Before the
Library of Congress
Copyright Office
Washington, D.C.

In the Matter of	
Exemptions to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies	Docket No. RM 2008-8

COMMENTS OF
COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION

Pursuant to the Notice of Proposed Rulemaking ("NOPR") and request for comments issued by the United States Copyright Office ("the Office") and published in the Federal Register at 73 Fed. Reg. 79,425 (Dec. 29, 2008), the Computer and Communications Industry Association ("CCIA") submits the following comments with respect to the Copyright Office's triennial rulemaking establishing temporary exemptions to the federal prohibition on circumvention of copyright protection systems for access control technologies. These comments support proposed classes 8A and 8B.

CCIA represents large, medium-sized, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications and Internet products and services – companies with more than $250 billion in annual revenues.

I. Supported Classes

CCIA expresses support for the following classes:

> *8A. Literary works, sound recordings, and audiovisual works accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished*

solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

8B. Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

III. Legal Argument

A. Summary

These comments support exemptions for classes of works pertaining to cybersecurity threats. They argue that the Office applies the wrong burden of proof, and that evidence in the record of these proceedings provides sufficient evidence to sustain the requested classes.

B. The Office Applies the Wrong Burden of Proof.

The Office requires that proponents of a temporary exemption meet a 'more likely that not' burden of proof.[1] This standard, which is equivalent to a 'preponderance of the evidence' burden, is not the proper standard to be applied. The proper burden of proof is a 'substantial evidence' standard. The 'substantial evidence' standard is not merely a "label" as suggested by the Notice of Inquiry; it is the legal standard which applicants are obligated to meet, and which the Office is obligated to apply.

By shifting to a 'preponderance' standard with the substitution of "more likely than not" for "likely," the NOI incorrectly increases an applicant's burden of proof to a level inconsistent with numerous in-force and pending free trade agreements (FTAs). The Dominican Republic-Central American Free Trade Agreement (CAFTA-DR), U.S.-

[1] *See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 73 Fed. Reg. 58,073, 58,075 (Oct. 6, 2008) ("This standard of ''likelihood'' requires proof that adverse effects are more likely than not to occur.").

Morocco Free Trade Agreement, and U.S.-Oman Free Trade Agreement all require that exemption proceedings require a showing in which "an actual or likely adverse impact… is demonstrated in a legislative or administrative proceeding by *substantial evidence*."[2] Similarly, the U.S.-Peru and U.S.-Colombia FTAs require that "any exception or limitation adopted in reliance on this subparagraph [regarding any limitations on anticircumvention protection] shall be based on the existence of substantial evidence."[3]

The 'substantial evidence' standard inquires whether the conclusions reached are supported by "substantial evidence," *i.e.*, whether a reasonable factfinder would arrive at the same conclusion. The Supreme Court described substantial evidence as "more than a mere scintilla. It means such relevant evidence as a reasonable mind might accept as adequate to support a conclusion." *Consolidated Edison Co. v. NLRB*, 305 U.S. 197, 229-30 (1938). The D.C. Circuit has made clear that a 'preponderance' standard is inconsistent with a 'substantial evidence' standard. *See Evans Fin. Corp. v. Director*, 161 F.3d 30, 34 (D.C. Cir. 1998) ("As we have said many times before, 'substantial evidence' means more than a 'scintilla,' *but less than a preponderance of the evidence*.") (emphasis added, internal quotations omitted). Accordingly, CCIA submits that applicants must satisfy a 'substantial evidence' standard rather than a 'preponderance' standard in order to justify an exemption.

[2] *See* CAFTA-DR Art. 15.5.7(e)(iii); US-Morocco FTA Art. 15.5(8)(d)(viii); U.S.-Oman FTA Art. 15.4.7(d)(viii).

[3] U.S.-Peru FTA Art. 16.7.4(f); U.S.-Colombia FTA Art. 16.7.4(f). The U.S.-Panama and U.S.-Korea FTAs include similar language, also mandating a substantial evidence standard.

C. Classes 8A and 8B Are Necessary to Protect Cybersecurity.

In the wake of the Sony rookit fiasco in 2006, CCIA proposed that the Office establish an exemption for all works that, like the Sony rootkit, threatened critical infrastructure. The final exemption, however, was narrowly tailored to the facts of the underlying crisis, such that researchers are able to investigate security problems only relating to technological protection measures on sound recordings, and audiovisual works associated with those sound recordings, that are distributed in compact disc format.[4] By so limiting the exemption – notwithstanding evidence in the proceeding that other classes of works could pose similar threats – the Office's 2006 Final Rule presented an incomplete solution to an apparent security threat. Cybersecurity threats cannot be managed in a reactive fashion. To require substantial evidence that the horse has bolted before closing the barn door (and even then, only for three years) is not a viable strategy.

The petition by Halderman *et al*. largely rectifies this problem by expanding the proposed exemption to include classes of works generally embodied in digital formats.[5] Under the 2006 Final Rule, security testing on DRM schemes employed in works other than sound recordings is deterred by uncertainty and a litigious environment. This undermines the secondary market in independent testing and quality assurance on DRM products that, the record indicates, is sorely needed.

---

[4] *See* Cong. Res. Serv., *The Digital Millennium Copyright Act: Exemptions to the Prohibition on Circumvention*, Feb. 21, 2007, at 11.

[5] Indeed, even this exemption may be unduly narrow insofar as it may be limited to general-purpose personal computers. While it is arguably true that the compromise of a dedicated system is less dangerous to the user than the compromise of a general-purpose computer, any system with a large installed base on a general network (e.g., the public Internet) may pose a threat to third parties if compromised in sufficient numbers.

Accordingly, CCIA supports the establishment of exemptions 8A and 8B.[6] A widely deployed, yet compromised technological protection measure has already created vulnerabilities in hundreds of thousands of machines. It is untenable to wait for a security crisis to occur with respect to each individual class of works before granting an exemption for that class. The prior existence of a security crisis affecting sound recordings establishes that a similar crisis is sufficiently likely to afflict other classes of works also distributed in digital form. For these reasons, exemptions 8A and 8B are warranted.

Respectfully submitted,

/s/ Matthew Schruers
Matthew Schruers
Senior Counsel, Litigation & Legislative Affairs
Computer & Communications Industry Association
900 Seventeenth Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070

[6] CCIA's support for these classes of exemptions is not intended to indicate opposition to any other exemptions proposed in this proceeding.