WILMERHALE

# Obama Administration Proposes Cybersecurity Legislation

2011-05-17

During recent congressional sessions, Members of Congress have introduced approximately 50 cyber-related bills. Congressional leaders have suggested, however, that no bill would move forward until the Obama Administration set forth its own proposals.

On Thursday, May 12, 2011, the Administration unveiled its recommendations for comprehensive cybersecurity legislation, which consist of seven separate proposals.[1] If enacted, the Administration's proposals would have a far-reaching impact on the cybersecurity practices of major sectors of the economy, including the defense, telecommunications, energy, electricity, banking, and financial services industries. This alert briefly addresses four of those proposals.[2]

*First*, the Administration proposes to increase the authorities of the Department of Homeland Security ("DHS") to direct federal cybersecurity efforts for civilian systems and to facilitate public-private cooperation on cybersecurity by immunizing certain private sector cooperation with DHS. To do so, the Administration proposes to amend the Homeland Security Act through a new "Department of Homeland Security Cybersecurity Authority and Information Sharing Act." *See*democrats.senate.gov/pdfs/WH-cyber-general-authorities.pdf. Although this proposal would establish a comprehensive framework for the Federal Government's cybersecurity activities, and would seek to remove legal barriers to the provision of private assistance to help the Government with its own cybersecurity defenses, it does not remove all uncertainty about the patchwork of federal and state laws, many of which predate the widespread use of the Internet, that may encumber private cybersecurity efforts. The Administration's proposal does contain limitations on liability for certain private sector cooperation and state law preemption provisions relating to private disclosure of cybersecurity information to the Federal Government.

*Second*, the Administration proposes to establish a new "Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act," which would impose significant new cybersecurity obligations upon owners and operators of designated covered critical infrastructure. *See*democrats.senate.gov/pdfs/WH-cyber-critical-infrastructure-provisions.pdf. In particular, it would require them to develop and implement cybersecurity plans, which would be subject to evaluation by private cybersecurity auditors. If owners and operators fail to address cybersecurity risks, they could

potentially be subject to certain regulatory actions by DHS. Owners and operators of covered critical infrastructure would also have to file annual certifications with either the SEC or DHS addressing the adequacy of their cybersecurity plans and their implementation efforts.

*Third*, the Administration proposes to establish a uniform federal standard for notifying consumers of certain data breaches. *See*democrats.senate.gov/pdfs/WH-cyber-breach-notice.pdf. The Administration's proposal would impose a new federal obligation on any business entity—with exemptions for certain health-care entities—in possession of personally identifiable information on more than 10,000 individuals to provide prompt notice to affected individuals about security breaches of certain personal data. The new federal requirement would be subject to enforcement actions for injunctive relief and monetary penalties by the Federal Trade Commission and state attorneys general, but not to enforcement by private parties. This uniform federal approach would preempt the data breach notification laws of 47 States and the District of Columbia by "supersed[ing] any provision of the law of any State, or a political subdivision thereof, relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data."

*Finally*, the Administration proposes to preempt state restrictions on the location of data centers. *See*democrats.senate.gov/pdfs/WH-cyber-data-center.pdf. The Administration's proposal states: "Except where expressly authorized by federal law, no law, rule, regulation or order, or other administrative action of any State or any political subdivision thereof shall require that a business entity locate a data center in such State or political subdivision thereof as a condition precedent to the certification, licensure, or any other approval relating to the operation of such business entity." The Administration acknowledges that the purpose of this proposed legislation is to facilitate the further innovation and adoption of "cloud computing" technology.

The Administration's public transmittal of these legislative proposals to Congress may lead to a renewed emphasis on enacting comprehensive cybersecurity legislation, an issue that has already attracted significant interest from many Members and a wide variety of congressional committees.

[1] The Administration's legislative proposals and a section-by-section analysis are available at the website of Senator Harry Reid (D-NV). *See*democrats.senate.gov/newsroom/record.cfm?id=332834&.

[2] This alert does not address the Administration's proposals to enhance the criminal penalties and civil remedies available for certain violations of the computer-crime statute in 18 U.S.C. § 1030; to amend the Federal Information Security Management Act of 2002, which allocates information security authorities within the Executive Branch; and to recruit and retain cybersecurity employees at DHS.

## *Authors*

# Benjamin A. Powell

**PARTNER**

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770