Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 32, ISSUE 24 / MAY 7, 2015

EXPERT ANALYSIS

Legislative and Executive Branches Work Toward Cybersecurity Compromise

By Mark L. Krotoski, Esq., and Brock Dahl, Esq.
Morgan, Lewis & Bockius

Amid increasing concerns about data security and privacy in the wake of several high-profile hacks, Washington has been alight with debates about policy solutions to America's cyber vulnerabilities. Recent legislative proposals follow on the heels of a White House executive order the administration hopes will promote greater cybersecurity primarily through voluntary information sharing.

In the coming weeks, Congress could potentially solidify the law regarding information sharing. In conjunction with the administration's approach that is already reflected in the recent executive order, this law will substantially influence cybersecurity in the years to come.

The concept of encouraging voluntary information sharing has become the focal point of the Washington policy community, largely as a response to public concerns that directly regulating cybersecurity would be ineffective and potentially harmful. In 2011, Congress debated a wide-ranging legislative push to unleash mandatory cybersecurity requirements upon a loosely defined critical infrastructure community.[1] The initiative failed, in part, because of fears of government overreach and concerns about privacy.

Subsequent attempts to "do something" about cybersecurity are largely shorn of the taint of regulatory overreach because they have focused on the concept of "voluntary information sharing."

At a highly simplistic level, information-sharing initiatives aim to encourage, but not require, American companies to provide technical information to the U.S. government about the types of cyberthreats they are facing. For example, a bank may see malware with a specific type of technical signature or an oil company may identify a phishing campaign in which multiple senior executives receive similar, questionable emails.[2] The government then hopes to use that threat information to educate the private sector more broadly so that companies can take necessary measures to defend themselves and the government can identify specific threat patterns and actors.

However, the transition to a focus on information sharing has led to heightened concerns about privacy and corporate liability. In particular, critics are concerned that information shared by companies may contain their stored private data about individuals. They are also concerned that sharing really is just a thinly veiled opportunity for mass data collection (some say "surveillance") by the U.S. government.[3]

Concerns also abound from various corporate quarters that information sharing could expose companies to suits either because of the actual act of sharing information or by shareholders or government agencies because the substance of information shared may reveal potentially negligent activity that led to security vulnerabilities in the first place.[4]

LEGISLATIVE INITIATIVES

To address these concerns, Congress is currently debating several iterations of legislation on information sharing. In the Senate, the discussion surrounds the Cybersecurity Information Sharing

Act of 2015, also known as CISA 2015 or S. 754[5]; in the House, the Protecting Cyber Networks Act, H.R. 1560, and the National Cybersecurity Protection Advancement Act of 2015, H.R. 1731, have both been subject to debate.[6]

Though the bills differ in their particulars, several key themes have emerged from the discussions about them. The bills generally:

- Aim to facilitate information by and between the private sector and federal government.
- Aim to provide heightened privacy protections for information provided to the government.
- Seek to offer certain liability protections to corporations.

It is still early in the legislative process. However, it appears that a consensus is forming on key aspects of meaningful legislation to encourage information sharing. Moreover, material disparities among the bills exist, and such disparities would require an entirely separate analysis to be adequately addressed. The point, for our purposes, is that these issues are being actively debated in the legislative sphere to an extent previously unseen. And, if the current trends continue, some resolution of these debates appears possible in this Congress.

Moreover, critical to understanding the import of these legislative debates is knowing that they have arisen in the wake of an executive order that takes several notable steps in the cybersecurity space. The executive order also provides a roadmap for the direction in which the administration will head once it receives legislative authority to act more aggressively on cybersecurity.

In the coming weeks, Congress could potentially solidify the law regarding information sharing, substantially influencing the cybersecurity space in the years to come.

