October 24, 2017

The Honorable Robert Lighthizer
United States Trade Representative
600 17th Street, NW
Washington, DC 20508

We the undersigned companies write to respectfully urge the United States Trade Representative (USTR) to ensure renegotiated copyright protections in the North American Free Trade Agreement (NAFTA) do not create new barriers to cybersecurity testing.

A modernized NAFTA that seeks to ensure "the highest standards covering the broadest possible range of goods and services" should include promotion of cybersecurity services such as independent security testing.[1] Cybersecurity is a large and growing industry in the U.S., and overbroad international cybersecurity regulations can put U.S. companies at a disadvantage. Facilitating international trade in cybersecurity services will foster continued industry growth, promote employment in the field of cybersecurity, and strengthen U.S. competitiveness and leadership in the cybersecurity marketplace.[2] Effective computer security domestically and abroad is key to strengthening the system of international trade and enabling businesses of all types to operate.

The NAFTA negotiating text is classified, and so we have not had the opportunity to review it. However, provisions of the US-Korea free trade agreement (KORUS) are illustrative of the approach we urge USTR to avoid. The text of KORUS replicates much of the statutory language of Sec. 1201 of the Digital Millennium Copyright Act (DMCA) with regard to security testing and circumvention of technological protection measures (TPMs).[3] In the years since KORUS entered into force, cybersecurity industry growth, increasing value of independent security testing, and new legal protections for security testing under DMCA Sec. 1201 have made the KORUS framework inappropriate for a modernized NAFTA.

Provisions that broadly forbid circumvention of TPMs can create legal hindrances and ambiguity for good faith security testing. Cybersecurity companies and researchers rely on the ability to independently circumvent TPMs to analyze software for vulnerabilities. The goal of good faith security testing is not to infringe (or enable others to infringe) upon intellectual property rights, but rather to evaluate and test software for flaws that could cause harm to individuals and businesses.[4] By identifying vulnerabilities in software and devices so that flaws

[1] Office of the United States Trade Representatives, Summary of Objectives for the NAFTA Renegotiation, Jul. 17, 2017, pg. 3, https://ustr.gov/sites/default/files/files/Press/Releases/NAFTAObjectives.pdf.
[2] Bipartisan Congressional Trade Priorities and Accountability Act of 2015, Pub. L. No. 114-26, Jun. 29, 2015, Sec. 102(a)(4).
[3] Compare KORUS Art. 18.4(7)(a), (d)(iv) with 17 U.S.C. 1201(a), (j).
[4] See, for example, Jay Radcliffe, Short Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201, before the U.S. Copyright Office Sixth Triennial Sec. 1201 Proceeding, 2015, https://www.copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Radcliffe_Class25.pdf. See also, Mark Stanislav, Short Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201, before the U.S. Copyright Office Sixth Triennial Sec. 1201 Proceeding, 2015, https://www.copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Stanislav_Class25.pdf.

can be mitigated, independent researchers strengthen digital product security and boost marketplace transparency and competition.

Recognizing that good faith security testing is generally a non-infringing activity with significant benefits, and that DMCA Sec. 1201's existing statutory protections are inadequate, the Librarian of Congress (upon the recommendation of the Copyright Office and National Telecommunications and Information Administration) granted a renewable temporary exemption for independent security testing in 2015.[5] Crucially, this temporary exemption does not require the researcher to obtain prior authorization of the owner of the object being studied.[6] In addition, the Copyright Office recently recommended that Congress make permanent changes to Sec. 1201 to provide greater clarity and flexibility for independent security testing. Among other things, the Copyright Office recommended revising 1) The definition of security testing to include computer programs rather than just computers, computer systems, or computer networks, 2) The requirement that the security testing be performed with prior authorization of the owner of the item being tested, and 3) The requirement that the testing must be performed for the sole purpose of correcting flaws on that computer, system, or network.[7] We agree with many of the Copyright Office's conclusions and recommendations – they support independent security testing, the cybersecurity industry, and ultimately the security of digital products and end users.

If NAFTA's anti-circumvention provisions too closely reflect DMCA Sec. 1201 as related to security testing, we are concerned that this may 1) Curtail independent security testing abroad in the absence of adequate temporary exemptions, 2) Force entities that perform security testing to expend resources in multiple jurisdictions to advocate for temporary exemptions, and to manage potentially differing and conflicting exemptions, and 3) Hinder passage of legislation to implement the Copyright Office's recommended revisions to DMCA Sec. 1201 to provide security testing with greater flexibility.[8]

To promote international trade in cybersecurity products and services, and to preserve the role of independent security research in strengthening the security of technology products, we respectfully urge USTR to ensure that anti-circumvention provisions of modernized trade agreements incorporate clear exceptions for independent security testing that are broader than the text of KORUS or DMCA Sec. 1201. We urge USTR to consider incorporating a security testing exception to anti-circumvention provisions that can accommodate the protections provided by the U.S. Copyright Office's temporary exemption for security testing.

---

[5] U.S. Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. 201, Oct. 28, 2015, pgs. 48-51, http://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf.

[6] *See* U.S. Copyright Office, Study on Section 1201 of Title 17, Jun. 22, 2017, pgs. 76-77, https://www.copyright.gov/policy/1201. Security testing "could be chilled if the owner cannot be located, does not respond, or refuses permission when located. [I]t may be difficult to identify the relevant owner, such as when the focus of the research is on general-purpose software that runs on a wide range of devices, or where the owner of software on a particular device is not known. Moreover, it may not be feasible to obtain authorization even where there is an identifiable owner."

[7] *Id.*, pgs. 74-79.

[8] The Copyright Office noted that compatibility with free trade agreements such as KORUS was a potential complication to its recommended statutory reforms of DMCA Sec. 1201. U.S. Copyright Office, Study on Section 1201 of Title 17, Jun. 22, 2017, pgs. 35, 104.

Thank you for your consideration. We hope to collaborate with you to develop a workable solution that achieves the trade goals of all stakeholders. Please do not hesitate to contact us with any questions or for more information.

Sincerely,

Rapid7
Bugcrowd
CA Technologies
Duo Security
HackerOne
Luta Security

Cc. Secretary Wilbur Ross, U.S. Department of Commerce