Morgan Lewis

alert

privacy and cybersecurity lawflash

November 19, 2014

NIST Draft Guide Advances the Debate on Cybersecurity Issues

Private sector entities looking to comment on the draft should focus on its recommendations surrounding sharing communities, standardized transfer mechanisms, and the handling of corporate legal considerations.

Information sharing has been a central part of the cybersecurity debate for policymakers and the tech community. Over the last few years, Congress has been considering a number of bills designed to promote different aspects of information sharing, but none have been finalized.[1] These measures in large part concern the sharing of cyber threat information by the intelligence community with the private sector and also information from the private sector with the U.S. government and others in the private sector. Advocates, like Senator Dianne Feinstein, see formalized information sharing as "an important step toward curbing" cyberattacks.[2] Others have raised concerns about information sharing and individual privacy.[3] Although it is unlikely that cybersecurity legislation will be enacted in the remaining months of the 2014 lame duck session, the framework of this policy debate will continue in the 114th Congress during 2015–16.

Entering the fray on October 31, 2014, the National Institute of Standards and Technology (NIST) released its draft publication *Guide to Cyber Threat Information Sharing* (Guide).[4] The draft calls for public comments by November 28. As opposed to prior efforts by NIST targeted only at critical infrastructure entities, this Guide seeks to advise all organizations on enhancing their information-sharing practices.[5] To encourage a framework that is more responsive to private sector concerns and establish a track record of reliable feedback, private sector entities may wish to review the draft and consider commenting on a number of areas certain to influence the debate about information sharing going forward, and this LawFlash suggests several areas of focus for private

1. The House of Representatives passed legislation in 2012 and 2013, which involves the sharing of cyber threat information by the intelligence community with the private sector. *See* Cyber Intelligence Sharing and Protection Act (CISPA), H.R. 3523, 112th Cong. 1st Sess. (introduced Nov. 30, 2011); and Cyber Intelligence Sharing and Protection Act of 2013 (CISPA), H.R. 624, 113th Cong., 1st Sess. (introduced Feb. 13, 2013). On July 10, 2014, the Senate Select Committee on Intelligence reported out legislation to the Senate. *See* Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong., 2d Sess.

2. Gregory S. McNeal, "Controversial Cybersecurity Bill Known as CISA Advances Out of Senate Committee," *Forbes* (July 9, 2014) *available at* http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/.

3. Mark Jaycox, "A Zombie Bill Comes Back to Life: A Look at the Senate's Cybersecurity Information Sharing Act of 2014," Electronic Frontier Foundation (June 29, 2014) *available at* https://www.eff.org/deeplinks/2014/06/zombie-bill-comes-back-look-senates-cybersecurity-information-sharing-act-2014.

4. The NIST draft *Guide to Cyber Threat Information Sharing,* Special Publication 800-150 (hereinafter Guide) is available at http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf.

5. On February 12, 2013, President Barack Obama issued an executive order requiring NIST to establish a voluntary cybersecurity framework for designated critical infrastructure entities. *See* Executive Order—Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; *see also* Stephen M. Spina and J. Daniel Skees, "President Obama Signs Executive Order on Cybersecurity," Morgan Lewis LawFlash (Feb. 14, 2013), *available at* http://www.morganlewis.com/pubs/Energy_LF_ExecutiveOrderOnCybersecurity_14feb13. The voluntary framework suggests standards and best practices that national critical infrastructure entities can use to guard against cybersecurity threats. In February 2014, NIST released the final version of the framework. *See* Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf; *see also* Gregory T. Parks, Ezra D. Church, "New Cybersecurity Framework Revealed," Morgan Lewis LawFlash (April 18, 2014), *available at* http://www.morganlewis.com/pubs/ACPP_LF_NewCybersecurityFrameworkRevealed_18april14.

 © 2014 Morgan, Lewis & Bockius LLP

sector consideration and comment.

Key Areas of Interest

The Guide makes many helpful suggestions that extend beyond information sharing. It proposes ideal security frameworks and a host of strategies for companies to shore up their data-protection practices. It also advises that organizations should conduct an information inventory. Moreover, NIST identifies several benefits and challenges of information sharing. Some of the benefits include shared situational awareness, enhanced threat understanding, and improved defensive "agility." Some of the challenges include disclosure risks, privacy concerns, and various technical barriers. Nonetheless, three areas particularly related to NIST's information-sharing recommendations are likely to be of greatest interest to private sector entities: NIST's recommendations on joining a sharing community, establishing standardized transfer mechanisms, and handling of various legal considerations.

