The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 10 October 2011

Congress Evaluates The Administration's Cybersecurity Proposal – Several Elements May Affect U.S. Businesses

Megan L. Brown, Julie A. Dunne, Nova J. Daly and Scott Weaver

WILEY REIN LLP

After more than a year of interagency coordination and discussions the Obama administration released in May 2011 its legislative proposal aimed at overhauling the nation's cybersecurity policies. The administration's plan, similar to several proposals introduced in the Senate, includes provisions that mandate the public disclosure of data breaches, regulate the operation of critical information infrastructure, and impose standards to secure government computer systems. The proposal, if enacted in whole or in part, could have a major impact on U.S. and foreign businesses that are part of the nation's information infrastructure; provide information technology, cybersecurity services or equipment to businesses or the government; store sensitive data; or have any involvement in the nation's growing information economy. This fall, Congress is expected to continue evaluating the administration's cybersecurity proposal and consider other pending legislation.

This article summarizes some of the key areas of interest, concern, and opportunity for the business community as it pertains to cybersecurity. Congress, particularly the Senate, has been engaged in various cybersecurity legislative proposals for the last year, as described in greater detail below. Stakeholders can expect to see hearings in the fall on a wide range of cyber-related topics, such as data breach notification, data security and infrastructure protection. In October, the House Cyber Task Force will provide its response to the administration's proposal and possibly its own legislative framework. As part of that response, stakeholders can expect to see momentum build toward legislation addressing narrow cybersecurity issues, such as data breach and privacy. While the outlook for comprehensive cybersecurity legislation is mixed in the near term, the administration's proposal along with congressional proposals, particularly in the Senate, could form the basis for congressional action. This would certainly be the case should the United States come under a damaging cyber attack. In either case, the administration proposal will certainly form the basis for debate on the proper policy response to the cybersecurity threat.

The Administration's Cybersecurity Proposal

The administration's cybersecurity proposal covers several areas including:

Megan Brown *is a Partner at Wiley Rein and has significant litigation, appellate and regulatory experience before state and federal courts and agencies across the country. Ms. Brown has developed particular expertise in litigation involving federal, state and local regulation raising complex constitutional, administrative law and statutory issues. In this capacity, Ms. Brown has been involved in many cases of first impression involving federal preemption at all levels of the federal judiciary. She regularly defends corporations in all phases of complex civil litigation in both federal and state courts and counsels clients about their rights and obligations under a variety of federal statutes, including the federal Communications Act, the Federal Arbitration Act and the Freedom of Information Act, as well as the U.S. Constitution. She may be reached at (202) 719-7579.*

Julie Dunne *counsels and represents government contractors on a broad range of contract administration and dispute matters, including bid protests and contract dispute litigation. She is a former associate general counsel at the Department of Homeland Security (DHS) and senior advisor at the Department of Commerce's Bureau of Industry and Security. Ms. Dunne also provides advice and counsel on a broad range of issues related to homeland security. She may be reached at (202) 719-7593.*

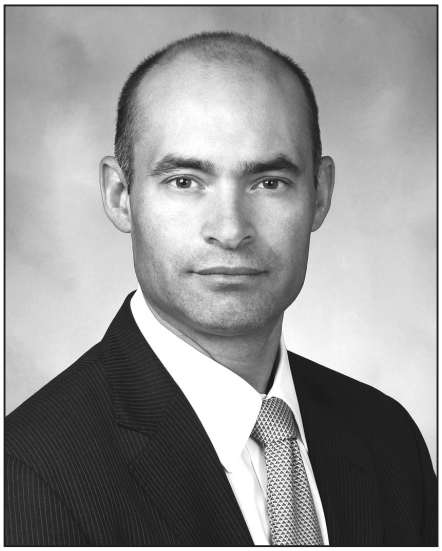
Nova Daly, *an international investment and trade policy expert, has held senior leadership positions at the U.S. Departments of the Treasury and Commerce, the White House and the U.S. Senate. Drawing on his experience in the management, development and implementation of U.S. economic and national security policies and programs, he provides both high-level insight and deep operational expertise to help clients navigate the policy and regulatory environment surrounding cross-border business activities, especially through the Committee on Foreign Investment in the United States (CFIUS). He may be reached at (202) 719-3282.*

