May 19, 2020

LES Standards Development Organization

Via email to: Standards@LES.org; psa@ANSI.org

Re: Comments in Response to Request for Public Comment re BSR/LES IPSC.001.1-202x, Management System for the Protection of Intellectual Property in the Supply Chain -Requirements (new standard), ANSI Standards Action at 22 (March 27, 2020)

Dear Colleagues:

As Chair of the Section of Intellectual Property Law of the American Bar Association (the “Section”), I write on behalf of the Section to provide the Section’s Comments and Recommendations responding to the request for public comment regarding BSR/LES IPSC.001.1-202x, Management System for the Protection of Intellectual Property in the Supply Chain Requirements, Version 1.0 – Draft for Initial Public Comments (“Draft Standard”), published at ANSI Standards Action at 22 (March 27, 2020). These Comments and Recommendations were developed by a task force of the Section’s Trade Secrets Committee with comments from the In-House IP Committee and were considered and approved by the Section’s Council. The views expressed herein are presented on behalf of the Section and have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the positions of the Association.

Since 1894, the ABA-IPL Section has advanced the development and improvement of intellectual property laws and their fair and just administration. As the forum for rich perspectives and balanced insight on the full spectrum of intellectual property law, the Section serves within the ABA as a highly respected voice within the intellectual property profession, before policy makers, and with the public.
The Section commends the comprehensive compilation of best practices for the protection of trade secrets and other confidential information in the Draft Standard by the LES IP Protection in Supply Chain Standards Committee. The Section appreciates this opportunity to share with the LES Standards Development Organization ("LES-SDO") some concerns about establishment of these best practices as standards for enterprise protection of trade secrets and other confidential information designated by the enterprise as “Critical IP” and recommends for LES-SDO’s consideration the below changes to the Draft Standard.

The Section’s Comments and Recommendations are grouped here as (I) questions regarding the scope of the Draft Standard as to different intellectual property rights ("IPRs") and their management across different jurisdictions and legal regimes implicated in many supply chains and recommended clarifications and further development of the management system; (II) questions of the appropriateness of standards for the management of trade secrets and other confidential information and recommended recasting as “best practices”; and (III) broad definitional issues of (A) whether designation of “Critical IP” may weaken protection for information not so designated but meriting protection and a recommendation of eliminating such designation; (B) whether “breach” is defined unfairly to the protected entity and a recommendation to eliminate that definition and (C) whether “risk” is defined too narrowly and a recommendation to eliminate that definition.

I. SCOPE

Even though the Draft Standard defines “IP” to include “any product of the human mind that is protected or is protectable by patent, copyright, trade secret, or trademark laws and information that is considered proprietary or confidential,” the focal “Critical IP” is defined as “information deemed by an organization to be critical.” Patents, copyrights and trademarks are rights – not information, although they may be based on information; indeed, patents are granted in return for disclosure of enabling information, U.S. copyrights until 1978 for publication with a copyright notice (and publication since that time not detrimental to the copyright) and U.S. trademarks for use of the “information” of the mark in connection with commerce in the product or service. The detailed security framework of the Draft Standard and its vocabulary such as “disclosure of IP” as “the action of releasing information” are mostly irrelevant to “traditional IP”.1 To avoid confusion of users – and to prevent misuse by adversaries in

---

1 Until relatively recently in the U.S., and still in most other jurisdictions, “trade secrets” were not considered “intellectual property” (a term that gained popularity with the World Intellectual Property Organization) which comprehends the European notions of “industrial property” (patents and trademarks) and authors’ rights (including the “economic rights” of copyrights). The seminal 1979 Uniform Trade Secrets Act (“UTSA”) was not cast a protection of a property right for at least the reason that different “owners” may develop the same protected information or “trade secret” independently, but as a right
business or litigation – the Section recommends that the Draft Standard not refer to “intellectual property” in its title and where all IP is not concerned, but instead refer to the “proprietary information” which it actually addresses.

Moreover, except for prescribing enterprise precautions in Section 13.0 for protecting its “Critical IP” in dealings with third parties (presumably under American competition, contract and employment law), the Draft Standard does not address transactional and jurisdictional issues that arise in supply chains linking entities in different business and legal regimes, whether interstate or international. Specific concerns include the different scopes of protection afforded by different jurisdictions for undisclosed information (some jurisdictions require tangible embodiment), different competition-IPR rules affecting “first sale” or “exhaustion” and standards-essential IPRs, and different rules for trademark quality control (for example, protecting reputation against child or prison labor). Again, to avoid confusion of users – and to prevent misuse by adversaries in business or litigation – the Section recommends that the Draft Standard not refer to “supply chain” in its title, which is best retitled to “Enterprise Management System for Proprietary Information.”

