Bloomberg Law Reports® Technology Law

White House Proposes Cybersecurity Legislation

Contributed By: Evan D. Wolff, Mark W. Menezes and Aaron P. Simpson, Hunton & Williams LLP

On May 12, 2011, the Obama administration announced a comprehensive cybersecurity legislative proposal in a letter to Congress. The proposal, which is the culmination of two years of work by an interagency team made up of representatives from multiple departments and agencies, aims to improve the nation's cybersecurity and protect critical infrastructure. If enacted, this legislation will affect many government and private-sector owners and operators of cyber systems, including all critical infrastructure, such as energy, financial systems, manufacturing, communications and transportation. In addition, the proposal includes a wide-reaching data breach notification law that is intended generally to preempt the existing state breach laws in 46 states plus Washington, D.C., Puerto Rico and the U.S. Virgin Islands.

Homeland Security Provisions

According to the administration, the proposed new cybersecurity legislation would strengthen privacy and protect the nation's critical infrastructure by providing the federal government with tighter oversight of critical infrastructure and by mandating that critical infrastructure operators develop frameworks for addressing cyber threats. These frameworks would be based on federally developed, risk-based standards tailored to each system's specific needs and circumstances. The proposal — which takes a cue from the existing federal program established four years ago to protect high-risk chemical facilities from terrorist attacks — would allow flexibility to private industry to develop their own approach to cybersecurity by working cooperatively with the federal government.

Under the proposal, the Department of Homeland Security ("DHS") would be required to work cooperatively with private industry to detect vulnerabilities to cyber attack. These provisions would require DHS to develop, in coordination with industry, a list of covered critical infrastructure facilities and a set of risk-based standards for those covered facilities. A covered critical infrastructure sector is selected based on relative interdependencies and components of covered facilities, relative size and "potential for the incapacity or disruption of the entity, a system or asset it operates or a service it provides to cause severe, negative consequences to national security, national economic security and national public health and safety." DHS would then establish risk-based tiers for the covered facilities based on threat, vulnerability and consequence of a cyber attack. Under the provisions, covered facilities would be mandated to develop cybersecurity plans to meet the risk-based standards. A covered facility also would be required to make a high-level overview of the plan publicly available. The plan would be required to be signed by a responsible

corporate officer, audited by a third party and certified annually by DHS or the Securities and Exchange Commission ("SEC"). DHS is empowered, as a means of enforcement, to publicize circumstances where a covered facility is not sufficiently addressing cybersecurity risk.

The proposal does not specifically mention types of infrastructure to be covered, such as energy or electric facilities, nor does it specifically authorize a role for the Federal Energy Regulatory Commission ("FERC") or the Department of Energy. The proposal does establish a collaborative process for agencies and regional councils to participate in the identification of critical infrastructure and authorizes the agencies with authority over such infrastructure to promulgate rules. The Office of Management and Budget ("OMB") can exempt certain infrastructure if sufficient regulation is already in place. In an effort to coordinate the nation's federal information security policy, the proposal would also grant DHS primary authority for information security across the federal government's civilian computers and networks, including formalizing DHS's responsibility for implementation of the Federal Information Security Management Act ("FISMA").

Finally, the proposal also seeks to address privacy protection issues. DHS and other agencies, with input from civil liberties experts and with oversight and approval from the attorney general, would be required to develop privacy and civil liberties procedures for information that they acquire or use. Companies that seek to share information with the government would need to make reasonable efforts to remove any identifying information unrelated to cyber threats. No information obtained could be used except as authorized. The goals of these procedures would be to: (i) minimize the impact on privacy and civil liberties; (ii) limit the collection and use of information and records to carry out DHS's responsibilities; (iii) safeguard individually identifiable information from unauthorized access or acquisition; and (iv) protect the confidentiality of individually identifiable information to the greatest extent practicable and require recipients of such information to disclose it only to protect against cybersecurity threats.

National Data Breach Notification Law

In addition to the Homeland Security issues, the proposal also calls for a lengthy and detailed national data breach notification law that would generally preempt existing state breach notification laws. The proposed breach law would require any "business entity" that uses, accesses or collects "sensitive personally identifiable information" about more than 10,000 individuals during a 12-month period to notify the individuals following a "security breach." The proposal contains many important provisions that will serve to both clarify and expand existing breach notification obligations. These provisions include:

• *Definition of Sensitive Personally Identifiable Information ("SPII")*: SPII is defined as "any information or compilation of information, in electronic or digital form that includes" (i) an individual's first and last name or first initial and last name in combination with two of the following: A home address or telephone number, mother's maiden name or birth date; (ii) a nontruncated Social Security number, driver's license number, passport number or government-issued unique identification number; (iii) biometric data; (iv) a unique account identifier such as a credit card number or routing code; or (v) any combination of an individual's first and last name or first initial and last name, a unique account identifier, or any security code, access code or password, or a source code that could be used to generate such codes or passwords. This definition of SPII addresses many of the definitional issues that arise under the existing state law framework and, if passed, will greatly expand breach notification obligations for all companies subject to the law.

