with public dissemination of the security research."

Security Researchers Class 25 Comment at 1.

The actual class of works as described by Professor Matthew D. Green would be as follows:

> "Literary works, including computer programs, databases, and documentation, protected by technological protection measures that control access to the work, for the purpose of finding, fixing, and disclosing security vulnerabilities, flaws, or malfunctions, commenting on or criticizing such vulnerabilities, flaws, or malfunctions, or engaging in scholarship and teaching about such vulnerabilities, flaws, or malfunctions, including where the technological protection measures control access to other works, such as graphic works, audiovisual works, and sound recordings, when the research cannot be performed without accessing the other works."

Green Class 25 Comment at 3.

Item 3. Overview

Although Class 25 is characterized by its proponents as an exemption to enable "good faith security testing," the proposal would in fact authorize the public disclosure of security vulnerabilities in ways that would expose the public to heightened security risks. By permitting the public disclosure of security vulnerabilities "concurrent[]" to their disclosure to the copyright owner, Class 25 lacks important safeguards. To be clear, BSA is not opposed to good faith security testing or to the coordinated disclosure of such research. However, prior to publicly disclosing the existence of a security vulnerability that is capable of being exploited by third-party hackers, the principle of coordinated vulnerability disclosure necessitates that researchers first inform and provide the relevant software publisher ample time to remediate the vulnerability.

This proposed class of works is unmoored from virtually all of the reasonable constraints Congress placed on good faith security research in 17 U.S.C. § 1201(j). First, the proposed exemption is not expressly limited to acts that do not constitute copyright infringement. Second, the proposed exemption is not expressly limited to lawful acts and does not reference closely related laws, such as the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Third, the proposed exemption does not require a researcher to have authorization from the owner of a computer, computer system or network prior to gaining access. Fourth, the proposed exemption would apply irrespective of (i) whether the information derived from the security testing was used "solely to promote the security" of the owner and/or developer of a program, computer, computer system or network; and (ii) whether "the information derived from the security testing was used or maintained in a manner that does not facilitate infringement…or a violation of applicable law…including a violation of privacy or breach of security." 17 U.S.C. § 1201(j)(3)(A)&(B).

Not only does the proposed class of works disregard the directives that Congress made in section 1201(j), it further aggravates the risks associated with security vulnerabilities by countenancing the public disclosure of information regarding vulnerabilities before the owner or developer of a program, computer, computer system or network has had an opportunity to take remedial steps to correct a problem. Given that the proponents seek to circumvent access controls on software that is, for example, crucial to running indispensable programs – such as those associated with the operation of nuclear power plants, medical devices, and automobiles – an exemption that lacks proper safeguards could be disastrous.

Although the Register and the Librarian have at times granted exemptions that closely relate to activities that are already addressed by existing statutory exceptions to section 1201's anti-circumvention prohibitions (*e.g.*, Recommendation of the Register of Copyrights, Section 1201 Rulemaking: Fifth Triennial Proceeding, 71 (Oct. 12, 2012) ("2012 Recommendation")), previous exemptions related to security testing have incorporated aspects of section 1201(j) to preserve the spirit of Congress' efforts to avoid exacerbating risks rather than reducing them. *See, e.g.,* Final Rule, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 75 Fed. Reg. 43,825, 43,839, July 27, 2010. The Copyright Office should not waver from this approach now.

In contrast with the targeted security testing exemptions previously recognized by the Register and the Librarian, the proposed classes of works relate not to vulnerabilities that are demonstrably *caused by access controls*, but instead to all software products that might contain vulnerabilities and that happen to be protected by access controls. Given the breadth of the proposed class of works, it is essential that the Copyright Office take measured steps to determine whether an exemption of any sort is necessary for security testing.

Item 4. Technological Protection Measure(s) and Method(s) of Circumvention

Given that the proposals do not focus on existing, specific access controls that create security vulnerabilities, but are rather seeking to enable circumvention to test all sorts of software-related security vulnerabilities, these proposals are much broader than exemptions that the Register and the Librarian have previously recognized.[1] For example, in 2006 and 2011, the Copyright Office endorsed exemptions related to circumventing specific access controls due to threats caused by those TPMs. *See* Recommendation of the Register of Copyrights in RM 2005-11; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 2 (Nov. 17, 2006); Recommendation of the Register of Copyrights in RM 2008-8; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 184 (June 11, 2010), 184 ("The goal of the research is to yield rigorous and accurate criticism or comment *about the technological measure attached to a work*."); (emphasis added).

While the Security Researchers continue to rely on events from nearly a decade ago that gave rise to previous exemptions endorsed by the Copyright Office, these types of incidents are no longer the focus of what is being requested. As such, very close attention to the potential adverse consequences of granting an exemption is required, especially considering that the proponents seek to circumvent access controls on software that is, for example, crucial to running indispensable programs associated with potentially hazardous materials, such as those involved with the operation of nuclear power plants. The exemption would also allow circumvention of access controls on other devices that could result in harm to people or property, such as medical devices, and automobiles.