Even then, Section 13.0’s reliance on the “IP [proprietary information] protection maturity level” of third parties to determine “appropriate contractual requirements” may fall short in protecting the enterprise’s “Critical IP” at least because appropriate contractual requirements may not be enforceable and because Section 13.0 only considers outward disclosure of “Critical IP” and not inbound information that may “poison” the enterprise’s “Critical IP.” For example, over-reaching non-disclosure agreements, restrictive covenants on downstream reverse engineering, and resale price controls based on rights in confidential information may be unenforceable. Certain “flavors” of open-source licensing downstream such as GPL 2.0+ may limit freedom to sell computer programs that incorporate the licensed information. History and assessment of “maturity” are dangerous substitutes for legal analysis. Accordingly, the Section recommends development and inclusion in Section 13.0, which should be retitled, of legal assessment of contracts and transactions involving both out-bound, in-bound and shared information.

II. PRESCRIPTIVE STANDARDS OR BEST PRACTICES?

The Draft Standard laudably provides a comprehensive compilation of best practices for trade secret protection, including state-of-the-art security components that apply the considerations required by the Security Rule promulgated under the Health Insurance Portability and Accountability Act and by state personal data security (written plans) and breach notification statutes, which have become pervasive in the personal data

against the unfair competition act of misappropriation of valuable information that was protected from disclosure using reasonable efforts.
security regime, to current security threats. In that regime, failure to comply with policies adopted to implement the required considerations may result in enforcement by a public agency, but the same public enforcement considerations do not apply with respect to trade secrets. The Section is concerned that a trade secret misappropriator may avoid liability based on “owner” non-compliance with similar standards. Even though the proposed standards are “voluntary,” standards can become baselines – a floor below which there may be an inference of liability (as in products liability cases) – or non-liability in the case of trade secrets misappropriation.

In addition to its concern about a de facto creation of a baseline for protection of trade secrets and other confidential information, the Section questions whether specific operational standards are appropriate for or even applicable to the wide range of valuable information protection of which should be enforceable. While the Section appreciates the best practices detailed in the Draft Standard to provide the core requirements of security and secrecy for protection of trade secrets and other confidential information, the Section maintains that the universal requirement of “reasonable measures” under TRIPS Article 39 to secure proprietary information cannot be set as a specific operational “standard” – as it is industry-, enterprise-, or situation-specific.

Contractual arrangements may be reasonable in some cases (such as protectable know-how and secrets mentally held), while encryption or biometric access may be required in others (such as highly sensitive and complex formulas and code). Different measures may be appropriate for different types of information within the same enterprise or for different circumstances under which the information is acquired, shared or used. This is consistent with the American law that has developed under state versions of the UTSA and under the federal Defend Trade Secrets Act.

Based upon these considerations, the Section urges the LES-SDO to advance its excellent security operational recommendations as best practices rather than as operational standards that may effectively pose an inappropriately high hurdle for legal protection of valuable confidential information.

III. SPECIFIC DEFINITIONAL ISSUES

The Section makes a friendly observation that although it is appropriate in technical standards to provide extensive definitions, where legal effects are directly implicated (such as the previous stated concerns about contractual duties of supply-chain participants), sometimes “less is more,” and flexibility to protect meritorious information should not be sacrificed for rigidly mandated security programs. The Section hopes that it will have another opportunity to comment on the consistency of mandated components with valuable information that foreseeably should be protected. Following are some central definitions of the Draft Standard that merit immediate consideration and change.
A. Classification as “Critical IP” Weaken Protection for “Other IP.”

The Draft Standard to classify information as “Critical IP” itself lowers the status of the information and thereby weakens protection for information not so specified at the time such classification is made. Section 6.3 by mandating classification of “Critical IP” according to “established definition” and “established process” may miss valuable, otherwise protectable information that may be acquired outside of such definitions or processes, for example, information acquired between meetings of an established invention review committee. Moreover, as discussed in the preceding section, standard operating procedures may not apply to some valuable information such as know-how that may be otherwise protectable in some contexts and jurisdictions. At the same time, “Critical IP” is so broad that it embraces third-party information independently developed or previously acquired by a third-party collaborator of the organization (see note 1 supra as to joint ownership). For example, the term “IP” embraces information “considered proprietary or confidential to the organization or to another entity” without further qualification. This classification may be unduly harsh to trade secret owners, supply chain providers, and collaborators independently possessing similar information.