• *Harm Threshold*: The proposal requires business entities to notify affected individuals whose SPII "has been, or is reasonably believed to have been,

accessed or acquired, unless there is no reasonable risk of harm or fraud to such individual." The notification threshold contained in the proposal is similar to existing state law, but the inclusion of the harm threshold at the national level would serve to streamline the breach notification process, as current state laws conflict with respect to the presence of a harm threshold. In some cases, under existing state breach laws, notification is required even if there is no reasonable risk of harm as a result of an information security incident.

• *Risk Assessment*: The proposal requires business entities to perform a detailed risk assessment to demonstrate that no risk of harm exists and must notify the FTC within 45 days after discovery of a breach of (i) the results of the risk assessment and (ii) the decision to invoke the risk assessment exemption. The risk assessment must contain "logging data" for the six months prior to the submission of the risk assessment that contains specified information regarding communications and logs.

• *Timing*: The proposal requires business entities to notify affected individuals without unreasonable delay, which means in 60 days or less unless (i) the business entity can demonstrate to the FTC that additional time is reasonably necessary or (ii) a federal law enforcement agency determines that the notification would impede a criminal investigation or national security activity. Notices to the entity designated by the secretary of Homeland Security, as described in more detail below, must occur either (i) 72 hours before notification is sent to affected individuals or (ii) 10 days after discovery of the security breach, whichever is earlier.

• *Other Notification Requirements*: In addition to the notice required to individuals, a business entity must notify the media in any state where more than 5,000 individuals are impacted by the breach. Business entities will also be required to notify "an entity designated by the Secretary of Homeland Security" if the security breach (i) affects more than 5,000 individuals; (ii) involves a database containing the SPII of more than 500,000 individuals; (iii) involves a database owned by the federal government; or (iv) primarily involves the SPII of federal employees or contactors involved in national security or law enforcement.

• *Enforcement*: The national data breach notification law would be enforced under the FTC Act as an unfair or deceptive act or practice in commerce. The law may be enforced by the FTC "irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the [FTC] Act." The law also provides enforcement authority to state attorneys general to enjoin any violations of the law, enforce compliance with the law or impose civil penalties of up to $1,000 per day for each affected individual, up to a maximum of $1,000,000 per violation unless the conduct is "willful or intentional," in which case there is no limit mentioned in the proposal.

• *Preemption*: The law contains a preemption provision that states that it "shall supersede any provision of the law of any State, or a political subdivision thereof, relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data" apart from any state laws that require victim protection assistance.

• *Scope*: The proposal excludes from coverage "covered entities," "business associates" and "vendors of personal health records" subject to the breach notification requirements of the Health Information Technology for Economic and Clinical Health ("HITECH") Act.

Outlook

Undoubtedly, this proposal will be thoroughly discussed in Congress, against the backdrop of numerous bills focused on cybersecurity infrastructure and privacy. These include the "Homeland Security Cyber and Physical Infrastructure Protection Act of 2011" introduced by Rep. Bennie Thompson (D-MS); the "Secure

High-voltage Infrastructure for Electricity from Lethal Damage Act" introduced by Rep. Trent Franks (R-AZ); and Sen. Lieberman's (I-CT) "Cybersecurity and Internet Freedom Act of 2011." The Senate Energy and Natural Resources is also considering Sen. Bingaman's (D-NM) "Critical Electric Infrastructure" Discussion Draft. Additionally, comprehensive privacy bills such as the "Commercial Privacy Bill of Rights Act of 2011" by Senators Kerry (D-MA) and McCain (R-AZ) have been introduced as well as separate bills addressing online tracking introduced by Senator Rockefeller (D-WV) and Representative Speier (D-CA). The administration's proposal incorporates elements already contained in some of these existing bills on cybersecurity and will undoubtedly be the source of further hearings. Interestingly, Deputy Undersecretary Phil Reitinger, DHS's top cybersecurity and lead interagency official resigned shortly after the Administration's release of its proposal. Mr. Reitinger played a key role in developing the Administrations' policy and the Administration must now replace him with someone who can explain the legislation to the several Congressional committees. If the proposal is eventually enacted, there will need to be extensive additional rulemaking by the FTC, DHS and other agencies to implement the legislation.

Evan D. Wolff serves as director of Hunton & Williams LLP's homeland security practice and can be reached at ewolff@hunton.com. Mark W. Menezes is co-head of the firm's regulated markets and energy infrastructure team and can be reached at mmenezes@hunton.com. Aaron P. Simpson is a partner in the firm's privacy and data security practice and can be reached at asimpson@hunton.com.