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

In the Matter of	
Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies	Docket No. RM 2005-11

COMMENTS OF
COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION
AND OPEN SOURCE AND INDUSTRY ALLIANCE

Pursuant to the Notice of Inquiry (NOI) and request for comments issued by the United States Copyright Office (the Office) published in the Federal Register at 70 Fed. Reg. 57,526 (Oct. 3, 2005), the Computer and Communications Industry Association (CCIA) and Open Source and Industry Alliance (OSAIA) submit 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.

I. About CCIA and OSAIA

CCIA represents large, medium 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 $200 billion in annual revenues. CCIA also operates OSAIA, a subsidiary project dedicated to the creation, use, and sustainability of open source software. OSAIA members range from small software providers to globally prominent open source development companies.

II. The NOI Employs an Erroneous Burden of Proof.

In the two previous triennial rulemakings, the Office has required proponents of a temporary exemption to meet a "preponderance of the evidence" burden of proof, derived from the legislative history of the Digital Millennium Copyright Act (DMCA).[1] In fact, the Office should have been applying the lower "substantial evidence" burden of proof. Given recent unambiguous Congressional pronouncements, CCIA and OSAIA are confident that the Office will apply the correct burden of proof going forward.

Much ink has been spilled upon the subject of the burden of proof. The current triennial rulemaking is no exception. After an extensive investigation of the legislative history of the DMCA, the NOI states that it would continue to require "substantial" adverse effects. The NOI observes that "the statutory language enacted [in Section 1201], however,… does not specify a standard beyond mere likelihood." NOI at 57,578. The NOI then relies heavily upon legislative history in the form of the House Manager's Report to conclude that Section 1201(a)(1)(C)'s usage of the word "likely" was in fact was intended to mean "more likely that not," *i.e.*, "a preponderance of the evidence." *Id.*

The peculiar transformation of Congress's "likely" into "more likely than not" cannot withstand unambiguous statements ratified by Congress in the Dominican Republic-Central American Free Trade Agreement (CAFTA-DR). Congress ratified CAFTA-DR and all of its provisions upon adopting the "Dominican Republic-Central America-United States Free Trade Agreement Implementation Act" on August 2, 2005.[2] The agreement therefore expresses Congress's will. Section 15.5.7 of CAFTA-DR provides for the implementation of an

[1] *See* Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[2] *See* Pub. L. No. 109-53, 119 Stat. 462 (2005). CAFTA-DR was signed and affirmed pursuant to the Bipartisan Trade Promotion Authority Act of 2002 and the Trade Act of 1974.

anticircumvention regime nearly identical to Chapter 12 of Title 17.[3] While CAFTA-DR has not yet entered into force, its language expresses a clear understanding by Congress as to the standard that the Office's rulemaking should apply. Section 15.5.7(e)(iii) of CAFTA-DR states that exemptions to the anticircumvention regime may be provided for

> noninfringing uses of a work, performance, or phonogram, in a particular class of works, performances, or phonograms, when an actual or likely adverse impact on those noninfringing uses is demonstrated in a legislative or administrative proceeding by *substantial evidence*; provided that in order for any such exception to remain in effect for more than four years, a Party must conduct a review before the expiration of the four-year period and at intervals of at least every four years thereafter, pursuant to which it is demonstrated in such a proceeding by *substantial evidence* that there is a continuing actual or likely adverse impact on the particular noninfringing use.[4]

The Administration and the implementing legislation have made crystal clear that CAFTA-DR is completely consistent with current federal law.[5] Accordingly, CAFTA-DR Chapter 15's articulation of the standard of proof required in administrative proceedings for anticircumvention exemptions demonstrates what Congress understands Section 1201(a)(1)(C) to require *presently*: the application of a "substantial evidence" burden of proof. From Section 15.5.7(e)(iii), one must conclude that Section 1201(a)(1)(C) rulemaking proceedings must be *and must always have been* governed by the "substantial evidence" burden of proof.[6] In light of a clear articulation of the burden of proof, statements in DMCA Section 1201(a)(1)(C) and

---

[3] *See* Pub. L. No. 109-53, § 102(a), 119 Stat. 462, 464. Similarly, The Report of the Industry Functional Advisory Committee on Intellectual Property Rights for Trade Policy Matters (IFAC-3) regarding Chapter 15 of CAFTA-DR describes CAFTA-DR's anticircumvention obligation as the

> requirement that the CAFTA countries implement protection for technological protection measures (TPMs) used by right holders to protect against unauthorized access and exploitation of their works to do so in virtually the same manner as did the U.S. in the DMCA in 1998. In addition, the text provides for a list of narrowly crafted exceptions – in close consistency with how the U.S. Congress approved those exceptions in U.S. law. (Article 15.5.7).

Report at 10 (Mar. 12, 2004), *available online at* <http://www.ustr.gov/assets/Trade_Agreements/Bilateral/CAFTA/CAFTA_Reports/asset_upload_file571_5945.pdf> (last viewed Nov. 21, 2005).

