

New Information Security Law Focus Under Obama Administration?

[Note from Michael Khoury: Kathy Ossian coincidentally wrote an article on the same topic I was going to address for this issue. That gave me the opportunity to invite her to expand her article for the Technology Corner. MSK]

Our news is frequently filled with the latest data security breach of well-known private and public organizations. Certainly, federal agencies, including the United States Department of State, the United States Department of Commerce, and even the Pentagon have experienced their share of such incidents. While many states, including Michigan, have passed laws directed at cybersecurity, including broadly based data breach notification laws,¹ there is no comprehensive federal law addressing this subject.

The Center for Strategic and International Studies (CSIS) Commission on Cybersecurity is a panel composed of leading government and information security industry experts. After deliberating over a 16-month period, the panel issued a report² urging President Obama to make information security an important focus of the new administration.

The CSIS panel's report calls for the creation of a new White House office to protect cyberspace—the National Office for Cyberspace or NOC.³ One of the primary goals in establishing the NOC is better coordination of military, intelligence, and civilian efforts against cyberattacks. The Commission on Cybersecurity coined the acronym DIME—diplomatic, intelligence, military and economic—as the necessary elements of a comprehensive federal cybersecurity plan.⁴

Among the panel's other recommendations is new legislation to facilitate quicker, more effective responses to security breaches. One such measure would be the proposed use of online "data warrants" to replace traditional search warrants, which according to the report "may be increasingly

impracticable in the online environment."⁵

The report also stresses the importance of recognizing individual privacy and confidentiality as "central values that any government cybersecurity initiative must respect."⁶ The panel suggests that government and private entities tailor authentication requirements to the level of risk involved. For example, it would be inappropriate to "demand robust credentials" from individuals seeking to access publicly available government records.⁷

While the panel's recommendations are understandably framed in terms of protecting national security, any new legislation or regulation involving security breaches will likely impact all organizations, both in the public and private sectors. Data security policies and practices will need to be examined and perhaps changed or updated in order to comply with the new laws.

The commission's recommendations are expected to be well received, particularly because several of its members are also members of President Obama's transition team.



Kathryn L. Ossian, of Miller Canfield, Paddock & Stone, PLC, Detroit, practices in the areas of information technology and intellectual property. She is a past chair of the Automation Alley Membership Services Committee. She is a member of the State Bar of Michigan Business Law and Computer Law Sections and the American Bar Association Intellectual Property Law Section. She is a frequent author and lecturer in her areas of expertise.

NOTES

1. See, e.g., the California Database Breach Act, Cal. Civ Code Section 1798.82(e) and the Michigan Identity Theft Protection Act, MCL Section 445.72(a).

2. "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency", December 2008. http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf

3. Page 5, CSIS Report, *supra*.

4. Page 1, CSIS Report, *supra*.

5. Page 68, CSIS Report, *supra*.

6. Page 64, CSIS Report, *supra*.

7. *Id.*, citing "Electronic Authentication: Guidance for Selecting Secure Techniques", National Institute of Standards and Technology, August, 2008 (<http://www.itl.nist.gov/lab/bulletns/bltnaug04.htm>).