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

Christopher Mohr, Vice President for Intellectual Property and General Counsel, Software and Information Industry Association, 1090 Vermont Avenue, Washington D.C. cmohr@siia.net

ITEM B. PROPOSED CLASS ADDRESSED

Class 13 (security)

ITEM C. OVERVIEW

SIIA is the principal trade association of the software and information industries and represents over 800 companies that develop and market software and digital content for business, education, and consumers. SIIA's members range from start-up firms to some of the largest and most recognizable corporations in the world, and one of SIIA's primary missions is to protect their intellectual property and advocate a legal and regulatory environment that benefits the software and digital content industries. SIIA member companies are market leaders in many areas, including but by no means limited to:

- software publishing, graphics, and photo editing tools
- corporate database and data processing software
- financial trading and investing services, news, and commodities exchanges
- online legal information and legal research tools
- protection against software viruses and other malware and
- education software and online education services

Our members depend on section 1201 to protect their works from infringement, and SIIA has participated in every rulemaking since the statute's enactment. In our view, Section 1201 has succeeded in performing its intended purpose: namely, to accomplish the "mutually supportive" goals of a "thriving electronic marketplace [that] provides new and powerful ways for the creators of intellectual property to make their works available to legitimate consumers in the digital environment," and a plentiful supply of intellectual property" to drive the demand for a more flexible and efficient marketplace."[1] Congress properly recognized that "the digital environment poses a unique threat to copyright owners" and that it "necessitates protection against devices that undermine copyright interests."[2]

For all these exemptions, we urge the Office to consider the practical effect of the Supreme Court's recent Eleventh Amendment jurisprudence*,* which immunized state entities from the consequences of infringement. As a result, state entities do not have to compensate copyright owners both for the harm caused by circumvention and any underlying infringement that may occur. As a general matter, the Office should consider conditioning every exemption on the presence of a waiver of the claiming entity's sovereign immunity.

With respect to security testing specifically, SIIA did not oppose renewal of the past exemption. Having received that exemption at the last triennial, many of the same petitioners now seek to strip the remaining limitations removed from the security research exemption: as they describe them, the "Use Limitations," and the "Other Laws Limitations."[3] Put in the affirmative, petitioners would like to be able to circumvent TPMs on a computer program for good-faith security research:

- even if the security research served another commercial and directly competitive purpose beyond advancing the state of the security research field, and even if other laws were violated.
- the actual harm suffered by the public or copyright owners.
- even if the act of security research violates any number of laws, including the Consumer Fraud and Abuse Act (18 U.S.C. 1030).
- irrespective of whether the result of the circumvention is primarily used in a manner that facilitates copyright infringement and is primarily used to destroy the security or safety of either the users of the system or the system itself.[4]

Eleventh Amendment issues aside, SIIA opposes that expansion as legally impermissible and unsupported by record evidence.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

[1] H. Rep. 105-551 (Part II), at 23.

[2] *Id.* at 25.

[3] See Halderman Comment at 3.

[4] *See id.*

The Exemption is Overbroad.
SIIA objects to petitioners' proposed class as overbroad. The Register has stated that

> "the description of the ''particular class'' ordinarily will be refined with reference to other factors so that the scope of the class is proportionate to the scope of harm to noninfringing uses. For example, a class might be refined in part by reference to the medium on which the works are distributed, or to the access control measures applied to the works. The description of a class of works may also be refined, in appropriate cases, by reference to the type of user who may take advantage of the exemption or the type of use that may be made pursuant to the designation. The class must be properly tailored to address not only the demonstrated harm, but also to limit the adverse consequences that may result from the exemption to the prohibition on circumvention. In every case, the contours of a class will depend on the factual record established in the rulemaking proceeding."[5]

By deleting the restrictions that make the security testing exemption narrow, what petitioners have done is to create a security testing exemption that applies to all computer programs, regardless of the access controls used, or the medium in which the works are distributed. This is the same class that was rejected in 2018. While the Office has acknowledged that a class of user may help define a class of work, it must do so in conjunction with other factors that narrow the class. Such an exemption lies beyond the scope of the Register's statutory authority.

Petitioners neither acknowledge nor propose any of these limitations. Their proposed limitations should be rejected.

The Evidence for a Broad Exemption is Lacking.
As an initial matter, SIIA questions any suggestion that cybersecurity research in general is suffering from the absence of a broader exemption. Adverse effects on that industry seem missing, as investment and revenues are growing at a rapid rate and have doubled several times in years when the Office did not issue an exemption.[6] At the same time, SIIA also did not oppose re-issuance of the 2018 exemption because, in practice, it believed that exemption to be sufficiently cabined.