Joining a Sharing Community

The Guide extols the benefits of joining a sharing community, suggesting that such communities can be organized around industry sectors or other shared characteristics.[6] NIST details the types of sensitive information that could be implicated by sharing, such as packet headers, payloads, and logs of organizational activity, and NIST recommends certain controls in the sharing process.[7] Moreover, the Guide recommends using the U.S. Computer Emergency Readiness Team's Traffic Light Protocol, a system for marking categories of information by color and clearly delineating the rules around sharing each category.[8]

In an appendix, NIST provides some real-life information-sharing scenarios. Some examples involve malware and distributed denial of service attacks against specific industry sectors where one company may have the expertise to analyze certain threats that are experienced by another company, permitting stronger defenses for both.

Notwithstanding these benefits, private sector parties may find that additional emphasis can be placed on the sensitivity of intellectual property and trade secrets and the substantial risks—both legal and commercial—of streamlined information-sharing procedures in exposing such risks. Indeed, although NIST makes passing reference to such concerns, it is likely the spillage of competitively sensitive information that is currently one of the most substantial hurdles to the type of widespread information sharing that the government currently envisions.

Establishing Standardized Transfer Mechanisms

Along similar lines, NIST recommends using open, standard data formats and transport protocols to facilitate the rapid—in some cases, nearly real-time—exchange of information.[9] NIST recognizes the need to scrub shared information for competitively sensitive data. But in an information economy where competitive advantage is frequently woven into unique systemic architecture, NIST's current framework may not adequately contemplate the substantial challenges faced by reconstructing meaningful threat information that does not simultaneously reveal sensitive corporate attributes. Moreover, although such streamlined data organization facilitates information sharing, it also creates added security vulnerabilities that potentially permit cyber spies and criminals to more readily access information as parties potentially adhere to uniform formats.

There are no easy solutions to these challenges, but the NIST framework may benefit from private sector insight on alternative solutions.

6. *See* Guide at 6, 12.
7. *See id.* at 30–31, 41–42.
8. *See id.* at 41.
9. *See id.* at 2, 29.

 © 2014 Morgan, Lewis & Bockius LLP

Sensitivity to Private Sector Legal Considerations

Finally, although NIST makes many nominal references to the need to consult legal counsel, it states that one of the primary challenges to information sharing is that organizations' "executive and legal teams may restrict the types of information that the organization can share," and NIST is concerned about unwarranted and arbitrary restrictions on such sharing.[10] Although theoretically legitimate, this formulation overlooks one of the prime impediments to currently pending information-security legislation: legal liability.

Companies are naturally reticent to divulge proprietary data where doing so could expose evidence that parties in litigation may seek to hold against them. Moreover, there are weighty corporate considerations that surround a potential waiver of attorney-client privileges. This is particularly true where threat information is identified because of some breach or other event loaded with legal considerations.

Opportunity to Contribute

The Guide clearly cannot address every area of information sharing in this complex arena. But, as is the case with the critical infrastructure framework, even voluntary standards can establish the baseline for future statutory and regulatory discussions. Thus, private entities must keep a watchful eye on best practice standards and would do well to review the draft Guide and provide feedback on those areas of most interest.

Contacts

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis lawyers:

Washington, D.C./Palo Alto
Mark L. Krotoski +1.202.739.5024/+1.650.843.7212 mkrotoski@morganlewis.com

Washington, D.C.
Brock D. Dahl +1.202.739.5029 bdahl@morganlewis.com

About Morgan, Lewis & Bockius LLP

Founded in 1873, Morgan Lewis offers more than 1,600 legal professionals—including lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists—in 26 offices across the United States, Europe, Asia, and the Middle East. The firm provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

This LawFlash is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered **Attorney Advertising** in some jurisdictions. Please note that the prior results discussed in the material do not guarantee similar outcomes. Links provided from outside sources are subject to expiration or change. © 2014 Morgan, Lewis & Bockius LLP. All Rights Reserved.

10. *See id.* at 8.