AMERICAN UNIVERSITY

WASHINGTON, DC

Jorge L. Contreras
202-274-4424
contreras@wcl.american.edu

April 8, 2013

National Institute of Standards and Technology (NIST)
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899
Attention: Diane Honeycutt
Via email: cyberframework@nist.gov

Re: *Request for Information: Developing a Framework to Improve Critical Infrastructure Cybersecurity (Docket No. 130208119-3119-01)*

Dear Ms. Honeycutt:

I appreciate the opportunity to share these comments in response to NIST's Request for Information (RFI) concerning "Developing a Framework to Improve Critical Infrastructure Cybersecurity". I am a professor of law at American University Washington College of Law, prior to which I spent nearly two decades as a practicing attorney representing technology-focused companies and organizations. Technical standardization is one of my principal areas of research and practice. I currently serve as Co-Chair of the National Conference of Lawyers and Scientists and Co-Chair of the American Bar Association's Section of Science & Technology Law Committee on Technical Standardization. I also serve on the National Academy of Science's Committee on Intellectual Property Management in Standard-Setting Processes. I was the editor of the *Technical Standards Patent Policy Manual* (ABA Publishing: Chicago, 2007) and have written numerous articles, book chapters and blog postings relating to intellectual property and standards development. These comments represent my own views, and not those of American University, Washington College of Law, or any of the other organizations mentioned above.

First, I commend the NIST on seeking public input regarding this critical and timely subject. As NIST correctly points out in the RFI, "[t]he national and economic security of the United States depends on the reliable functioning of critical infrastructure." The following two suggestions are offered in an attempt to aid NIST as it develops a national cybersecurity framework (the Framework) to reduce cybersecurity risks throughout the nation:

1. The Framework should expressly require public interest representation in developing and selecting standards for a national cybersecurity infrastructure.

2. The Framework should adopt approaches that prevent patent disputes from disrupting the broadest possible adoption of cybersecurity standards. Such approaches may include selecting standards for inclusion in the cybersecurity infrastructure only if patent holders have (a) agreed to offer licenses on a royalty-free basis, (b) consented to observe an aggregate royalty cap for all patents covering the standard, or (c) waived their rights to seek injunctive relief.

These recommendations are discussed in more detail below.

1. *The Framework should require public interest representation*.

It is tempting to view standards development purely as a technical exercise in which the most efficient, cost-effective and reliable technology should prevail. Standards for the interconnection of computer components, the transmission of wireless signals and the compression of digital content are largely, though not exclusively, technical in nature. Most such standards are developed in large, open standards-development organizations or smaller industry-focused consortia, in each case the membership of which is comprised of companies that manufacture, purchase and/or use the relevant technology. This well-documented standards-development 'ecosystem' has worked remarkably well to produce standards that have revolutionized the computing, communications and electronics industries.[1]

But cybersecurity is different; cybersecurity affects all Americans in ways that are deeper and more intimate than the selection of features on a smart phone. Inadequate security invites threats that can severely disrupt individual lives, healthcare and finances, expose personal information to misappropriation and abuse, and endanger individual security and privacy. On the other hand, excessive security measures have been criticized for their potential to limit online freedom, dampen free speech and association, and enable intrusive governmental oversight, surveillance and censorship. Despite years of debate, there is no clear line between inadequate security and overly burdensome security. What is clear, however, is that technical choices that are made when security standards and protocols are developed, selected and mandated will have a profound impact on this balance. As Larry Lessig has written, "[w]e can build … cyberspace to protect values that we believe are fundamental, or we can build … cyberspace to allow those values to disappear. There is no middle ground."[2]

In short, cybersecurity affects not only businesses, but individuals. As such, the technical design and selection choices that are made under the Framework will affect individual rights and liberties just as much as they affect security and the safeguarding of business information. For this reason, I urge NIST to include in the Framework a requirement that public interest representatives be included in the process of considering, selecting and approving cybersecurity standards.

---

[1] *See, e.g.*, Brad Biddle, *et al.*, *The Expanding Role and Importance of Standards in the Information and Communications Technology Industry*, 52 JURIMETRICS 177 (2012).

[2] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999). *See also*, LAURA DENARDIS, PROTOCOL POLITICS: THE GLOBALIZATION OF INTERNET GOVERNANCE (2009).

