FEDERAL INFORMATION SECURITY AND MANAGEMENT ACT (FISMA)

The Federal Information Security and Management Act (FISMA) requires federal agencies to provide security protections for "information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."[1] FISMA applies to both federal government agencies and organizations that possess federal information, but only if they are using it on behalf of a federal agency.[2] For example, FISMA clearly applies to systems that support the operations and assets of a federal agency, including those provided or managed by another agency, contractor or other source.

Determining FISMA's applicability to contractors or third parties that are not directly supporting the operations and assets of an agency is more difficult. The OMB recently issued guidance clarifying FISMA's scope, and states that an agency's security program applies only to organizations that possess federal information or operate, use, or have access to federal information systems on behalf of a federal agency. [3] The term organization includes contractors, grantees, state and local governments, industry partners, and providers of software subscription services that use federal information or information systems on behalf of a federal agency.[4]

Although OMB guidance clearly identifies the breadth of entities that could be subject to FISMA, it does not provide guidance on when potential entities are acting on behalf of an agency, and thus subject to FISMA. In its most recent Reporting Instructions Memo, OMB reiterates that FISMA's requirements follow agency information into any system when the ultimate responsibility and accountability for control of the information continues to reside with the agency.[5]

The purpose of FISMA is to provide for the development and maintenance of minimum controls necessary to protect federal information and information systems commensurate with the risk and magnitude of harm resulting from unauthorized access, use, or disclosure.[6] FISMA applies to all federal information and information systems including data, information systems, and information technology (*i.e.* networks and computers), all forms of information (such as paper, electronic and audio), and all types of information (including sensitive and personally identifiable information).[7] However, as stated above, FISMA only applies to information that is collected or maintained by a

[1] Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3544 (2006).
[2] Office of Mgmt. & Budget, Executive Office of the President, OMB M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* 13-14 (2010) [hereinafter OMB M-10-15].
[3] *Id.* at 13.
[4] *Id.*
[5] *Id.* at 16.
[6] *See generally* 44 U.S.C. § 3544.
[7] OMB M-10-15, *supra* note 211, at 5.

federal agency or an organization on the agency's behalf and where there is risk of harm from unauthorized use or disclosure.

Further, FISMA requires the head of an agency to provide protection and report on security programs for all information systems used or operated by the agency or an organization on the agency's behalf.[8] The term information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[9] An agency's annual FISMA report must summarize the performance of an agency's program to secure all of the agency's information and information systems, in any form or format, whether automated or manual.[10] NIST provides guidance on establishing information system boundaries, which can help the agencies identify their systems.[11]

Generally, FISMA compliance requires agencies to: 1) Develop an agencywide information security program;[12] 2) Conduct annual reviews on the effectiveness of the agency's information security and privacy programs and report the results to OMB annually;[13] and 3) Produce a complete and accurate inventory of all information systems, including their security status and requirements.[14]

Agencies must plan for security needs as they develop new and operate existing systems and as security weaknesses are identified. OMB issued guidance on this issue in OMB Memo M-00-07, which remains in effect. In brief, agencies must do two specific things: 1) integrate security into each system and fund it over the lifecycle of each system as it is developed;[15] and 2) ensure that operations of legacy (steady-state) systems meet security requirements before funds are spent on new systems (development, modernization, or enhancement).[16]

FISMA vests the OMB with supervisory authority over all agency information security programs.[17] OMB must approve each agency's plan for FISMA implementation, receive regular updates on agency compliance,[18] and submit annual reports to Congress detailing each agency's progress and shortcomings in achieving information security.[19]

---

[8] FISMA at § 3544(1)(A).
[9] 44 U.S.C. § 3502(8).
[10] OMB M-10-15, *supra* note 211, at 5.
[11] *Id.*; *see* Nat'l Inst. Of Standards & Tech., U.S. Dep't of Commerce, NIST Special Publication 800-37, *Guide for Applying thee Risk Management Framework to Federal Information Systems* (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf [hereinafter NIST Special Publication 800-37].
[12] FISMA at § 3544(b).
[13] FISMA at §§ 3544(c); 3545(a).
[14] 44 U.S.C. § 3505.
[15] Office of Mgmt. & Budget, Executive Office of the President, OMB M-00-07, *Incorporating and Funding Security in Information Systems Investments* (2010) [hereinafter OMB M-00-07]; FISMA § 3544(b)(2)(C).
[16] OMB M-00-07, *supra* note 249, at 6-7.
[17] FISMA at § 3543(a).
[18] FISMA at § 3544(b).
[19] FISMA at § 3542(a)(8)(B)-(C).

FISMA empowers OMB to enforce compliance through a list of suggested sanctions.[20] These sanctions include:

- **Appropriate Action:** any action that the Director considers appropriate to enforce accountability.
- **Agency Budget:** recommend a reduction or increase in the amount of information resources that the head of an agency proposes for the budget submitted to Congress.
- **Appropriations:** reducing or adjusting apportionments for information resources.
- **Other Administrative Controls:** restrict the availability of information resources to the agency.
- **Private Sector Contracts**: designate agency to contract with private sector sources for the management of information technology and resources.[21]

Additionally, the OMB annual reports on agency compliance with FISMA serve as an enforcement tool by making an agency's failing grade publicly available.

[20] *See* FISMA at § 3543(a)(4) (granting the OMB Director authority to use any and all measures available under 40 U.S.C. § 11303 to ensure agency compliance with FISMA).
[21] 40 U.S.C. § 11303(b)(4)-(5) (2006).