This is a Word document that allows users to type into the spaces below. The comment may be single-spaced, but should be in at least 12-point type. The italicized instructions on this template may be deleted.

UNITED STATES COPYRIGHT OFFICE

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

ITEM A. COMMENTER INFORMATION

Christian Troncoso (christiant@bsa.org) on behalf of BSA | The Software Alliance ("BSA") (www.bsa.org).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 10: Computer Programs – Security Research

ITEM C. OVERVIEW

As businesses that rely on consumer trust, BSA members understand the importance of ensuring the security of their products and services. At every stage of the software development life cycle, from design to deployment, BSA members invest substantial resources into securing their products. In addition to maintaining their own security teams, BSA members also actively cooperate with the security research community to identify potential vulnerabilities and prevent their exploitation.

BSA members agree that the DMCA should not impede legitimate, good-faith security research. Recognizing the importance of such research to the security of the software system ecosystem, BSA supported renewal of the Class 25 exemption granted by the Librarian of Congress during the 2015 DMCA rulemaking cycle. The 2015 Exemption reflects a careful balance that accommodates the needs of the independent security research community, the property interests of copyright owners, Congressional intent about the scope of "good-faith security research" reflected in § 1201(j), and the significant public safety risks that could be implicated by an overly-broad exemption. To balance these interests, the 2015 Exemption included a number of critical safeguards:

1. **"Good-faith Security Research" Limitation:** The exemption is limited to "accessing a computer program solely for purposes of good faith testing, investigation and/or

correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement."

2. **"Device" Limitation:** The exemption is limited to research involving: (1) a device or machine primarily designed for use by individual consumers (including voting machines), (2) a motorized land vehicle, and (3) a medical device designed for whole or partial implantation in patients or a corresponding monitoring system, that is not and will not be used by patients or for patient care.
3. **"Other Laws" Limitation:** The exemption is limited to circumvention undertaken on a "lawfully acquired device or machine" for purposes of research that "does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act."

The petitions submitted by Professors Ed Felten and J. Alex Halderman, the Center for Democracy and Technology, and Professor Matthew Green (collectively, "Petitioners") seek to eliminate *all* of these critical safeguards. In support of their request, Petitioners argue that the safeguards adversely affect their ability to engage in certain forms of non-infringing security research. However, the adverse effects cited by Petitioners largely stem from: (1) unfairly restrictive interpretations of the 2015 Exemption, (2) limitations that are necessitated by Congressional intent and the DMCA's limited grant of authority to the Librarian of Congress under § 1201(a)(1), and/or (3) safeguards that are justified by significant public safety concerns. Accordingly, BSA respectfully opposes Petitioners' request.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

[Intentionally left blank]

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

1. Good-faith Security Research Limitations

Petitioners raise a number of arguments with respect to the definition of "good-faith security research." Petitioners do not offer an alternative definition. However, taken together, Petitioners' arguments amount to a request for the Copyright Office to define the term as follows:

> "Good-faith security research" means accessing a computer program ~~solely~~ for purposes of good faith testing, investigation and/or correction of a security flaw or vulnerability, ~~where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.~~

For the specific reasons outlined below, the Copyright Office should reject this invitation.

1. Access Limitation

The Access Limitation provides that circumvention must be performed "solely for purposes good-faith testing, investigation and/or correction of a security flaw." Petitioners argue that the Access Limitation prevents them from "circumventing TPMs in furtherance of scientific dialogue, academic peer review, and classroom teaching" thereby "unconstitutionally limiting post-circumvention First-Amendment-protected speech."[1] Petitioners similarly argue that the Access Limitation creates ambiguity about "whether activities that use the results of the noninfringing testing and investigation – for example, publishing papers – are covered" by the exemption.[2]

A fair reading of the Access Limitation does not support Petitioners' claims. The Access Limitation merely limits initial eligibility for the exemption to beneficiaries who are performing acts of circumvention "solely for the purpose of good-faith testing, investigation and/or correction of a security flaw or vulnerability." It does not, however, have any impact on post-circumvention activity. Provided an initial act of circumvention is performed "solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability," a beneficiary is free to use insights gleaned from the research for "scientific dialogue, academic peer review, and classroom teaching." Indeed, in recommending that the Librarian of Congress grant the 2015 Exemption, the Register of Copyrights expressly acknowledged that it would enable research activity "aimed in part at advancing the state of knowledge in the field."[3]

b. Use Limitation

The Use Limitation requires beneficiaries of the 2015 Exemption to ensure that "information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer operates, or those who use such devices or machines, and is not used or maintained in a manner that facilities copyright infringement." Petitioners characterize the Use Limitation as ambiguous, suggesting that courts "might interpret 'primarily' to mean 'only' – such that if a research is found to have used the information for anything that is beyond the given uses, they have violated this term."[4] They assert that requiring beneficiaries to use information derived from good-faith security research "primarily to promote the security or safety" of the devices or device-users could potentially prevent them from issuing public safety warnings.[5] Finally, Petitioners argue that the Use Limitation impermissibly conditions eligibility for the exemption on the "future behavior of a third party with whom a researcher may have no direct relationship."[6]