Including public interest considerations in standards development is not a new idea. The Standards Council of Canada notes that "Consumer and public interest stakeholder participation in standardization benefits industry and government users of standards by integrating the consumer and public interest perspective into the standards development discussion, and by helping raise public awareness about the value and importance of standards in our everyday lives."[3] And more than a dozen years ago, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) recommended greater consumer participation in standardization activities.[4] To this end, some U.S.-based SDOs such as ASTM International attempt to "balance" standardization committees by encouraging consumer representation at certain meetings.[5]

Public interest representation is not common, however, at most U.S.-based standards organizations, which are heavily dominated by the commercial sector. And even the "consumer" representatives who participate in standardization meetings are often industry consultants, rather than representatives of civil society or non-governmental organizations (NGOs).[6] It is thus important that the Framework make explicit provision for the inclusion of genuine public interest representation at any "umbrella" standards organization that may be created in the cybersecurity area,[7] and strongly encourage such representation at any independent SDO whose standards will be considered for inclusion in the national cybersecurity infrastructure. In the case of cybersecurity, there are a number of well-respected public interest organizations having the requisite technical and policy expertise to provide this representation.[8]

One of the principal barriers to effective public interest participation in standardization activities is funding. NGOs typically operate on tiny budgets provided by charitable contributions and foundation support. They are often unable to afford the staff time and travel expenses that would be necessitated by participation in a variety of standardization organizations. It is for this reason that ISO/IEC recommends that national standards bodies financially support

---

[3] Standards Council of Canada, Participation in Standardization – Guide for Consumer and Public Interest Representatives 9 (2010) (available at http://www.scc.ca/sites/default/files/migrated_files/DLFE-1291.pdf).

[4] ISO/IEC Statement on Consumer Participation in Standardization Work (May 2001) (available at http://www.iso.org/iso/copolcoparticipation_2001.pdf).

[5] ASTM Intl., Regulations Governing ASTM Technical Committees §7.1.3 (Apr. 2012).

[6] For example, on the 21-member Board of Directors of the Smart Grid Interoperability Panel (SGIP), there is a single "consumer" sector representative. The individual filling this role, however, is a 25-year industry veteran who currently operates an energy management consultancy. Of the two SGIP "At-Large" board members, one is a high-level manager at a major public utility, and the other is employed by a multinational equipment manufacturer. *See* http://sgip.org/board-of-directors/.

[7] An "umbrella" standards organization is one that reviews, comments on and selects standards developed by other SDOs for some overarching purpose. The Smart Grid Interoperability Panel (SGIP) is an example of an umbrella standards organization in the area of smart grid standards. *See* Carter Eltzroth, *'Umbrella' Standards Bodies: Framing Their IPR Policies* (Nov. 2012) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2170744).

[8] Such organizations include the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC). I have not consulted with either of these organizations in making this recommendation, and base my recommendation solely on the publicly-stated missions and track records of these organizations.

their participation in priority areas of standardization.[9] NIST may also wish to consider allocating a portion of its budget for cybersecurity standardization to this end.

2. *The Framework should adopt approaches that prevent patent disputes from disrupting the broadest possible adoption of cybersecurity standards*.

Patents offer an important financial incentive for technology developers to innovate and create new and improved products. In the area of cybersecurity it is crucial that the most advanced and innovative technologies be brought to bear. As such, permitting, and even encouraging, the patenting of technologies used in the national cybersecurity infrastructure seems advisable.

Standards, however, represent a special and limited exception to this general rule. In the area of the national cybersecurity infrastructure, it is likely that standards will be selected both to ensure interoperability among products offered by different vendors (interoperability standards) and to establish minimum levels of security that are acceptable in various contexts (quality standards).[10] In each of these cases, there is a strong national interest in having such standards adopted as broadly and rapidly as possible. That is, in order to avert looming cyber threats, quality standards that assure minimum levels of security and interoperability standards that enable products to interact in a secure and reliable manner should be implemented as soon as possible in every networked product and service offering. Failure to implement these standards broadly will create gaps and vulnerabilities in the national cybersecurity infrastructure that are likely to erode the benefits that such an infrastructure could bring.