EXECUTIVE ACTION TO FILL THE VOID

On Feb. 13, President Barack Obama signed an executive order that his administration highlighted as being a catalyst for promoting information sharing about cybersecurity threats within the private sector and between the private sector and the government.[7] The federal government has taken a number of steps, but more remain to be taken toward accomplishing this objective.[8]

The executive order still leaves certain hot-button questions such as liability and privacy issues open to debate and subject to private-sector concerns. The new order also seems to add bureaucracy to an already heavily laden information-sharing framework, and the proposed lines of authority between government agencies and the newly envisioned non-governmental organizations must be better explicated to be of practical value.

In the end, it will be necessary to pass the currently debated legislation in order to provide the private sector with meaningful incentives to fully engage in the type of information sharing that the government envisions and to ensure limits on a potential future regulatory expansion into the private sector with respect to cybersecurity. Until these issues can be tackled, the government's envisioned holistic solution will remain out of reach. The key features of the new executive order which could figure prominently in the information-sharing landscape in the coming years are reviewed below.

MORE ROBUST DHS AUTHORITIES

The order's most immediate tangible change is to integrate the Department of Homeland Security into the National Industrial Security Program, making cybersecurity information sharing an explicit part of that program. Since its inception in 1993, the NISP has primarily provided a means for the defense industrial base to exchange classified information to facilitate government contracting work and private-public partnerships.

Although historically the NISP has authorized four agencies — the Department of Defense, the Department of Energy, the Central Intelligence Agency and the Nuclear Regulatory Commission — to manage the passage of classified information to the private sector, the order elevates DHS to equal status with these four agencies. This provides a ready-made mechanism for DHS to share sensitive information.

The amendments, more generally, also make DHS an integral player in the NISP program, signaling the critical function DHS is expected to play in the nation's cybersecurity as an interface with the private sector for threat information and solutions.[9]

NEW INFORMATION-SHARING BUREAUCRACY: GOVERNMENT AND PRIVATE-SECTOR ROLES

At the core of the cybersecurity information-sharing debate are a host of questions about the role of government in the process.

- What is the best role of government and the private sector in promoting cybersecurity information sharing?
- Should the government impose new regulatory standards on the private sector or provide incentives for voluntary private-sector participation?
- What role can government serve to address privacy concerns and liability protections for the private sector?
- To what extent are new agencies or layers of bureaucracy needed, and can these functions be fulfilled by existing agencies?
- On the issue of privacy, how will the government use the information it obtains?

Though these questions may require legislation to be addressed with finality, the new executive order also highlights their importance. Also, the administration has again encouraged the establishment of voluntary sharing organizations as a way to provide forward momentum on cybersecurity without seeming to intervene too directly.

Notably, the new executive order comes almost two years to the day after Executive Order 13636 and Presidential Policy Directive 21, both of which focused on strengthening the cybersecurity of U.S. critical infrastructure sectors.[10] However, the most recent executive order creates new bureaucracy based on information sharing that expands far beyond the government's previous focus on protecting critical infrastructure sectors.

Although this bureaucracy seems to encompass the current structure of entities meant to address critical infrastructure concerns, it also introduces the possibility of government involvement in nearly every sector that may adhere to the information-sharing mechanisms. The executive order encourages the development of organizations intended to facilitate information sharing (called Information Sharing and Analysis Organizations, or ISAOs) and directs DHS to engage a non-government organization to create voluntary information-sharing standards.

Recent information-sharing initiatives aim to encourage, but not require, American companies to provide technical information to the U.S. government about cyberthreats.

EXPANSION OF ISAOS

The order states that the DHS secretary shall "strongly encourage" the development of ISAOs. It envisions that these organizations will be structured around sectoral, sub-sectoral or regional grounds, or around "any other affinity." The order plans to create more formalized structures that would drive information-sharing initiatives, probably under the overall prodding of DHS. It remains to be seen, however, how this will work in practice and differ from the status quo in the critical infrastructure sector.

A fairly elaborate framework already exists for collaboration among the nation's critical infrastructure providers. The National Infrastructure Protection Plan, the most recent version of which was released in 2013 by DHS, explains this structure.[11] Pursuant to a presidential policy directive,[12] a total of 16 "critical infrastructure sectors" have been identified as being essential to the stability and well-being of the United States. Coordinating councils within each sector are charged with collaboration on security issues.

