PUBLICATION

President Obama Signs Several Bills Aimed at Cybersecurity

Authors: Alisa L. Chestler
December 23, 2014

On December 18, 2014, President Barack Obama signed several significant cybersecurity bills into law. These bills include the Federal Information Security Modernization Act, the Border Patrol Agent Pay Reform Act, the Cybersecurity Workforce Assessment Act, the National Cybersecurity Protection Act and the Cybersecurity Enhancement Act of 2014. The bills aim to achieve the following goals:

1. To enhance the federal government's ability to train, recruit and retain cybersecurity professionals, as well as identify necessary skillsets that need to be filled.
2. To strengthen cyber research and development, including improving education for cybersecurity professionals.
3. To increase coordination across the federal government, as well as facilitate public-private communication and collaboration to better prepare for, and combat, cyber-attacks.
4. To research and develop standards, protocols and awareness initiatives to reduce cyber risks to critical infrastructure.

Of particular interest to our clients is the Cybersecurity Enhancement Act of 2014, which authorizes the National Institute of Standards and Technology (NIST) to facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures and processes to cost-effectively reduce cyber risks to critical infrastructure assets. The Act also requires NIST to coordinate closely and regularly with relevant private sector personnel and entities in the development of the new standards and guidelines. Accordingly, it is anticipated that several new standards will be published in the coming months and years.

It is important to note that, although the NIST standards and guidelines are "voluntary," these will likely create baseline "reasonable" standards for addressing cybersecurity threats. Thus, as an unintended consequence, it is possible that, should an incident exposing personal information occur, a failure to acknowledge or address these standards could support either (1) an enforcement action brought by an attorney general in a state that mandates "reasonable" measures to secure personal information, such as Massachusetts or Florida, or (2) a negligence lawsuit brought by the increasingly active plaintiffs' bar.

Ultimately, these bills represent a significant bipartisan step towards addressing cybersecurity threats across the private and public sector. Should you have any questions about this legislation, or any other data security issues, please contact a member of Baker Donelson's Privacy and Information Security Group.