For this reason, it is important to reduce, to the greatest extent feasible, patent-related impediments to broad adoption and implementation of cybersecurity standards. In the past few years, litigation over standardized technology has dramatically increased both in quantity and potential market impact. Most significant among these recent suits are the so-called "smart phone wars", in which the largest global manufacturers of mobile devices and software have been engaged in a high-stakes battle over the infringement of dozens of patents, including many that are essential to key industry standards. As observed by one senior government official, "[t]he world . . . is awash in lawsuits related to patented technologies used to make mobile

[9] ISO/IEC Consumer Participation Statement, *supra* note 4, at 3 (Item 4: "If consumers are not able to finance their participation in the standardization process themselves, the national body should enable consumers to participate in priority areas of consumer interest.")

[10] *See, generally*, AM. BAR ASSN. SECT. OF ANTITRUST L., HANDBOOK ON THE ANTITRUST ASPECTS OF STANDARD SETTING 6-10 (2nd ed. 2011). The Federal Trade Commission recently observed the need for more robust cybersecurity technologies in its investigation of and settlement with HTC America. In its complaint against HTC, the Commission alleged that the smart phone vendor's failure to implement reasonable security measures in the Android mobile telephony software platform constituted "unfair acts and practices" in violation of Section 5 of the FTC Act. *In re. HTC America, Inc*., Complaint, No. 122-3049 (Feb. 22, 2013). It is hoped that NIST will enlist the cooperation of all relevant Federal agencies, including the FTC, in developing the Framework and any resulting cybersecurity "quality" standards, so that the market will have clear guidance regarding the Federal government's position regarding the adequacy of cybersecurity measures.

devices."[11] The result of this litigation has been the introduction of uncertainty to affected product markets, not to mention the diversion of large sums of money to litigation.

In the commercial context, such litigation may be viewed by some merely as a necessary (though large) transaction cost required to sort out private entitlements to the lucrative market for smart phones.[12] Under such a view, governmental intervention would be seen as counterproductive and unnecessary to the normal functioning of the market. As noted above, however, the case of technical standards describing critical national infrastructural elements is different. The technology required to implement such standards should be adopted as broadly throughout the market as possible, without the cost, uncertainty and delay occasioned by widespread patent litigation. Cybersecurity standards forming a part of the national cybersecurity infrastructure should thus be insulated, to the greatest extent feasible, from the types of litigation that are currently endemic to commercial technology markets.

There are several ways that this goal could be accomplished. I have outlined a range of possible approaches in prior work on the national smart grid, another area of critical national infrastructure.[13] These include direct legislative action and the exercise of governmental "march-in" rights. In the case of the national cybersecurity infrastructure, however, I believe that a simple selection bias would be the most effective, and least intrusive, means for reducing patent-related risk. That is, the Framework could establish that, in selecting standards for inclusion in a national cybersecurity infrastructure, the selecting agency (whether NIST or an umbrella standards organization) could favor or disfavor certain standards based on patent-related commitments made by relevant parties. These commitments would fall into three categories, each of which is intended to promote the broadest and most rapid adoption of cybersecurity standards in the marketplace:

a. *Royalty-Free Standards*. Much of the current litigation concerning patented standards relates to the royalty rates sought by patent holders, and whether these royalty rates comply with patent holders' commitments to offer licenses on terms that are "fair, reasonable and non-discriminatory" (FRAND).[14] In order to reduce the likelihood of such litigation and the cost and uncertainty that it brings, the Framework could favor standards that can be implemented on a royalty-free basis. That is, holders of all patents essential to the implementation of the standard have committed either not to assert their patents, or to license their patents on a royalty-free basis. Many commercially significant standards are currently available on a royalty-free basis, including the ubiquitous Uniform Serial Bus (USB) and Bluetooth standards, together with many standards produced by the Worldwide Web Consortium (W3C) and OASIS. There are thus viable commercial models that support the use and broad adoption of royalty-free

[11] Renata Hesse, *Six "Small" Proposals for SSOs Before Lunch*, Remarks Prepared for the ITU-T Patent Roundtable, at 9 (Geneva, Switzerland, Oct. 10, 2012).
[12] Many, including myself, disagree with this view, but that debate is beyond the scope of these comments.
[13] *See* Jorge L. Contreras, *Standards, Patents and the National Smart Grid*, 32 PACE L. REV. 641, 669-75 (2012)
[14] *See* Jorge L. Contreras, *Fixing FRAND: A Pseudo-Pool Approach to Standards-Based Patent Licensing* (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2232515) (describing current status of FRAND litigation).

