# CRS Insights

Cybersecurity: FISMA Reform

Eric A. Fischer, Senior Specialist in Science and Technology (efischer@crs.loc.gov, 7-7071)

November 24, 2014 (IN10186)

Two bills to revise the Federal Information Security Management Act (FISMA, 44 U.S.C. Chapter 35, Subchapter III) are being considered in the 113th Congress. H.R. 1163 passed the House in April 2013, and S. 2521 was reported to the Senate in September 2014.

## Current FISMA Requirements

Enacted in 2002, FISMA created a security framework for federal information systems. It emphasizes risk management and gives specific responsibilities to the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and individual federal agencies.

FISMA gives OMB responsibility for overseeing federal information-security policy, evaluating agency information-security programs, and promulgating cybersecurity standards developed by NIST. It requires executive agencies to inventory major computer systems, identify and provide appropriate security protections, and develop, document, and implement agency-wide information-security programs. Agencies must provide security protections commensurate with risk and comply with applicable security standards. They must perform risk assessments, determine and implement necessary security controls in a cost-effective manner, and evaluate those controls periodically. Each agency must designate an information-security officer, with responsibilities including agency-wide information-security programs, policies, and procedures, training of security and other personnel, processes for remedial action to address deficiencies, and procedures for handling security incidents and ensuring continuity of operations. Agencies must also develop performance plans, effect independent annual evaluations of their cybersecurity programs and practices, and provide annual reports on compliance and effectiveness to Congress. FISMA security requirements also apply to contractors who run information systems on behalf of an agency.

The act exempts national security systems (NSS) from its requirements, except with respect to enforcement of accountability by agencies for meeting requirements, and reporting to Congress. NSS fall under the jurisdiction of the interagency Committee on National Security Systems (CNSS). However, FISMA requires that CNSS and FISMA standards be complementary to the extent feasible. It also gives responsibility for protection of mission-crucial systems in DOD and the CIA to the Secretary of Defense and the CIA Director, respectively.

The law also established a central federal incident center, overseen by OMB, to analyze incidents and provide technical assistance relating to them, to inform agency operators about current and potential threats and vulnerabilities, and to consult with NIST, NSA, and other appropriate agencies about incidents.

## Issues and Concerns

A commonly expressed concern about FISMA is that it is awkward and inefficient in providing adequate cybersecurity to government IT systems. The causes cited have varied but themes have included inadequate resources, a focus on procedure and reporting rather than operational security, lack of widely accepted cybersecurity metrics, variations in agency interpretation of the mandates in the act, excessive focus on individual information systems as opposed to the agency's overall information architecture, and insufficient means to enforce compliance both within and across agencies. Weaknesses in FISMA implementation have been cited by GAO. In 2010, OMB attempted to address some of the operational issues administratively by delegating some operational responsibilities to the Department of Homeland Security (DHS).

Debate over legislation to amend FISMA has involved several issues, including the following:

- *The roles of OMB and DHS.* Some observers believe that DHS should be given statutory authority for the operational responsibilities that have been delegated to it, arguing that such authority would clarify those responsibilities and help strengthen DHS capabilities. Others, however, believe that OMB should retain the capability to delegate operational responsibilities, given the continuing rapid evolution of the cybersecurity threat environment and uncertainties about DHS capacity to be effective in this role.
- *Revisions to agency responsibilities.* Some believe that agency responsibilities should be modified to include specific operational requirements such as continuous monitoring and use of metrics, and that more emphasis should be placed on risk-based rather than minimum security measures. Others argue that such specific requirements should not be codified in statute but included instead in the NIST standards, which can be revised more readily in response to changes in the information technology environment.
- *Changes in reporting requirements.* Some argue that more emphasis should be placed on immediate sharing of cybersecurity information aimed at preventing and mitigating attacks, rather than periodic reporting of compliance. Others argue that such reporting is needed for adequate oversight, and that FISMA currently provides sufficient flexibility to permit rapid information sharing.
- *Cybersecurity requirements for contractors.* Some argue that FISMA provisions relating to contractor cybersecurity should be more stringent, especially given the absence of specific contract-language requirements relating to FISMA in the Federal Acquisition Regulations (FAR). Others argue that current statutory authority is sufficient, and that any improvements needed can be accomplished via NIST standards and changes to the FAR.

Current Bills

Among the changes to FISMA being considered in current bills are the following:

- S. 2521 would provide operational authority to DHS; H.R. 1163 would not.
- H.R. 1163 would require automated and continuous monitoring of agency information systems; S. 2521 would not.
- Both bills stress timely reporting of incidents after discovery.
- H.R. 1163 would strike the requirement for annual independent evaluations; S. 2521 would retain it.
- S. 2521 would transfer authority for the federal incident center to DHS; H.R. 1163 would not and would require OMB to ensure that the incident center has the capabilities needed to ensure fulfillment of its mission.
- S. 2521 would require OMB to establish procedures to be followed after a cybersecurity incident involving a breach of personally identifiable information; H.R. 1163 has no corresponding provision. However, H.R. 3635, which passed the House in July 2014, would amend FISMA to establish requirements in the event of such a data breach.

Neither H.R. 1163 nor S. 2521 directly address the issue of contractor compliance with FISMA requirements, but NIST has developed a draft set of standards for nonfederal systems on protection of federal information that they contain or process. Neither bill mentions the DHS National Cybersecurity and Communications Integration Center (NCCIC) which serves as the FISMA incident center through its United States Computer Emergency Readiness Team (US-CERT) branch. However, H.R. 3696 and S. 2519 would establish the NCCIC in law.