Petitioners have requested that the Copyright Office throw even more limitations by the wayside. The evidence of adverse effects cited by petitioners is insufficient to support the breadth of the exemption that they request.

[5] 75 Fed. Reg. at 65260, 65261 (October 26, 2012).

[6] Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach 84.7 Billion in 2017, https://www.gartner.com/newsroom/id/3784965; Cybersecurity market report, https://cybersecurityventures.com/cybersecurity-market-report/ (noting that security market has increased thirty-five fold in the last thirteen years, and is predicted to have

As interpreted by the Register, section 1201 must be *"the* cause" of the adverse effects that allegedly support the petition.[7] Here, the existing exemption for security research requires that the user's activity not be in violation of other statutes, most notably the CFAA. This limitation ensures that section 1201 is the factual and legal cause of any adverse effects that may exist. Conversely, if the CFAA, or ECPA (or a similar statute) prevents certain activity, then 1201 does not cause the adverse effect as a matter of law.

And we have doubts about the DMCA's relation to these causes. For example, some commenters point to an undifferentiated (and recently debunked) fear that voting machines may be manipulated to change totals.[8] But the DMCA is no obstacle for investigation: section 1201 (e) provides a broad exemption for any government-authorized "information security" activity, even were that to be done on a volunteer basis.[9] Proponents of this exemption do not explain why or how this defense is inadequate, as all it requires is the existence of a contract. Nor do they explain how this fear for one specific kind of device ought to map across all forms of networks and devices.

Causal and overbreadth problems with this position aside, the "other laws" limitation should remain. Congress was aware of these other limitations and built them into the statute holistically. More to the point, many copyrighted works are made available on platforms or over networks. It is for this reason that SIIA views the "other laws" limitation as a sensible protection against piratical anti-circumvention activity. Indeed, some of these arguments ignore ordinary rules of statutory construction: there is nothing in the DMCA suggesting that the phrase "applicable law" renders U.S. firms' liability dependent on Chinese statutes.[10]

To the extent that 18 USC 1030 is narrowed (or expanded) by the Supreme Court, the right forum for response is Congress. And to the extent that the expansion of technology has broadened the potential scope of this rulemaking, we believe the Copyright Office's approach of soliciting expertise when it believes appropriate has worked.

Should the Office be tempted to eliminate remaining exemptions, SIIA urges circumspection. We acknowledge that making truly "harmless" connection attempts to *publicly available* computers or devices is not an activity that SIIA or its members would necessarily object to. The difference (to use an admittedly simplified analogy) are questions of degree: the differences between walking on a sidewalk at night and noticing who left their blinds up or picking the front door locks. The difference between these fact patterns is usually set through

[7] 1201 Study, at 115 (emphasis supplied).

[8] *See* Halderman Comment, at 37.

[9] 17 USC 1201(e) (providing broad exemption for law enforcement activity).

[10] Rapid 7, at 5. *Compare Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010) (describing presumption against extraterritoriality and stating that "When a statute gives no clear indication of an extraterritorial application, it has none.").

shared set of customs and usages generally followed by the security community and those who they seek to protect.

As to the "use" limitation, petitioners (again) seek to expand the scope of the anti-circumvention provision beyond the text of the statute, and argue that the use limitations chill their ability to publish research. Case law has long settled the difference between the source code for a particular circumvention tool, discussion of the tool, and use of the tool itself.[11] We are aware of no case that would prevent petitioners from being able to inform consumers that a system is insecure so they can protect themselves, and investment in cybersecurity, although down from pre-pandemic levels, continues to grow despite COVID related strain.[12]

Conclusion.

Although we may disagree with several parts of their arguments and oppose their suggested revisions to the existing regulation, we do not believe that petitioners are interested in committing, facilitating or enabling copyright infringement. SIIA is, instead, concerned that others will misuse an overbroad exemption to place works in the clear, and by so doing cause harm to copyright owners. And to the extent that the security commenters would like to see the security testing defense revised, their complaint is with Congress, not the Copyright Office.

[11] *E.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445–46 (2d Cir. 2001).

[12] *See* Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020, available at https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem#:~:text=Information%20security%20spending%20is%20expected,its%20December%202019%20forecast%20update.&text=%E2%80%9COverall%20we%20expect%20a%20pause,software%20and%20services%20during%202020.%E2%80%9D.