Technical restrictions on otherwise protectable confidential information have been disfavored perennially by the Section.2 The disfavored restrictions were exemplified by the “use requirement” of American state common law prior to the UTSA and requirements of use or tangibility in some other countries. However, the Draft Standard, modeled on technical product and process standards, introduces a technical restriction at a process level for what qualifies as “Critical IP” and its adequate protection. While the Draft Standard presents an excellent catalog of best practices, mandating those practices for subjective and often temporal “Critical IP” may be unduly restrictive both for information so classified according to established processes and for meritorious information missed by such processes.

For these reasons, and for those set forth in Section I above, the Section recommends eliminating the “Critical IP” concept—including a change from “IP” to “proprietary information” everywhere patents, copyrights or trademarks are not implicated—and recasting the procedures and facilities prescribed by the Draft Standard as “best practices.”

---

2 E.g., EXPANDED FEDERAL JURISDICTION FOR TRADE SECRETS (Passed by Council 11/09/2012 410-1) (favoring a federal framework in with”[a] definition of trade secrets that is expansive versus restrictive”); TRADE SECRET CLAIMS (Passed by Council 9/16/2014 R410 -3) (favoring ”[a] definition of trade secret that is clear and effective and not unduly restrictive or overly technical”).
B. Because of the Potential for Abuse, the Definition of “Breach” Should Be Deleted.

The Section appreciates the current security-savvy adaptation of the personal data breach notification (“incident response”) procedure to breaches of security of “Critical IP,” but questions whether the consumer breach framework with designated incident response teams (Section 7.0) is necessary or appropriate for an enterprise invested in protecting its “Critical IP” (and perhaps that of supply-chain partners), particularly if the enterprise is a smaller entity. Although it is important to provide information to enterprise decision-makers about loss and to mitigate such loss, there is not a consumer data breach requirement to notify a large public so that that individuals may act to protect themselves. Obligations to supply-chain partners can be negotiated.

The Draft Standard defines “breach” as a loss “resulting from flaws in controls for protection of information.” This implies a breach can only occur due to a problem or defect in the company’s controls. However, in the real world, a breach is not always the result of a “flaw” in a control – even if the control meets minimal standards. It is often the intentional result of someone overriding or evading a valid control. Relative to corporate security and secrecy policies, a breach may be the result of a failure to comply by even well-meaning employees who are absorbed in their primary duties, for example, a failure to “lock down” information shared during joint development and brainstorming with development partners.

The Section is concerned that in litigation, the Draft Standard definition of “breach” could be misused to presumptively cast responsibility on the trade secret owner for not having sufficient compliance practices in place rather than on a wrongdoer who might have overridden valid controls. There is concern about whether “breach” of an overly high standard of control defeats the proprietor of information because of inability to meet the self-imposed control and whether such “breach” is to be charged to a third party. Further, the term “breach” may create confusion in a contractual dispute setting involving “Critical IP.”

The Section recommends reconsideration of and rolling back of the “Incident Response” Section 7.0 to what is actually necessary for enterprises to protect their proprietary information. The definition of “incident” as including “compromise” may be adequate, and even if “breach” is necessary in a context, its meaning can be gleaned from that context without a definition that may be abused.

C. The Definition of “Risk” Should Be Deleted As Too Limiting and Ambiguous.

“Risk” is defined by the Draft Standard as the possibility that “an unforeseen event” or “deviation from the expected” will negatively affect the organization. This is
unduly limiting. In the protection of trade secrets certain “risks” are known in that they can be foreseen and are even expected, just not the exact time and extent (e.g., misconduct involving departing employees). The “risk assessment” mandated by the Draft Standard as a commendable application of well-accepted security policy would involve some effort to foresee events that may result in loss, but yet allow broad, undefined contingencies. The definition of “risk,” which is not expressly incorporated in the definition of “risk assessment,” should therefore be or deleted as extraneous and ambiguous.

*****

The ABA-IPL Section appreciates the opportunity to provide feedback to the LES Standards Development Organization on the Draft Standard. ABA-IPL looks forward to further dialog with the LES-SDO or its IP Protection in Supply Chain Committee with regard to the issues raised and recommendations made above.

Sincerely,

George W. Jordan III
Chair, ABA Section of Intellectual Property Law