1. **Given concerns raised by participants regarding disclosure of research results to manufacturers, please provide any additional thoughts you may have as to how the Office might approach this issue if it were to recommend the requested exemption. If some sort of disclosure to the manufacturer were required, what would that process be? Please address any relevant First Amendment or regulatory issues in your response.**

2. **Please briefly address how the proposed exemption might relate to or be limited by other federal or state laws or regulations, including but not limited to the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, and any other statutory or regulatory provisions.**

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 share proponents' interest in ensuring that the DMCA does not impede legitimate, good faith security research. The Copyright Office should, however, approach the proposed Class 25 exception cautiously. We have deep reservations about empowering through this rulemaking third parties to self-judge when such identified vulnerabilities can be disclosed to the public at large. Such so called "zero day" approaches to disclosure inevitably increase the risk that disclosed vulnerabilities will be exploited by bad actors to perpetrate identity theft, financial fraud, and potentially other malicious attacks on U.S. critical infrastructure. These economic and national security considerations are far removed from the Copyright Office's core competencies.

Proponents of Class 25 seek an exception to the DMCA with broad implications for cybersecurity generally, from a context in which authors' rights are at best only a collateral consideration. In fact, the Copyright Office is being asked to weigh in on issues that are at the very heart of a broader cybersecurity debate within the Administration and Congress about how and when it is appropriate to obtain and share information related to cyber-threats and cyber-vulnerabilities.

- The National Telecommunications & Information Administration (NTIA) recently solicited comments from the public to identify "cybersecurity issues that affect the digital ecosystem and digital economic growth where broad consensus, coordination action and the development of best practices could substantially improve security for organizations and consumers."[1] NTIA has proposed to convene a multistakeholder process to identify best practices for ensuring that

[1] http://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf

20 F Street NW, Suite 800
Washington, DC 20011
P 202-872-5500
W bsa.org

vulnerability disclosures do not expose the public to unnecessary risks.[2] We submit, with due deference, that the NTIA's proposed multistakeholder process is better venue than the current DMCA rulemaking for prescribing specific practices related to vulnerability disclosures.

- Separately, the Department of Commerce's Bureau of Industry and Security recently issued a Proposed Rule that would impose controls and license requirements on the "export, reexport, or transfer (in-country)" on a broad range of cybersecurity items, including tools used to hack systems to find or exploit vulnerabilities.[3] Notwithstanding BSA's substantial reservations about specific aspects of the proposed export control, BIS's Proposed Rule is aimed at preserving international cybersecurity by instituting controls on the disclosure (export) of technologies that enable repressive regimes and other bad actors to find and exploit security vulnerabilities. These same cybersecurity policies are implicated by Class 25, but the Librarian is being asked to make a determination from a narrow perspective and with woefully inadequate information about broader domestic and international security considerations.

- The Department of Homeland Security has also recently sought public input on best practices for Information Sharing and Analysis Organizations (ISAO) that are being established under the Executive Order signed by the President on February 13, 2015.[4]

- Both the Senate and House of Representatives are currently considering legislation regarding the terms and conditions under which parties should share information about cybersecurity threats both with private parties and the government.[5] Developing the right balance between advancing legitimate cybersecurity goals and affected parties' interests has been challenging. BSA has been a strong advocate of new laws on cybersecurity information sharing, and we believe it is the role of Congress to establish sound policy and new law in a matter of such critical national importance.

In addition to these broader cybersecurity policy considerations, the Copyright Office must also be mindful of the legislative intent underlying the DMCA. When Congress codified the DMCA nearly 20 years ago, it anticipated that the anti-circumvention provisions could interfere with socially beneficial security research. Congress therefore included the § 1201(j) exception to facilitate such research. Notably, § 1201(j) includes a number of safeguards that collectively reflect Congress's intent "to permit circumvention under the appropriate circumstances for purposes of security testing…[as well as] the conditions Congress believes should be imposed on those who take advantage of an exemption for security testing."[6]

Proponents argue that Class 25 is needed in order to resolve ambiguities about the scope of § 1201(j). They note, for instance, that "it is unclear whether Section 1201(j) applies in cases where the person engaging in security testing is not seeking to gain access to, in the words of Section 1201(j), 'a computer, computer system, or computer network.'"[7] However, Class 25 would do much more than merely clarify

---

[2] *Id.* at 14362

[3] http://www.bis.doc.gov/index.php/forms-documents/doc_download/1236-80-fr-28853

[4] https://www.federalregister.gov/articles/2015/05/27/2015-12691/notice-of-request-for-public-comment-regarding-information-sharing-and-analysis-organizations#h-5

[5] *See*, *e.g.,* H.R. 1731 – National Cybersecurity Protection Advancement Act of 2015; H.R. 1560 – Protecting Cyber Networks Act; S.754 – Cybersecurity Information Sharing Act of 2015.

[6] 2010 Determination of the Librarian of Congress at 43833

[7] Professor Green Reply Comments at p. 10

statutory ambiguities. Indeed, while Class 25 covers activity that is functionally equivalent to that permitted by § 1201(j), Class 25 contains *none* of the important safeguards Congress included within the statutory exception. [8]

Among the important safeguards included in § 1201(j) is an explicit carve out for testing that violates the Computer Fraud and Abuse Act ("CFAA").[9] This carve out makes clear that the exception to engage in security testing is subservient to the broader cybersecurity interests as governed, *inter alia*, by the CFAA. Congress was also extremely concerned about the potential damage that might arise from the public dissemination of vulnerability information. Section 1201(j)(3) therefore requires courts to evaluate whether such information is "used solely to promote the security of the owner…or developer" of a computer system and whether it is "used or maintained in a manner that does not facilitate…a violation of privacy or breach of security."

Given the ongoing Congressional and Executive branch focus on the very issues raised in this rulemaking regarding appropriate vulnerability disclosure practices, we urge the Copyright Office not to endorse specific disclosure practices at this time. Should the Copyright Office determine an exemption is necessary, it should, consistent with the spirit of § 1201(j), amend proposed Class 25 so that it: (1) explicitly prohibits unrestricted public disclosures of vulnerabilities, and (2) requires beneficiaries of the exception to undertake a "good faith effort to provide" notification to the relevant software manufacturer and (3) maintain vulnerability information "in a manner that cannot facilitate a breach of security."

[8] *See* BSA Initial Comments ("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).")

[9] 17 U.S.C. § 1201(j)(2).

20 F Street NW, Suite 800 P 202-872-5500
Washington, DC 20011 W bsa.org