standards.[15] The elimination of royalties on cybersecurity standards would encourage the broadest possible adoption, without the uncertainty and increased cost associated with royalty demands from patent holders.

b. *Aggregate Royalty Caps*. As an alternative to royalty-free standards, the Framework could favor standards as to which aggregate royalty caps have been set or, more proactively, establish such a cap itself. It is well-known that as the number of patents covering a standard increases, so does the uncertainty associated with the royalty burden of implementing that standard in a product. This is the familiar problem of royalty stacking, which has been discussed extensively in the literature.[16] As many commentators on the stacking issue have pointed out, the aggregate royalty burden that results from multiple separate royalty demands can be excessive and has the potential to make a standardized technology uncompetitive in the marketplace or less broadly adopted. This is the case even if individual royalty rates meet some threshold of "reasonableness" when considered separately. As Joseph Farrell explains, "[t]his is because the sum of the incremental values of [multiple] patents exceeds their value in combination."[17]

The establishment of an aggregate royalty cap on all patents covering a particular standard could effectively eliminate the patent stacking problem. Such a cap could be established by the relevant SDO, or by patent holders outside of the SDO context.[18] Such an approach, while still untested in practice, appears to be viable in the view of the relevant antitrust law authorities.[19] Alternatively, the Framework itself could establish a reasonable cap on standards

[15] *See* Andy Updegrove, *Do Royalty-Free Standards 'Stifle Innovation'?*, The Standards Blog (Mar. 4, 2011) (available at http://www.consortiuminfo.org/standardsblog/article.php?story=20110304122357355).

[16] *See, e.g.*, Mark A. Lemley, *Ten Things to Do About Patent Holdup of Standards (and One Not to)*, 48 B.C. L. Rev., 149, 152 (2007); Mark Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 Tex. L. Rev. 1991 (2007); Carl Shapiro, *Navigating the Patent Thicket: Cross-Licenses, Patent Pools and Standard Setting, in* 1 INNOVATION POLICY AND THE ECONOMY 119 (Adam B. Jaffe et al. eds.) (2001). *But see* J. Gregory Sidak, *Patent Holdup and Oligopsonistic Collusion in Standard-Setting Organizations*, 5 J. Competition L. & Econ. 123, 128 (2009) ("the existence and severity of royalty stacking are still conjectures rather than empirically substantiated facts").

[17] Joseph Farrell et al., *Standard Setting, Patents, and Hold-Up*, 74 ANTITRUST L.J. 603, 642 (2007); *see also* Mark Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 TEX. L. REV. 1991, 2013-15 (2007) (describing the well-known problem of Cournot-complements, which arises when multiple suppliers with market power sell complementary products and thereby, causing overall prices to increase above the level that would be set by an integrated monopolist).

[18] Different SDO-based approaches to establishing royalty caps have been proposed in Contreras *Fixing FRAND*, *supra* note 14, and Lemley *Ten Things*, *supra* note 16.

[19] Antitrust concerns regarding potential "group negotiation" of royalty rates in the standards-setting context have largely been dismissed by the Department of Justice, which expressly approved an arrangement whereby an SDO required its members to disclose their "most restrictive" licensing terms and royalty rates in advance. See U.S. Department of Justice, *Business Review Letter to VMEbus International Trade Association* 3 (Oct. 30, 2006). *See also* Deborah Platt Majoras, *Recognizing the Procompetitive Potential of Royalty Discussions in Standard Setting* p. 8 (Remarks prepared for "Standardization and the Law: Developing the Golden Mean for Global Trade," Stanford Law School, Sept. 23, 2005). Such arrangements also appear to be viable under European Union competition law. *See* European Commission, Guidelines on the Applicability of Article 101 of the Treaty on the Functioning of the European Union to Horizontal Co-operation Agreements, ¶299 (2011).

selected for inclusion in the national cybersecurity infrastructure.[20] Accordingly, the Framework should encourage the adoption of aggregate royalty caps to eliminate the uncertainty associated with patent stacking, and should favor standards that are secured by such a royalty cap.