[1] Felten petition at 24-25.
[2] *Id.*
[3] 2015 Recommendation at pg. 309
[4] Felten petition at 25
[5] Felten at pg. 25
[6] Felten at pg. 26

Here, too, Petitioners arguments largely derive from an unlikely reading of the 2015 Exemption. We disagree with the fundamental premise of Petitioners' argument, namely, that "primarily" might be interpreted to mean "only." Setting aside the threshold issue of interpretation, the Register of Copyrights concluded that the Use Limitation was needed in order to align the 2015 Exemption with Congress's clear intention that security research exceptions "primarily promote the security of the types of devices containing the computer programs on which the research is conducted, or those who use those devices."[7]

Importantly, the Register also recommended the Use Limitation to avoid any "definitive disclosure requirements [that] might implicate First Amendment concerns" while at the same time ensuring that "[b]ad-faith activities…fall outside of the exemption."[8] In this respect, the Use Limitation is a means of limiting the exemption to "good-faith research" without promulgating prescriptive requirements (or exclusions) that would otherwise be necessary to adhere to Congress's intent and prevent the public safety risks that could arise from bad-faith actors. While Petitioners now criticize the ambiguity of the Use Requirement, proponents of the 2015 Exemption cautioned against a more prescriptive approach:

> An overly complex or rigid disclosure requirement would undermine the very purpose of the proposed security research exemption. . . .Good-faith security researchers, including several proponents of the proposed exemption, have a strong record of practicing responsible disclosure techniques appropriate to the situation at hand. Numerous published guidelines offer best practices for disclosing security vulnerabilities in a variety of situations. These evolving guidelines accommodate the complexity involved in making disclosure decisions and are based on the combined experience of researchers and vendors dealing with a number of unique circumstances. However, those guidelines are too varied and complex to capture effectively in a qualification to the proposed exemption.[9]

The Use Limitation thus plays a critical role in ensuring that the exemption: (1) adheres to congressional intent, (2) prevents bad actors from benefiting from the exemption, and (3) avoids over-prescriptiveness that would ultimately undermine its value to security researchers.

c. Controlled Environment Limitation

The Controlled Environment Limitation requires circumvention to be "carried out in a controlled environment designed to avoid any harm to individuals or the public." Petitioners argue that the Controlled Environment Limitation is ambiguous and suggest that it has a chilling effect on any research not performed "within the confines of a lab."[10] At the same time, Petitioners caution the Copyright Office against providing additional guidance about the contours of the limitation,

[7] 2015 Recommendation at pg. 319. The requirement for beneficiaries to ensure that security research information "is not used or maintained in a manner that facilitates copyright infringement" is likewise derived from congressional intent, as expressed in section 1201(j).
[8] Id.
[9] Center for Democracy & Technology and New America's Open Technology Institute, Class 25 Post-Hearing Letter at 2-3.
[10] Felten petition at pg. 22.

noting that it is "not the appropriate body to improve the quality, uphold the standards, or provide certification in information security research."[11]

Petitioners' claim that the Controlled Environment Limitation restricts good-faith security research to a lab setting is belied by the record of the 2015 Exemption and by the nature of the research they seek to engage in. The purpose of the Controlled Environment Limitation is to mitigate the risks to the public that can arise when security research is performed haphazardly.[12] For purposes of the 2015 Exemption, "controlled environment" should be understood as encompassing testing environments where "harm to individuals or the public" can be mitigated. Petitioners note that the type of field research they seek to engaging in "does not include research that would risk human injury or harm," because they "follow strict norms and customs that protect against such harms."[13] Such research should not be chilled by a fair reading of the Controlled Environment Limitation. Indeed, much as the Use Limitation deftly avoids over-prescriptiveness, the Controlled Environment Limitation provides good-faith security researchers with sufficient flexibility to rely on well-established norms and customs to mitigate third party risks in a manner that accounts for the unique factual considerations at hand.