[4] Similar language appears in Article 15.5(8) (d)(viii) of the U.S.-Morocco Free Trade Agreement, ratified by Congress on July 22, 2004.

[5] *See supra*.

[6] Indeed, in its final regulation in 2003 the Office noted as instructive "the Supreme Court's treatment of the term" in its "substantial evidence rule". *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 68 Fed. Reg. 62,011, 62,013 (Oct. 31, 2003).

CAFTA-DR Section 15.5.7(e)(iii) that the adverse impact may be actual *or* "likely" merely serves to establish that a proponent need not undertake the impossible task of proving with certainty that a future event will occur.[7]

This unambiguous expression of Congressional intent obviates any need for further reference to the House Manager's Report. *See Consumer Product Safety Commission v. GTE Sylvania, Inc.*, 447 U.S. 102, 108 (1980) ("We begin with the familiar canon of statutory construction that the starting point for interpreting a statute is the language of the statute itself. Absent a clearly expressed legislative intention to the contrary, that language must ordinarily be regarded as conclusive.")

Upon concluding that the substantial evidence standard governs this proceeding, the question turns to what exactly that standard requires. Again, given clear judicial construction of the "substantial evidence" burden of proof, reference to legislative history is entirely unnecessary. Courts have held that 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).

In applying this standard, the U.S. Court of Appeals for the District of Columbia Circuit has stated in unambiguous language: "As we have said many times before, 'substantial evidence' means more than a 'scintilla,' <u>*but less than a preponderance of the evidence*</u>." *Evans Fin. Corp.*

[7] Of course, "substantial evidence" as an administrative law burden of proof is entirely different from the "substantial adverse impact" rule which the Copyright Office has applied in previous rulemakings.

v. Director, 161 F.3d 30, 34 (D.C. Cir. 1998) (emphasis added, internal quotations omitted). Thus, in light of Congress's additional guidance via CAFTA-DR's requirement that exemptions must be shown by substantial evidence,[8] the Office's previous interpretation that Section 1201(a)(1)(B) imposes a "preponderance of the evidence" standard must be modified.

III. The Office Should Grant an Exemption for Classes of Works that Employ Access Control Measures which Threaten Critical Infrastructure and Potentially Endanger Lives.

Subject to the standard noted above, CCIA and OSAIA request an exemption for the following classes of works:

Classes of Works:

Sound recordings or audiovisual works (including motion pictures) embodied in copies and phonorecords, computer programs or video games, or pictorial, graphic, or literary works or compilations distributed in formats protected by access control measures which threaten critical infrastructure and potentially endanger lives.

Summary:

Recent events demonstrate that technological protection measures can threaten critical infrastructure. Misguided efforts to cloak technological protection measures from consumers have in fact created computer security vulnerabilities worldwide, including on government and military systems. Computer security and other mission critical applications that protect critical infrastructure must not be compromised by technological protection measures. Where such measures threaten critical infrastructure and potentially endanger lives, prohibiting their circumvention – if only to disable or remove them – is an absurd result that Congress could not

[8] *Compare with* Notice of Inquiry, 67 Fed. Reg. 63,578, 63,580 (Oct. 15, 2002) (declining to modify practice where Congress had not applied any additional guidance).

have intended. A temporary exemption to circumvent dangerous access control measures so as to make the non-infringing use of disabling or deleting these measures or the underlying work which they are meant to protect is therefore necessary.

Facts:

CCIA and OSAIA have long advocated for greater computer security. The recent debacle over Sony's XCP and SunComm DRM rootkits illustrates that this mission is not complete. In early November, reports surfaced that Sony BMG had implemented digital rights management technology on 52 music CD albums which, when installed on a user's computer, disguised its own presence and could potentially disguise the presence of other malware. The high technology community was shocked by the revelation that Sony may have surreptitiously installed, in potential violation of state anti-spyware laws, the XCP or SunComm copy control measures on the computers of as many as 20 million consumers who purchased certain copy-protected discs.[9] Even more alarming was the revelation that the cloaking device Sony used to disguise this rootkit from consumers is now being exploited by hackers to launch malicious computer attacks.[10] Because of the security threat posed by these rootkits, several leading security software vendors, including Microsoft, Computer Associates, and Symantec, identified them as security risks and updated security patches to remove or disable them.[11]

This situation demonstrates the need to provide adequate anticircumvention exemptions to ensure that professionals can safeguard national computer security without violating federal

---

[9] Jefferson Graham, *Sony's CD Woes Grow with Texas Lawsuit; Attorney General Cites State Anti-Spyware Law*, USA TODAY, Nov. 22, 2005, at 1B.

[10] Robert McMillan, *Microsoft to Root Out Sony Spyware*, Infoworld.com, Nov. 14, 2005, *available at* <*http://www.infoworld.com/article/05/11/14/HNmicrosoftsony_1.html*> (last viewed Nov. 22, 2005) (noting first instances of hackers employing "XCP's cloaking capabilities to hide malicious software of their own").