More importantly, Information Sharing and Analysis Centers, or ISACs, already exist for the aviation, defense industrial base, financial, electricity and other sectors.[13] Their relationship to the newly promoted ISAOs will require clarification. The White House seems to think that current ISACs might constitute the ISAOs under the new order,[14] but that begs the question of what exactly is *new* about the current conceptualization. How will the new ISAOs function with respect to the extant groups? What role is envisioned for the ISAOs that differs from what is currently being done? This is not a critique, so much as a request for clarification that may have to be worked out in the coming months.

Critics are concerned that companies may share private data about individuals that they store or that sharing is really a thinly veiled opportunity for mass data collection or surveillance.

NEW STANDARD-SETTING ORGANIZATION

The order also commands the DHS secretary to "enter into an agreement" with a to-be-determined non-governmental organization to serve as a voluntary standards organization for ISAOs. It remains to be seen whether the administration is trying to distinguish what might otherwise appear as government regulatory activities, perhaps in an attempt to make them more attractive to the private sector.

This instruction also overlooks the central role served to date by the National Institute of Standards and Technology in standard-setting activities. In fact, just two years ago, it was the White House that charged NIST with leading "the development of a framework to reduce cyber-risks to critical infrastructure," dubbed the "Cybersecurity Framework."[15] In light of that directive, NIST released the first version of the framework Feb. 12, 2014, and a draft guide to cyberthreat information sharing in October.[16] What role will NIST continue to play in the process, and how will it relate to any new private standard-setting organization?

LINGERING PRIVATE-SECTOR CONCERNS

The most significant open questions, however, circulate around continuing liability and privacy concerns that are left essentially unaddressed by the order. Although impending legislation may fill the gap left in this area, as discussed at greater length above, certain interest groups continue to be concerned that congressional efforts are also insufficient.

Other questions remain about what the government will do with the information it obtains from the private sector. Some leaders have noted the importance of restoring trust in the government's role in collecting and using information for law enforcement purposes.[17] Section 5 of the order requires the government agencies to coordinate with their privacy and civil liberties officials and calls for regular assessments by such officials.[18]

But assurances of oversight alone have been insufficient in the past, and Congress will bear the responsibility for adequately addressing these concerns.

THE REMAINING NEED FOR LEGISLATION

When considered against the standards for meaningful cybersecurity information sharing, the executive order highlights the need for legislation to establish firm protections and limits on government engagement. This is particularly the case because the new order appears to contemplate government involvement — albeit through participation in voluntary and decentralized private cooperatives — in nearly every sector of business and society.

The currently debated legislation makes extensive government involvement a certainty, but its deferral to the administration on specifics also means that the broad structural outlines present in the executive order will solidify into established mechanisms upon the passage of relevant legislation and regulations.

Thus, significant debate continues about whether the current versions of information-sharing bills and the most recent executive order provide adequate comfort on privacy and liability matters. The onus is upon Capitol Hill to provide more definitive answers, and for that reason its discussions in the coming weeks are important to watch.

NOTES

[1] *See* Cybersecurity and Internet Freedom Act of 2011, S.413, 112th Cong. (1st Sess. 2011), *available at* http://1.usa.gov/1Fkz5oA.

[2] Phishing is a form of "social engineering" whereby potential attackers send emails to individuals in an attempt to get those individuals to divulge sensitive information that will permit the attackers to use that information to attack a company's network.

[3] Andy Greenberg, *CISA Cybersecurity Bill Advances Despite Privacy Concerns*, WIRED, Mar. 12, 2015, http://wrd.cm/1z1JF2O.

[4] Some corporate associations have more recently been voicing support for amendments that they think adequately address such liability concerns. *See* Cory Bennett, *Business Group Launches DC Ad Blitz Backing Cyber Bills*, THE HILL, Apr. 20, 2015, http://bit.ly/1EzXx6n.