Scott Weaver, *an experienced senior-level Capitol Hill staffer and public policy advocate, assists clients to advance their business interests in Washington, DC. Throughout his career, he has worked closely with Members of Congress on both sides of the aisle, as well as Committee staff and government agencies. He may be reached at (202) 719-3273.*

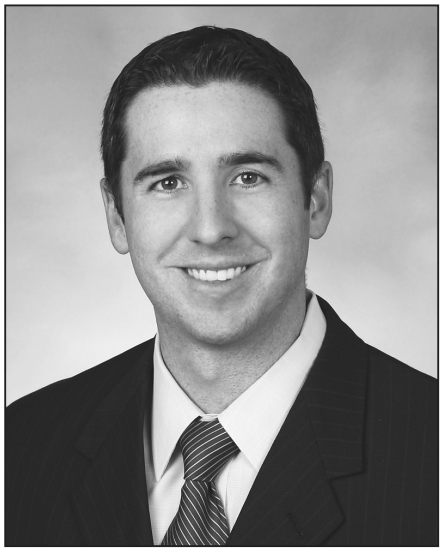
Please email the authors at mbrown@wileyrein.com, jdunne@wileyrein.com, ndaly@wileyrein.com or sweaver@wileyrein.com with questions about this article.

Megan L. Brown

Julie A. Dunne



Nova J. Daly



Scott Weaver

• Standardization of data breach notification requirements at the federal level.

• Toughening penalties for cybercrime.

• Direction and delegation of authority to the Department of Homeland Security (DHS) to: (1) protect civilian federal computer systems; (2) regulate critical information infrastructure; (3) implement cyber-incident response and cyber-threat detection and prevention; and (4) facilitate public-private-sector information sharing.

• Federal Information Security Management (FISMA) reform to formalize DHS's role in securing federal systems and to focus on operational security.

• Federal civilian personnel authorities to facilitate hiring cybersecurity professionals including activation of a government-wide information technology exchange program.

• Prohibition on non-federal requirements for specific locations for data centers.

The business community should take particular note of several of the administration's cybersecurity legislative provisions – specifically, data breach notification, proposals that delegate new authority to DHS to regulate critical infrastructure, and enhanced DHS authorities to secure federal computer systems.

Data Breach Notification and Related Proposals

The administration's proposal on data breach notification would establish a national reporting framework for data breach incidents and authorize the Federal Trade Commission (FTC) to implement the reporting requirements.

• The proposal would apply to entities that handle "sensitive personal identifying information" for more than 10,000 individuals in a 12-month period.

• Subject to certain exceptions, covered business entities would be required to notify individuals should there be a security breach of personally identifiable information.

• The proposal also would require certain business entities to notify designated law enforcement and national security authorities of information related to cybersecurity incidents, threats and vulnerabilities.

• A violation of the data breach notification requirements would be considered an unfair or deceptive act or practice under the Federal Trade Commission Act and would be enforced by the FTC and state attorneys general.

• The proposal provides for coordination of activity, such as rulemaking and enforcement, with the Federal Communications Commission (FCC) when the activity relates to customer proprietary network information.

• The proposal has a narrow preemption provision that generally supersedes state law relating to notification of breaches of computerized data.

As with other elements of the administration's proposals, many of the details would be committed to the discretion of the relevant agencies and explained in subsequent regulatory proceedings.

The proposal's data breach notification requirements were met with skepticism at a hearing in June before the House Homeland Security Committee Subcommittee on Cybersecurity. One congressman characterized the proposal as a public "name-and-shame" framework to promote cybersecurity goals. Rep. Michael McCaul (R-TX) described the administration's approach as counterproductive, and one witness argued that mandatory public notification of data breaches would discourage organizations from conducting proper cyber-security investigations and monitoring, for fear that they would discover and be forced to publicly announce a breach.

Given the burdens associated with any notification regime and the concomitant desire for certainty, the specific requirements of any data breach notification regime will be critical and are worth monitoring. Equally noteworthy will be

efforts to establish national notification requirements, along with their preemptive effect on additional or different state regimes.

Designation, Regulation, and Protection of Critical Infrastructure

The administration's proposal would give DHS a lead role and significant new regulatory authority to secure what the proposal refers to as "critical infrastructure" against cyber threats. These proposals, if enacted, could have significant consequences for a variety of U.S. industries and businesses. The proposal would charge DHS with filling in substantial interpretive and policy gaps related to critical infrastructure.