The proponents certainly have not established that the Copyright Office should endorse the ISO standards (29147 and 30111) that the Security Researchers would have the Office require software developers to comply with or risk having their products exposed to circumvention. *See* Security Researchers Class 25 Comment at 1. First, the proponents have

[1] It is clear from a review of the proponents' comments that they seek an exemption that allows circumvention related to researching all software products that might contain vulnerabilities and that happen to be protected by access controls, even if the access controls are not to blame for the vulnerabilities. *See, e.g.*, Security Researchers Class 25 Comment at 2 (describing a project related to voting machines that "discovered numerous serious exploitable vulnerabilities in almost every component of every vendor's system that was examined"); Green Class 25 Comment at 12 (expressing a desire to circumvent to study whether "[f]laws in the software powering [video recorders, game consoles, and other home appliances] may result in serious security problems such as permitting a malicious user to eavesdrop on a home surveillance system and view what the system has recorded").

not even articulated for the record precisely what these standards require. Second, they fail to acknowledge that there would be no way for an independent researcher to know whether a company was compliant with these standards.[2] Third, the Copyright Office is not, and should not try to become, the arbiter of what a responsible software company's policies and practices should be. The endorsement of specific security-related standards is far afield from the Copyright Office's mission and expertise and this proceeding is not designed for a full debate on such topics.

Item 5. Asserted Noninfringing Use(s)

The proponents seek to engage in such a wide variety of activities that it is impossible to assess whether all of these activities qualify as non-infringing. This is especially problematic because the proposed exemption is not expressly limited to acts that do not constitute infringement.

Item 6. Asserted Adverse Effects

The proponents of the exemption have put very little in the record to demonstrate that researchers are currently declining to engage in good faith security testing as a result of the prohibition against circumvention of access controls contained in 17 U.S.C. § 1201(a)(1).[3] In reality, a significant amount of independent security research is conducted every day with little to no interference from the Digital Millennium Copyright Act ("DMCA")'s anti-circumvention prohibitions. Indeed, many of the member companies represented by BSA actively encourage independent research and actively participate in an ecosystem that includes academics, companies, and non-profit institutions who seek to preserve and protect the integrity of computers and systems that run all varieties of software. Almost all software companies already have in place carefully tailored processes for identifying vulnerabilities and working with independent researchers and members of the public to address them.[4]

It appears, however, that the proponents of the exemption seek permission to exceed the bounds of what Congress previously endorsed as good faith security research. See, e.g., Green Class 25 Comment at 21-22. When it passed the DMCA, Congress instructed as follows:

> [T]he scope of permissible security testing under the Act should be the same as permissible testing of a simple door lock: a prospective buyer may test the lock at the store with the store's consent, or may purchase the lock and test it at home in any manner that he or she sees fit – for example, by installing the lock on the front door and seeing if it can be picked. *What that person may not do , however, is test the lock once it has been installed on someone else's door, without the consent of the person whose property is protected by the lock*.

[2] A exemption that authorized circumvention of software developed by a copyright owner so long as that copyright owner was not complying with the standards would be unworkable because independent researchers would have no way of verifying whether a developer was in compliance with the standards absent access to the developer's internal practices. This is especially true of ISO 30111, which outlines *internal* policy requirements that need not be made public.

[3] Although Professor Green cites some examples of legal threats made against security researchers, these cases are more than a decade old. Green Class 25 Comment at 18-19. While the Security Researchers do state that they have "altered both the subject matter and the methodology of [their] intended research in cases where they were advised by counsel of DMCA section 1201 risks," and provide some specific examples of these alterations, they do not explain why these projects in particular involved substantial risks under Section 1201. Security Researchers Class 25 Comment at 6, 9-10.

[4] Almost all software companies already have in place carefully tailored processes for identifying vulnerabilities and working with independent researchers and members of the public to address them. *See, e.g.*, Coordinated Vulnerability Disclosure, Microsoft, https://technet.microsoft.com/en-us/security/dn467923.aspx.

Conference Report at 67 (emphasis added). Here, proponents seek an exemption that would not only permit them to test security measures "without the consent of the person whose property is protected by the lock," but also to publicly disclose the results of such efforts in a manner that would enable others to breach those security measures. BSA submits that the inability to engage in unlawful or irresponsible methods of security research that exacerbate the threats posed by security vulnerabilities is not a substantial adverse impact caused by access controls under the statute.

Accordingly, any exemption granted must impose at least the following limitations:

- The conduct at issue must not constitute copyright infringement;
- The conduct at issue must be lawful, including under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
- The researcher must have authorization from the owner of a computer, computer system or network prior to gaining access thereto;
- The information derived from the security testing must be used "solely to promote the security" of the owner and/or developer of a program, computer, computer system or network; and
- The information derived from the security testing must be used and maintained in a manner that does not facilitate infringement or any other violation of applicable law, including a violation of privacy or breach of security.

Item 7. Statutory Factors

The most important Section 1201(a)(1)(C) factor to consider in relation to the proposed classes of works is the third factor: "the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research." As discussed above in Item 6, the proponents have put very little in the record by the way of specifics to support their claims that legitimate security research, commentary or educational activity is being chilled by Section 1201. However, even assuming *arguendo* that we can credit their assertions that their conduct is being impacted by the DMCA, they have not justified any exemption by which the Copyright Office would encourage hasty, public disclosures of the results of security research. The best solution to fixing a security vulnerability is to go directly to the software developer to reveal the identified flaws and provide that developer with the information needed to correct the vulnerability.

Accordingly, BSA opposes the incorporation into any exemption of the language put forward by the Security Researchers suggesting that a copyright owner need not be notified of a security vulnerability until the general public is also notified. Endorsing that approach in all instances could result in unnecessary escalation of risks that could otherwise be limited or eliminated before malicious actors discover them.