[5] *See* Cybersecurity Information Sharing Act of 2015, S.754, 114th Cong. (1st Sess. 2015), *available at* http://1.usa.gov/1cDJ797.

[6] *See* Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (1st Sess. 2015), and National Cybersecurity Protection Advancement Act of 2015, H.R. 1731, 114th Cong. (1st Sess. 2015), *available at* http://1.usa.gov/1EoHR3Y and http://1.usa.gov/1EoHWER, respectively.

[7] *See* Exec. Order No. 13691, 80 Fed. Reg. 9349 (Feb. 13, 2015) [hereinafter Cybersecurity Information Sharing Executive Order], *available at* http://1.usa.gov/1OnFSyi. *See also* White House Press Sec'y, Fact Sheet: Executive Order Promoting Private Sector Cybersecurity Information sharing, (Feb. 12, 2015) [hereinafter Cybersecurity Information Sharing Fact Sheet], *available at* http://1.usa.gov/1G1IkZ9.

[8] *See, e.g.*, Mark L. Krotoski, *Reading recent advances on the information sharing front*, Law360, Feb. 11, 2015, http://bit.ly/1PYMKpe (summarizing "recent government efforts to advance cybersecurity information sharing and identif[ying] further necessary efforts to address liability concerns which remain essential to accomplish the objective"); Mark L. Krotoski & Brock D. Dahl, *NIST Draft Guide Advances the Debate on Cybersecurity Issues*, Morgan Lewis LawFlash Client Alert (Nov. 19, 2014) (update about NIST draft report promoting information sharing), http://bit.ly/1DfKEYn.

[9] *See* Exec. Order. No. 13549, 75 Fed. Reg. 51609 (Aug. 18, 2010), *available at* http://1.usa.gov/1yCxeKF; *see also* Dep't of Homeland Sec., Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive (February 2012), *available at* http://1.usa.gov/1In506o.

[10] Exec. Order. No. 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013), *available at* http://1.usa.gov/1OOPrbx; White House Press Sec'y, Presidential Policy Directive 21 — Critical Infrastructure Security and Resilience, (Feb. 12, 2013), *available at* http://1.usa.gov/1yCyD3F.

[11] *See* Dep't of Homeland Sec., National Infrastructure Protection Plan 2013 (2013), *available at* http://1.usa.gov/1OOQpof.

[12] *See* Presidential Policy Directive 21, *supra* note 10.

[13] For more information, *see* the website for the National Council of ISACs, http://www.isaccouncil.org/home.html.

[14] *See* Cybersecurity Information Sharing Fact Sheet, *supra* note 7.

[15] Exec. Order. No. 13636, 78 Fed. Reg. 11739.

[16] Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* http://1.usa.gov/1ISUB5M; Chris Johnson, Lee Badger and David Waltermire, NIST Special Publication 800-150 (Draft), Guide to Cyber Threat Information Sharing (Draft), Nat'l Inst. of Standards & Tech. (October 2014), *available at* http://1.usa.gov/1zq6t6U.

[17] *See, e.g.*, U.S. Dep't of Justice, Leslie R. Caldwell, Assistant Att'y Gen., Speech at Cybercrime 2020 Symposium (Dec. 4, 2014), *available at* http://1.usa.gov/1HgztnT (noting "a growing public distrust of law enforcement surveillance and high-tech investigative techniques" which "can hamper investigations and cyber security efforts" and the need "to engage the public directly on these issues and to allay concerns").

[18] Cybersecurity Information Sharing Executive Order, *supra* note 7.

Mark L. Krotoski (L) is a partner in the litigation, privacy and cybersecurity, and antitrust practice groups in the Silicon Valley office of **Morgan, Lewis & Bockius**. He can be reached at mkrotoski@morganlewis.com. **Brock Dahl** (R), an associate in the firm's litigation and privacy and cybersecurity groups, is a resident in the Washington office. He can be reached at bdahl@morganlewis.com. The views expressed are those of the authors and are not necessarily those of the firm or any of its clients.