- Covered critical infrastructure operators, defined or identified by DHS, would be required to develop a plan to address cyber-threats and have a third-party auditor, approved pursuant to DHS criteria, assess the plan. The plan would have to "be signed and attested by an accountable corporate officer" and be available for evaluation by DHS.
- The proposal would require annual certifications that cyber-threat plans have been developed and are being implemented. The proposal also would require disclosure of "high-level summaries" of the plans and prompt notification to the DHS Secretary of "any significant cybersecurity incident."
- If the Secretary finds that an entity designated as covered critical infrastructure is not sufficiently addressing the cyber risk, the Secretary may enter "discussions" with the owner or operator and, if unsuccessful in resolving the concern, may "issue a public statement that the covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks."

The process for designating "covered critical infrastructure" subject to regulation would be developed and implemented by DHS. While there are many unanswered interpretive questions, it seems likely that the term could include communications service providers, Internet Service Providers (ISPs), various utilities, the nation's energy grid, and even some manufacturing sectors.

Important questions are being asked about the designation and regulation of critical infrastructure. DHS would be given substantial discretion to craft and impose potentially onerous regulatory requirements on what entities it deems to be critical infrastructure, but the administration's proposal does not provide a great deal of specific guidance about what criteria would justify such a designation. Accordingly, a key issue at a June 2011 hearing on the proposal before the Senate Judiciary Committee Subcommittee on Crime and Terrorism was the definition of critical infrastructure and what entities, industries and functions would be covered. Subcommittee Chairman Sen. Sheldon Whitehouse (D-RI) specifically asked administration witnesses (from the Departments of Justice, Homeland Security, and Commerce) whether they believed ISPs would be classified as operators of covered critical infrastructure and thereby subject to potentially sweeping DHS regulatory authority. The witnesses noted that this designation would take place through a rulemaking process, making specific results hard to predict. But the Acting Deputy Under Secretary for National Protection and Programs Directorate at the Department of Homeland Security (the component that would be charged with making the designation) was confident that ISPs would indeed be classified as critical infrastructure and, therefore, be the targets of new cyber-security regulations.

The administration's proposal to give the Secretary of DHS sweeping authority to create and implement a framework both for the designation of critical infrastructure, and the obligations that are attributed to such designation once made is consistent with provisions of the Cybersecurity and Internet Freedom Act (S. 413), which is co-sponsored by Senators Joseph Lieberman (I-CT), Olympia Snowe (R-ME) and Tom Carper (D-DE), chairman, ranking member and member of the Senate Homeland Security and Governmental Affairs Committee, respectively. In a published op-ed in the July 8, 2011 edition of *The Washington Post* the Senators urged Congress to act on cybersecurity legislation and touted their proposal to "give DHS statutory authority to work with industry to identify and evaluate the risks to the country's most critical cyber-infrastructure." Their legislation would call on DHS "cyber experts" to review corporate protection plans and immunize from liability companies that are in compliance with their approved plans.

Given the discretion and authority that would be vested in DHS, ISPs and companies in the communications, information, technology, energy and any other sectors vital to the U.S. economy should monitor closely these proposals as they make their way through Congress. Of particular significance would be opportunities to influence or obtain guidance about the criteria for designation as critical infrastructure and the obligations that would follow such a designation.

Protection of Federal Computer Systems

The Administration's proposal also would provide DHS with additional tools to protect federal systems, which may be of interest to government contractors and others working with the federal government. For example, for purposes of protecting federal computer systems, DHS would be authorized to operate "consolidated intrusion detection, prevention, or other protective capabilities and the use of countermeasures…". In addition, DHS would be authorized "to acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on federal systems and to deploy countermeasures…" provided such activity is consistent with a privacy and civil liberties framework and the DHS Secretary makes a number of certifications.

This proposal has been met with some skepticism, including from those who want the government to be able to do more to address threats to private systems. Some participants in a June hearing before the Senate Judiciary Committee Subcommittee on Crime and Terrorism expressed interest in developing techniques for the government to legally intrude in privately-owned information systems in an emergency, perhaps by creating a program for infrastructure operators to preauthorize this sort of intervention in their systems. No doubt this type of intervention would be met with skepticism from the civil liberties community as well as the business community. Government contractors and others doing business with the federal government should pay close attention to proposals concerning the protection of federal data and systems.