[11] Robert McMillan, *Microsoft Targets Sony 'Spyware'*, PCWORLD.COM, Nov. 15, 2005, *available at* <http://www.pcworld.com/news/article/0,aid,123543,00.asp> (last viewed Nov. 22, 2005); Tom Sanders, *Computer Associates Blacklists Sony DRM, Pressure Mounts on Sony to Abandon Insecure Technology*, VNUNET.COM, Nov. 10, 2005 *available at* <http://www.vnunet.com/vnunet/news/2145811/ca-blacklists-sony-drm> (last viewed Nov. 22, 2005).

law. While the DRM rootkits in question are in fact copy controls – for which no exemption rulemaking exists – this fact is happenstance. In light of the current security risks, the possibility that the next technological protection measure could be an access control is substantial evidence that an exemption should be granted to ensure that the access control and/or the work can be disabled or removed. In the Sony rootkit scenario, security experts estimated that 568,200 servers were likely to have been infected – including military and government sites.[12] Security professionals must have unfettered ability to remove these dangerous applications so as to adequately protect critical infrastructure, yet current anticircumvention law may render such activities a violation of federal law.

Argument:

As the NOI makes clear, this rulemaking governs non-infringing uses. If a technological protection measure poses a security risk, a security professional or application designed by such a professional must remedy it. In this case, it is likely that, as in the Sony DRM rootkit scenario, the technological protection measure must be deleted, thereby leaving "unprotected" the underlying work. Remedying a security risk may also require accessing, modifying, or destroying the underlying work. Such uses are non-infringing. Under the current anticircumvention regime, such acts are nevertheless prohibited, thus requiring a temporary exemption.

Section 1201(i) Does Not Address The Required Exemption

The question of so-called "spyware" has previously been brought to the attention of the Register, although never against the backdrop of so serious a security risk. In the 2003

[12] Quinn Norton, *Sony Numbers Add Up to Trouble*, Wired News, Nov. 15, 2005, *available at* <http://www.wired.com/news/print/0,1294,69573,00.html> (last viewed Nov. 22, 2005).

Rulemaking, an exemption was sought for circumventing "spyware." *See* Recommendation of the Register, pp. 194-95. At that time, the Register appears to have taken the meaning of the term "spyware" as necessarily implicating some form of espionage, when in fact the term is generally used to refer to surreptitiously installed applications such as the Sony DRM rootkit. *Id.* Thus, merely because an application is described as "spyware" in the lay context, it should not necessarily be assumed to be collecting personally identifying information, nor should, as the Register concluded in 2003, the exemption in Section 1201(i) be assumed to remedy security risks posed by the application. If a technological protection measure that threatens critical infrastructure does not collect "personally identifying information" as required by Section 1201(i), for example, then that exemption is inapplicable. *See* 17 U.S.C. § 1201(i)(2).

Other factors render this exception inadequate. The statute only authorizes circumvention to disable information collection, *see id.* § 1201(i)(1)(A), although the only means to diminish the capability to collect information may be, as in the Sony rootkit situation, to deactivate or remove the control entirely. Moreover, the circumvention is only authorized in order to protect a "natural person who seeks to gain access to the work protected," *see id.* § 1201(i)(1)(D), when, as in the Sony rootkit situation, non-natural persons were placed at risk, such as governments and corporate operators of critical infrastructure. Additionally, the Sony rootkit functioned by installing stand-alone software separate from the protected work, and thus the risk it created manifested regardless of whether anyone attempted to access – or was even *aware of* the existence of – the underlying work.

Section 1201(j) Does Not Address the Required Exemption

The security testing exemption in Section 1201(j) also proves insufficient. Section 1201(j) only allows accessing "a computer, computer system, or computer network," and does not permit either (a) accessing the offending work itself, so as to disable it, or (b) accessing an electronic device that is not a computer. *Id.* § 1201(j)(1). Therefore, accessing a device such as a consumer electronics product, wireless telephone or Blackberry is not necessarily protected. Furthermore, because Section 1201(j) requires authorization of the owner or operator of the computer, situations in which the nature of the security risk may prevent or render impossible such authorization will not be addressed by Section 1201(j).

In light of these risks, CCIA and OSAIA respectfully suggest that a temporary exemption for the circumvention of access control technologies be permitted for sound recordings or audiovisual works (including motion pictures) embodied in copies and phonorecords, computer programs or video games, or pictorial, graphic, or literary works or compilations distributed in formats protected by access control measures which threaten critical infrastructure and potentially endanger lives.

Respectfully submitted,

/s/ Matthew Schruers
Matthew Schruers
Senior Counsel, Litigation & Legislative Affairs
Computer & Communications Industry Association
666 Eleventh Street NW, Sixth Floor
Washington, D.C. 20001
(202) 783-0070