National Law Journal

December 10, 2012

Cybersecurity standards for owners of critical infrastructure

By Mark W. Menezes, Frederick R. Eames and Evan D. Wolff

On November 15, the U.S. Senate declined to approve S. 3414, the Cybersecurity Act of 2012, introduced by senators Joe Lieberman (I-Conn.) and Susan Collins (R-Maine), and supported by the Obama administration. The proposed legislation would have set voluntary cybersecurity standards for owners of the nation's critical infrastructure, such as gas pipelines, utilities and banks. The bill also would have authorized companies and the government to share information about online threats. Most supported the information-sharing provisions of the proposed legislation, but many businesses were concerned that even voluntary standards could impose new liabilities upon them and that the act did not provide adequate liability protection to address those risks.

In the absence of cybersecurity legislation, the Obama administration now is considering taking action through an executive order. Making a final plea for S. 3414, Lieberman argued that an order would be of grave consequence to businesses: "[An executive order] will not be able to offer the private-sector owners the liability protection our bill offers for voluntarily adopting cybersecurity practices developed jointly by the private sector and the government. Without such protections, the private sector will be exposed to substantial liability once the Executive Branch begins to promulgate industry-wide standards."

Failing to get the Cybersecurity Act passed, administration officials have drafted an executive order that would encourage companies to meet cybersecurity standards. As with S. 3414, similar concerns are being expressed about the absence of liability protections in the draft order, and the potential impact of a final order upon critical infrastructure owners is subject to considerable debate and uncertainty.

Are critical infrastructure owners worse off under an executive order instead of S. 3414, as Lieberman argues? If an executive order is issued, what new liabilities might businesses face if a company's critical infrastructure is compromised as a result of a cyberintrusion?

Under current law, critical infrastructure owners and operators may be liable for damages that others experience resulting from a cyberattack on their systems. This will depend on a variety of case-specific facts — e.g., whether the company exercised reasonable care in protecting its systems, whether it had notice of a potential vulnerability, whether it had a direct (e.g., customer) or only indirect relationship with the plaintiff, whether contractual obligations may apply,

whether sector-specific standards (such as the Federal Energy Regulatory Commission's Critical Infrastructure Protection standards) may apply and the applicability of state laws.

The original version of S. 3414 would have allowed the U.S. Department of Homeland Security (DHS) to create mandatory cybersecurity compliance standards for each critical infrastructure sector. S. 3414 was revised to make these cybersecurity standards voluntary, providing incentives for participation, including limited liability protection. Yet some felt even these voluntary standards could set the legal standard of care for critical-infrastructure cybersecurity, thus potentially compelling compliance. Some businesses also expressed concerns that the liability protections included in the proposed legislation were too limited because, among other reasons, they would not apply to an incident not identified by an assessment conducted under the statute, did not address liability for substantial consequential damages that could arise from a cyberattack, and would preclude punitive damages only in limited circumstances.

A draft of the executive order now under consideration by the Obama administration would institute a voluntary cybersecurity-standards structure for critical infrastructure similar to S. 3414's, but without liability protection. As a discussion paper accompanying the draft order notes, "Liability protection requires statutory authority; therefore, the Executive Order cannot establish such an incentive." The draft executive order directs the U.S. Department of Commerce to have the National Institute of Standards and Technology coordinate development of a cybersecurity framework. The DHS would invite critical infrastructure owners and operators to "participate in a voluntary program to encourage the adoption" of the framework. Sector-specific agencies would report to the president on their authorities to regulate the cybersecurity of critical infrastructure, and after DHS review would be encouraged to propose regulations within a year. The executive order has the potential to create additional liability for companies, in addition to the concerns noted above about any voluntary standards morphing into a legal standard of care. First, as with S. 3414, the executive order should result in enhanced information sharing between the government and private sector for those private companies that choose to participate. While this appears to be a positive development, it presents difficulties for private companies, as they will be expected to have the sophistication and ability to respond swiftly to such information and warnings. Not responding, whether due to lack of a technological solution, a lack of resources or differing assessments of the threat's gravity, may put private companies in a worse liability position as they will have demonstrable actual knowledge of the threat and may be seen as not adhering to the standards.

Second, there may be some private companies that choose not to participate in the voluntary standards. These companies will certainly not receive the information from the government, but if victimized by a threat may still need to contend with the voluntary standards, particularly if adherence to such standards could be argued to have nullified or mitigated the threat. In addition, insurers may rely on the standards in evaluating or underwriting polices, and regulatory bodies may use them when evaluating indirect action, such as disclosure obligations.

The government has looked before at the issue of liability protection for critical infrastructure and provided what many believe is a good solution in the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, known as the SAFETY Act. The SAFETY Act authorizes the DHS to grant significant liability protections to entities that sell or use qualified products and

services to protect against an "act of terrorism." The significant protections of the act — including caps on damages to the company's insurance coverage, a bar on punitive and other noncompensatory damages and the ability to use the government contractor defense in litigation — have been applied to a very broad range of products and services including cybersecurity products and services. Thus, the SAFETY Act could be used as a tool to mitigate some of the liabilities that may arise from a final executive order, but a real question remains regarding the extent of this coverage and an understanding of what a triggering event is.

If an executive order proceeds, information sharing-only legislation — an idea many businesses preferred to a more comprehensive bill — could be a beneficial step. Through the legislation, Congress can authorize the types of liability protections that not only will protect companies who are collaborating with the government and each other to enhance cybersecurity, but also will encourage greater information sharing and increased security.

Mark W. Menezes is co-head of Hunton & Williams' regulated markets and energy infrastructure team and can be reached at mmenezes@hunton.com. Frederick R. Eames is a partner in that team. He can be reached at feames@hunton.com. Evan D. Wolff serves as director of the firm's homeland security practice and can be reached at ewolff@hunton.com.