Hill Scrutiny Identifies Emerging Issues, Disputes And Opportunities

Since the administration released its cybersecurity legislative proposal, Senate and House committees and subcommittees have held a number of hearings. To date, cybersecurity has not been a partisan issue, though policy fault lines are emerging as proposals take shape.

- The Senate Committee on Home-

land Security and Government Affairs held a hearing on May 23, 2011, soon after the administration released its proposal. It was chaired by Sen. Lieberman, who was generally supportive of the Administration's efforts, though he expressed concern that the Administration's proposal did not create a White House Office of Cybersecurity with a Senate-confirmed director and that it did not address the President's authority to act in the event of a cyber emergency.

• The Senate Judiciary Committee Subcommittee on Crime and Terrorism held a similar hearing on June 22, 2011 to evaluate the Administration's proposal. It was chaired by Senator Sheldon Whitehouse who, while generally receptive to the Administration's proposals, appeared interested in the definition of critical infrastructure.

• The House Homeland Security Committee Subcommittee on Cybersecurity held a hearing on June 27, 2011, to evaluate the Administration's proposal. This hearing, chaired by Rep. Dan Lungren (R-CA), turned a more critical eye on aspects of the proposal and focused on the breach notification obligations and explored the possibility of using the private insurance market to mitigate cybersecurity concerns in the private sector.

An Uncertain Legislative And Regulatory Environment Creates Risk and Opportunity

While it is clear that both the White House and the Congress are eager to take some action to address the growing cyber threat, a consensus approach has yet to emerge. The resulting debates and proposals generate substantial regulatory uncertainty, but also present opportunities to shape what could be a new frontier of regulation and public-private partnerships aimed at many of the country's core businesses and technologies.

Critical questions will focus on how to classify and protect critical infrastructure, how to balance security against privacy interests, and how to put the right incentives in place to encourage private entities to take necessary steps to secure our nation's infrastructure, data, and technology. In particular, corporations are rightly concerned about the security and confidentiality of sensitive business information and risk assessments. Adequate protection of information made available in the context of government disclosures and dialogue is necessary to promote successful public-private partnerships on cybersecurity. Finally, it will be important to clarify the proper role for state activity and the preemptive effect of any federal legislation or regulations in any and all of these areas. This will help ensure certainty and national uniformity of companies' cybersecurity obligations.

Though many stakeholders believe that some government intervention is necessary to protect critical infrastructure from cyber threats, Congressional discussions identified two competing approaches: (1) direct action through regulation and (2) indirect action through the creation of market incentives. One example of possible incentives is the insurance market. Before the House Homeland Security Committee Subcommittee on Cybersecurity, Larry Clinton, President and CEO of the Internet Security Alliance, which has been active on cybersecurity issues, argued that the Administration's approach does not allow enough flexibility to counter effectively modern cyber threats. According to Mr. Clinton, cybersecurity legislation could encourage the development of a cybersecurity insurance market which would achieve, through market forces, the administration's cybersecurity goals without burdensome regulation. To make this proposal a reality, Mr. Clinton suggested that the government should establish a revolving fund, as it did to stimulate the formation of the crop and flood insurance markets, and that it should facilitate the public release of actuarial information that is currently kept private. Whether there is an appetite among policy makers for such an initiative remains to be seen..

While much Congressional attention is focused on big picture budget issues, there are many key decision makers who want to make producing cybersecurity solutions a priority. Should significant cyber attacks occur in the coming months, cybersecurity issues could come into focus rather quickly on the Congressional agenda. In the meantime, the Administration's proposal, pending Senate proposals, and the upcoming House Cybersecurity Task Force report will lay the groundwork for how Congress and the Executive branch will respond to the ever-growing cybersecurity threat. Thus, cybersecurity legislation bears watching in the months ahead.

* * *

Cybersecurity issues cut across industries and regulatory agencies. Wiley Rein, with core practice groups spanning the federal regulatory landscape and expertise in emerging technologies, privacy regulation, government contracting, as well as insurance and risk management, is well-positioned to help large and small businesses understand and take advantage of these proposals and any legislation or regulation that emerges in the area of Cybersecurity and Network Security. Wiley Rein has a deep bench of practitioners with experience before the spectrum of federal regulators, as well in government at the Departments of Homeland Security, Defense, Justice and Commerce.