CARLTON FIELDS

The White House is Finalizing an Executive Order on Cybersecurity

December 26, 2012

With Capitol Hill and the media both focusing on the “fiscal cliff,” the White House has quietly moved one step closer to issuing an executive order (“EO”) on cybersecurity.

In a recently leaked version of the draft order, the White House has added several provisions that are the direct result of meetings with private sector leaders. The draft EO calls for cooperation and information sharing between the private sector and government. However, it is already catching criticism for what some experts say are incentives that may force some companies to participate.

The EO would give the Secretary of Homeland Security 150 days to identify critical infrastructure where a cyber incident “could reasonably result in a debilitating impact on national security, national economic security, or national public health and safety.” While this language is a bit ambiguous, healthcare organizations, financial institutions, and energy companies are likely to be deemed as “critical” and therefore should pay close attention to the developments surrounding this EO.

The EO also orders the National Institute of Standards and Technology (NIST) to create something called the “Cybersecurity Framework” Presumably this will be a set of best practices or industry standards. The EO only gives the NIST 240 days to publish a preliminary version of its Cybersecurity Framework. Anyone familiar with the federal government knows that the bureaucracy is ill-suited to move that quickly but even at that pace, whatever framework is created will probably be obsolete the moment it becomes final, since by then new technologies will exist bringing with them new vulnerabilities that the Cybersecurity Framework does not address.

Nonetheless, the EO makes several proposals to the private sector in order to compel businesses to follow the Cybersecurity Framework “voluntarily.” First, the EO calls for the Secretary of Homeland Security to encourage the owners and managers of “critical infrastructure” to follow the “voluntary” standards being created by the NIST. Second, each sector-specific federal agency would be required

to report to the President—within 90 days of the publication of the Cybersecurity Framework—on the extent of its existing regulatory power to mandate cybersecurity requirements for the industry it regulates. These sector-specific agencies include the SEC, the FTC, the FAA, the Department of Energy, HHS, and every other regulatory agency. Finally, the EO recommends that each agency propose regulations to mitigate cybersecurity risks within 14 months of the order.

So, if you are a bank, a hospital, an energy provider, or you think your business might fall under what is deemed "critical infrastructure," you need to be aware that this EO is out there and that it will affect your business as soon as it is signed. Carlton Fields is monitoring the developments surrounding this EO and we will provide more information as it moves closer to being signed by the President.

Authored By

Dennis J. Olle

Related Practices

Business Transactions