wiley

ARTICLE

Get Ready for Cybersecurity Laws

Law360
August 10, 2011

With Washington's attention focused on the debt ceiling debate, an ominous warning from Defense Secretary Leon Panetta went largely unnoticed. During his Senate confirmation hearing last month, Panetta told lawmakers that the "next Pearl Harbor we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems."

Chairman Darrell Issa of the House Oversight Committee also recently said, "the number of cyber incidents affecting federal agencies shot up 39 percent in 2010." For all the partisan acrimony that divides elected officials, the Obama administration and Congress appear to agree the cyber-threat must be addressed. But how to address it remains an open question.

On May 12, the administration released its proposal for legislation to overhaul cybersecurity regulations. Sen. Joe Lieberman, D-Conn., chairman of the Senate Homeland Security and Government Affairs Committee and co-sponsor of the Cybersecurity and Internet Freedom Act (S.413), welcomed the administration's proposal. Meanwhile, Larry Clinton, president and CEO of the Internet Security Alliance has objected to the administration's approach, citing a lack of flexibility to effectively counter cyber-threats. Instead, Clinton has suggested developing a cybersecurity insurance market.

The administration's proposal focuses on mandating the public disclosure of data breaches, regulating the operation of the nation's critical information infrastructure, and imposing standards to secure government computer systems. If enacted, the overhaul would have a major impact on organizations involved in the nation's growing information economy.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Telecom, Media & Technology

In its current form, adoption of the administration's cybersecurity proposal includes provisions that would affect government contractors in a number of areas, namely:

- Data breach notification standardization at the federal level.
- Cybercrime statutory amendments to toughen penalties for cybercrime.
- Department of Homeland Security (DHS) authorities: (1) to protect civilian federal computer systems; (2) to regulate critical information infrastructure; (3) to implement cyber incident response and cyber threat detection and prevention; and (4) to facilitate public-private sector information sharing.
- Federal Information Security Management (FISMA) reform to formalize DHS's role in securing federal systems and to focus operational security.
- Personnel authorities to facilitate hiring cybersecurity professionals including activation of a government-wide information technology exchange program.
- Prohibition on nonfederal requirements for specific locations for data centers.

The administration's proposal gives DHS the lead role and significant new regulatory authority to secure "covered critical infrastructure" from cyber threats. The DHS Secretary is directed "to assist in national efforts to mitigate communications and information technology supply chain vulnerabilities to enhance the security and resiliency of federal systems and critical information infrastructure." There is no specific direction on how the secretary is to implement this provision. The proposal also includes a "special provision for federal contracts" in the title establishing DHS' regulatory framework for protection of critical infrastructure.

In addition, the proposal provides DHS with tools to protect federal systems, including the authorization to operate "consolidated intrusion detection, prevention, or other protective capabilities and ... countermeasures ..." DHS would also 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 ..."

These proposals, if enacted, could have significant consequences for sectors such as the defense industrial base and telecommunications. 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. If the secretary finds the covered critical infrastructure is not sufficiently addressing the cyber risk, the secretary may enter "discussions" with the owner or operator and, ultimately, the secretary may "issue a public statement that the covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks."

Finally, the administration's proposal would establish a national reporting framework for data breach incidents and provide the Federal Trade Commission regulatory authority to implement the reporting requirements. The new regulations would apply to entities that handle more than 10,000 individuals' sensitive, personally identifiable information during any 12-month period.

Since the administration released its cybersecurity proposal, there have been a number of hearings in the Senate and the House. Sen. Lieberman, who has sponsored his own legislation (S.413) along with Sens. Susan Collins, R-Maine, and Tom Carper, D-Del., welcomed the administration's proposal as a basis for negotiations. The House established a GOP task force to evaluate the administration's proposal and report to House leadership in October 2011. Given this level of activity, stakeholders should look for increased congressional movement on cybersecurity legislation this fall.