LOCKE LORD® QUICKStudy
Privacy and Data Security Practice
December 10, 2012

President Obama Expected to Issue Executive Order on Cyber Security, Data Security and Privacy

By: Bart W. Huffman and Paul C. Van Slyke (Locke Lord LLP)
Shane Doucet (Locke Lord Strategies LLP)

In December 2012, or soon thereafter, President Obama is expected to issue a comprehensive Executive order on cyber security, data security and privacy that will boost the administration's effort to improve the digital defenses of critical infrastructure. The Obama administration has sped up its efforts to improve the country's digital defenses, after the Senate failed for a second time to pass S. 3414, the 2012 Cyber Security Act (CSA), during the lame duck session currently under way (President Obama had supported S. 3414).

Industries that are expected to require compliance with regulations that may be adopted include telecommunications, electric utilities, Internet, railways, airlines, airports, stock exchanges, commodity exchanges, banking, chemical plants, refineries, seaports, military contractors, technology and other critical infrastructure. A draft executive order released by the White House excluded "commercial products."

The Draft Executive Order

This Executive Order is expected to pull together the provisions of some of the pending bills, proposed bills, proposed cross border codes of conduct, international privacy laws and codes and changes in existing U.S. laws. Included in the list are the Electronic Communications Privacy Act (ECPA), the Safe Web Act, the UK Information Commissioner's Office ("ICO") "Anonymisation: Managing Data Protection Risk Code of Practice" and Apec Cross-Border Privacy Rules System.

A copy of the most recent draft text of the Executive Order leaked by the White House is available by clicking here. The draft Order directs certain federal agencies to engage in a review of their authority to adopt regulations carrying out the framework of the Order. The draft Order also gives key roles to the Director of Homeland Security, Secretary of Defense, Secretary of Energy, Director of the National Insitute of Standards and Technology, Secretary of the Treasury and Secretary of Commerce.

The draft Executive Order released by the White House requires certain federal agencies to begin immediately to identify critical infrastructure where a cyber security incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security or national security.

Action Steps for Industry

As mandated in the draft Executive Order, the owners and operators of critical infrastructure industry segments should begin to take proactive action as follows:

- Get involved with their trade associations to begin creating a set of standards and industry best practices to the fullest extent possible.
- Engage government relations counsel to be ready for any potential regulatory changes and legislation before Congress.
- Begin identifying the content, structure and types of information most critical to the industry for action to reduce and mitigate risks.

The attorneys in the Privacy and Data Security practice of Locke Lord LLP and its government relations attorneys and lobbyists will be closely monitoring the issues raised here and will be issuing further bulletins. To be assured that you are on our emailing list for further bulletins, please e-mail Ryan Jiloca at rjiloca@lockelord.com.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact one of the authors:

Bart W. Huffman | 512-305-4746 | bhuffman@lockelord.com
Paul C. Van Slyke | 713-226-1406 | pvanslyke@lockelord.com
Shane Doucet | 202-220-6929 | sdoucet@lockelord.com