SMITH ANDERSON
expectexcellence®

WILL THE CYBERSECURITY FRAMEWORK CREATE A NEW STANDARD OPERATING PROCEDURE FOR BUSINESSES?

05.21.2014

On February 12, 2013, President Barack Obama issued Executive Order 13636 (EO 13636) entitled "Improving Critical Infrastructure Cybersecurity."[1] EO 13636 noted the importance of cybersecurity for the nation's security and economy and directed the National Institute of Standards and Technology (NIST) to create the **Cybersecurity Framework** (the Framework) for critical infrastructure.[2] On February 12, 2014, NIST released the Framework.[3] The Framework is the result of a public-private collaboration with 3,000 individuals and organizations rather than the creation of Washington regulators.[4] The Framework is essentially a guidebook of risk-based principles and practices for all businesses to manage cybersecurity threats. It is not unique to critical infrastructure industries.

At the present time compliance with the Framework is not required, as the Framework is not an act of Congress. Also, EO 13636 directed NIST to create the Framework expressly for critical infrastructure. However, the Framework could be applied by *any* organization. The Framework has three parts to assist organizations in managing cybersecurity risks: the Framework Core, the Framework Profile and the Framework Implementation Tiers.[5] Together, they provide a strategic way to identify activities and outcomes, create goals and measure progress. The Framework is intended to be flexible and molded to suit organizations of a variety of sizes and from a variety of industries.

While voluntary, businesses should pay attention to the Framework, even those outside of "critical infrastructure." There are at least three reasons to be mindful of the Framework:

1. EO 13636 called for various federal government agencies to provide incentives to companies using the Framework. Currently, the United States Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security, is providing non-monetary incentives, including guidance on how to implement the Framework.[6] Other incentives, including monetary ones, are being considered and could become available.[7]
2. The Framework provides a "best practices" roadmap for cybersecurity. As such, it might be used as evidence in court of what a company *should have done* prior to a cybersecurity or data breach. Because the Framework is not a "one size fits all" solution, there are theoretically best practices that could apply to any company. Failure to implement the Framework could be used as evidence of fault in the event of a cybersecurity incident.[8]
3. Although the Framework is currently voluntary, in the future federal and state governments could link compliance with the Framework to grants, contracts and regulated industries. In the private sector, insurance companies might tie premiums to compliance with the Framework.[9] Thus, the Framework may become mandatory in practice, even if legally voluntary.

Cybersecurity threats are on the rise. Companies of any size and from any sector could be the next target. The Framework should be reviewed and considered carefully by any company that holds data. The availability and flexibility of the Framework lends itself to being applied if there is a government investigation or litigation arising out of a data breach. Aside from the potential use in litigation, implementation of the Framework could put your company ahead of the curve to receive potential incentives and if the Framework becomes mandatory in practice.

---

[1] Exec. Order No. 13,636, 78 Fed. Reg. 33 (Feb. 19, 2013).

[2] *Id.* §§ 1, 7.

[3] Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity.

[4] Wyatt Kash, *Why Businesses Can't Ignore US Cybersecurity Framework*, Info. Week (Feb. 14, 2014).

[5] Framework, *supra* note 3, at 1, 7-12.

[6] *Critical Infrastructure Cyber Community Voluntary Program*, US-Cert, (last visited April 15, 2014).

[7] Chris Strohm, *Obama Cybersecurity Plan Seen Lacking Perks for Business*, Bloomberg (Feb. 11, 2014),

[8] Kash, *supra* note 4.

[9] Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, The White House Blog (Aug. 6, 2013, 11:04 AM).

PROFESSIONALS

Jackson W. Moore

Christopher G. Smith

PRACTICE AREAS

Data Privacy

Government Contracting

Intellectual Property