2. Device Limitation

Pursuant to the Device Limitation, the 2015 Exemption applies only to good-faith security research performed on: (1) devices and machines "primarily designed for use by individual consumers (including voting machines)," (2) motorized land vehicles, and (3) medical devices designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care. Petitioners take aim chiefly at the limitation to devices "primarily designed for use by individual consumers," which they characterize as ambiguous. Petitioners request that the Copyright Office eliminate the Device Limitation to facilitate research of "nuclear power plants, smart grids, industrial enterprises, air traffic control functions, train systems, or traffic lights," which would otherwise be chilled.[14]

Removal of the Device Limitation would render the 2015 Exemption impermissibly broad. Indeed, the Register explained that it was statutorily compelled to include the Device Limitation because "an open-ended exemption…encompassing all computer programs on all systems and devices, including highly sensitive systems such as nuclear power plants and air traffic control systems" would be inconsistent with the DMCA's requirement that exemptions relate to a "narrow and focused subset of the broad categories of works…identified in section 102 of the Copyright Act."[15] The Register moreover noted that the proponents of the 2015 Exemption failed

[11] Id. at 21.

[12] *See* 2015 Recommendation at pg. 318 ("[T]he Register takes seriously the concern expressed by other agencies that acts of security testing not put members of the public at risk. On this record, there appeared to be some consensus as to common-sense limitations on the exemption to avoid that risk. In the context of a general security research exemption, there appeared to be universal agreement among proponents that testing in "live" conditions—such as cars being driven on public roads—is wholly inappropriate. The Register thus recommends that the exemption provide that security research must be conducted in a controlled setting designed to avoid harm to individuals or the public.")

[13] Felten petition at pg. 38

[14] Felten petition at pg. 21

[15] 2015 Recommendation at pg. 317, quoting H.R. Conf. Rep. No. 105-551 at 38.

to "explain why research into critical systems is not being or could not be conducted with the authorization of the relevant copyright owner."[16] The considerations that necessitated inclusion of the Device Limitation in the 2015 Exemption apply with equal force today. Proponents have presented no evidence to address the unique public safety risks and regulatory compliance considerations that would arise if the Device Limitation were eliminated.[17] Nor have Proponents presented evidence to demonstrate that they are unable to obtain the consent necessary to perform testing of critical systems.

3. Other Laws Limitation

The Other Laws Limitation provides that circumvention can be undertaken only on a "lawfully acquired device or machine" and that it must "not violate any applicable law, including without limitation the Computer Fraud and Abuse Act." Petitioners assert that the Other Laws Limitation chills good-faith security research by introducing uncertainty about "the lawfulness of the acquisition of software and the lawfulness of the security research."[18] They argue, for instance, that disputes over the "lawfully acquired" requirement could arise if a researcher obtains a device on the secondary market from a seller who is violating the terms of a license with the original vendor.[19] Proponents also caution the Other Laws Limitation inappropriately introduces "complex questions under the Computer Fraud and Abuse Act (CFAA), state contract law, and figural regulatory systems such as those governing medical and telecommunications equipment."[20]

The Register recommended inclusion of the Other Laws Limitation in the 2015 Exemption to ensure that it would be faithful to the intent of "the congressionally enacted exemption in section 1201(j)" and to mitigate the significant public safety and regulatory concerns raised by the Food and Drug Administration, the Department of Transportation, and the Environmental Protection Agency.[21] When it passed the DMCA, congress understood that the prohibition on circumvention could have an adverse impact on important security research. It therefore included a statutory exemption, explaining that:

> [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.[22]

---

[16] 2015 Recommendation at pg. 306

[17] *See* 2015 Recommendation at pg. 315 ("On this record, the Register is persuaded that, under the fifth statutory factor allowing for considerations of additional matters as appropriate, the significant issues raised by opponents concerning the public safety and regulatory compliance, as amplified by regulatory agencies with a derect interest in these matters, are unfavorable to the proposed exemption. Despite the fact that other statutory factors largely favor proponents, the Register must take seriously these additional substantial concerns.")

[18] Felten Petition at pg. 23.

[19] Id.

[20] Id. at 24.

[21] 2015 Recommendation at pg. 318.

[22] H.R. Rep. No. 105-796, at 67 (1998).

The Other Laws Limitation remains critically important to ensuring that the 2015 Exemption is consistent with congress's intent in codifying the DMCA and the type of security research it intended to exempt. Moreover, Petitioners have asserted no material change in law, fact or circumstance since the 2015 rulemaking to warrant the removal of the Other Laws Limitation.

DOCUMENTARY EVIDENCE

[Intentionally left blank]