c. *Limiting Injunctive Relief.* The Framework could also favor standards as to which relevant patent holders have waived their right to seek injunctive relief against infringers. Much of the uncertainty associated with the current standards-essential patent litigation arises from the threat that a patent holder could prevent a competitor from manufacturing and selling its products. Volumes have been written concerning whether it is appropriate for a patent holder who is bound by a FRAND commitment to seek an injunction preventing the use of standardized technology after the parties have failed to agree on licensing terms.[21] It has been argued that a prohibition against the sale of a standardized product in such a case would run counter to the "public interest" prong of the test for injunctive relief formulated by the Supreme Court in *eBay v. MercExchange*.[22] Similar "public interest" arguments have been made in the context of exclusion orders that may be issued by the International Trade Commission (ITC).[23] The literature on this topic is extensive and a full review of it is beyond the scope of this comment. However, suffice it to say that if it is in the public interest to prevent injunctions against the manufacture and sale of commercial products such as smart phones, then the public interest in preventing injunctions against the implementation of critical elements of the national cybersecurity infrastructure should be all the more compelling.[24] And, rather than relying on the case-by-case judgments of courts and the ITC, or on enforcement actions by the FTC and other regulatory agencies, NIST could bring certainty to the equation by building into the Framework a preference for standards as to which patent holders have agreed to waive their right to injunctive relief.[25]

---

[20] Such an agency-mandated cap would not be unprecedented. *See* Resp'ts Req. Temporary Relief, *Vizio, Inc. v. Funai Electric Co*., 24 F.C.C.R. 2880 (Feb. 20, 2009) (describing the FCC's approved 5% royalty rate for the patent pool associated with the mandatory ATSC standard for digital television transmission).

[21] *See, e.g*., U.S. Dept. Justice & U.S. Patent & Trademark Off., Policy Statement on Remedies for Standards-Essential Patents Subject to Voluntary F/RAND Commitments (Jan. 8, 2013); Colleen V. Chien & Mark A. Lemley, *Patent Holdup, the ITC, and the Public Interest*, 98 CORNELL L. REV. 1 (2012); Suzanne Michel, *Bargaining for RAND Royalties in the Shadow of Patent Remedies Law*, 77 ANTITRUST L.J. 889 (2011); Colleen Chien et al., *RAND Patents and Exclusion Orders: Submission of 19 Economics and Law Professors to the International Trade Commission*, Santa Clara University School of Law Legal Studies Research Paper Series (No. 07-12, Jul. 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2102865 [hereinafter Professors' ITC Submission]; Brian T. Yeh, *Availability of Injunctive Relief for Standard-Essential Patent Holders*, CRS Report for Congress 7-5700 (Sept. 7, 2012); Joseph Farrell, et al., *supra* note 17, at 616; Lemley & Shapiro, *supra* note 17.

[22] eBay, Inc. v. MercExchange, L.L.C., 547 U.S. 388, 389 (2006) (holding that in order to obtain a permanent injunction against use of an infringing article, a patent holder must demonstrate "(1) that it has suffered an irreparable injury; (2) that remedies available at law are inadequate to compensate for that injury; (3) that considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction").

[23] *See, e.g.*, Chien & Lemley, *supra* note 21; and Professors' ITC Submission, *supra* note 21.

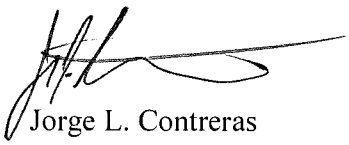
[24] It also being the case, as discussed in note 10, *supra*, that many such cybersecurity standards will likely be implemented in precisely those smart phones and other commercial products.

[25] Certain limited exceptions to this rule, such as those discussed in Professors' ITC Submission, *supra* note 21, would, of course, be appropriate.

Finally, whether or not any of the above approaches are adopted, it is important at a minimum that the Framework mandate the collection and evaluation of as much information as possible regarding potential patent "roadblocks" to widespread implementation of standards selected for the national cybersecurity infrastructure. Such information should include any information known to the relevant SDO and its participants relating to patent assertions, claims, transfers and disputes concerning the standard.[26]

Thank you again for the opportunity to offer these comments in response to the RFI. Please do not hesitate to let me know if there is any additional information that I can provide in support of this important project.

Respectfully yours,



Jorge L. Contreras

[26] The ambivalent results of the SGIP effort in this regard may be informative. *See* Contreras *Smart Grid*, *supra* note 13, at 668-69.