On December 18, 2014, President Obama signed a bill reforming the Federal Information Security Management Act of 2002 ("FISMA"). The new law updates and modernizes FISMA to provide a leadership role for the Department of Homeland Security, include security incident reporting requirements, and other key changes.

**Background:** FISMA was originally passed in 2002 to provide a framework for the development and maintenance of minimum security controls to protect federal information systems. FISMA charged the Director of the Office of Management and Budget ("OMB") with oversight of agency information security policies and practices.

**Changes:** The newly signed law, the “Federal Information Security Modernization Act of 2014” (FISMA 2014”), makes several key changes to FISMA.

First, the law authorizes the Secretary of the Department of Homeland Security ("DHS") to assist the OMB Director in administering the implementation of agency information and security practices for federal information systems. Among the Secretary's responsibilities are convening meetings with senior agency officials, coordinating government-wide efforts for information security, consulting with the Director of the National Institute of Standards and Technology ("NIST"), and providing operational and technical assistance to agencies. Perhaps most importantly, the Secretary is tasked with developing and overseeing the implementation of “binding operational directives” to agencies to implement policies, principles, standards, and guidelines developed by the OMB Director. “Binding operational directives” are defined in FISMA 2014 as a “compulsory direction” to an agency “for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability or risk.”

This delegation of responsibility is likely related to another new law codifying DHS’s cybersecurity role, and authorizing a cybersecurity information-sharing hub, the National Cybersecurity and Communications Integrations Center.

Second, the law changes the agency reporting requirements, modifying the scope of reportable information from primarily policies and financial information to specific information about threats, security incidents, and compliance with security requirements. The revisions to the law direct the OMB Director to provide guidance as to what constitutes a “major incident” as applies to agency reporting requirements. It also requires the OMB Director, in consultation with the Secretary of DHS, to report to Congress on an annual basis the “effectiveness of [federal agency] information security policies and practices,” including a summary of information security incidents, thresholds for reporting major information security incidents, a summary of the results of federal agency information system risk assessments, and agency compliance with data breach notification policies and procedures.

Third, the law updates FISMA to address cyber breach notification requirements. Specifically, the OMB Director is required to ensure that federal agency “data breach notification policies and guidelines are updated periodically” and that federal agencies provide notice to Congress “expeditiously” but no later than 30 days after the date an agency discovers the breach. In that notice, agencies must provide a variety of information about the breach,
including the estimated number of individuals affected, the assessed risk of harm to those individuals, and when notice will be made to those individuals.

Fourth, within one year of the enactment of FISMA, the OMB Director, is required to revise Budget Circular A-130 to eliminate inefficient or wasteful reporting. Circular A-130 implements the Clinger-Cohen Act of 1996 and “establishes policy for the management of Federal information resources.” The Circular was last updated in 2000. The elimination of “inefficient or wasteful” reporting requirements would allow federal agency information security personnel to allocate more resources to the protection of government systems.

Finally, the law makes some other key additions, including allowing for the Comptroller General to provide technical assistance to agency heads and Inspector Generals in carrying out their duties. FISMA 2014 also updates the functions of the Federal Information Security Incident Center to provide intelligence information about cyber threats, vulnerabilities, and incidents to assist agencies.

Impact on Contractors: This update to FISMA represents the federal government’s internal policies and procedures for protecting federal information and federal information systems. While the new law is aimed at the federal government, these requirements will likely trickle down to government contractors handling government information.

There is also potential for additional contractor opportunities. FISMA 2014 requires each federal agency to have an independent evaluation of its information security program and practices performed annually, the results of which must be submitted to the OMB Director. Commercial contractors also stand to benefit because the law explicitly recognizes that commercially developed information security products offer “advanced, dynamic, robust, and effective information security solutions.” Despite the clarification of OMB and DHS oversight, the law explicitly provides that the selection of specific information security solutions from among commercially developed products should be left to individual agencies.

Moreover, to the extent that they operate government information systems, contractors will need to understand these requirements. These changes follow GAO’s August 2014 Report, which criticized agency oversight of contractors that are responsible for and have “privileged access” to government systems.

© 2019 Covington & Burling LLP