CYBER SECURITY
INDUSTRY ALLIANCE

FISMA: Get the Facts

September 2006

FISMA: Get the Facts

What is FISMA?

The Federal Information Security Management Act (FISMA) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. Its purpose is to bolster computer and network security within the federal government and affiliated parties (such as government contractors) by mandating yearly audits.

FISMA permanently authorized and strengthened the information security program, evaluation, and reporting requirements that were first introduced by the Government Information Security Reform Act of 2000 (GISRA). Frustrated with the limited progress agencies were making to comply with GISRA, Congress replaced it with FISMA.

FISMA does not address technical specifications, but rather senior management responsibility, including the Chief Information Security Officer (CISO) and the head of the agency. Agencies must show how the overall information security strategy and budget fit in with the general mission and goals of the agency.

What is the goal of FISMA?

The intent of FISMA is to inform and raise awareness among federal agency heads of the importance of information security programs and to facilitate the development of security programs through mandatory comprehensive reporting and evaluation.

How are agencies evaluated under FISMA?

FISMA requires annual objective assessments of the effectiveness of security controls for every federal computer system. Two assessments are required: an internal assessment headed by the CIO and an independent evaluation conducted by the agency Inspector General.

The key element in demonstrating FISMA compliance is the comprehensive annual report that the CIO and the head of each agency provide to Congress and to the Office of Management and Budget (OMB). This report includes evaluations of the effectiveness of the information security programs, including providing evidence that the agency has developed a coordinated strategy of analyzing security threats and responding accordingly. If an agency implements a technology solution to boost their score in one year, they may score lower the following year if they fail to demonstrate how the solution fits into the agency's overall information security strategy.

Who is responsible for FISMA oversight and guidance?

OMB and the National Institute of Standards and Technology (NIST) are the key federal agencies that issue policy and guidance for unclassified information technology security.

OMB is responsible for developing and overseeing the implementation of government-wide policies, principles, and standards, as well as providing guidance for the federal government's information technology security program. OMB oversight and enforcement are achieved by reviewing and evaluating the following:

- Information technology budget submissions and business case justifications for major information technology investments;
- Annual agency and inspector general FISMA reports to OMB;
- Agency remediation efforts as demonstrated through their development, prioritization, and implementation of program and system level plans of action and milestones (POA&M);
- Quarterly updates from agencies to OMB on their progress in remediating security weaknesses through completion of POA&M;
- Quarterly updates from agencies to OMB on their performance against key security measures;
- Quarterly assessment of agencies security status and progress through their e-Government Scorecard under the President's Management Agenda; and
- Annual OMB report to Congress.

NIST, under the Commerce Department, is responsible for developing technical security standards and guidelines for unclassified Federal computer systems. NIST publications are designed to:

- Promote, measure and validate security in systems and services;
- Educate consumers; and
- Establish minimum security requirements for Federal systems.

In accordance with FISMA, NIST must prepare an annual report describing activities completed in the previous year as well as detailing future actions to carry out FISMA responsibilities.

What defines FISMA compliance?

FISMA compliance requires that agency heads work with CIOs and CISOs to address eight broad categories:

- **Risk Assessments.** Periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or computer system.

- **Policies and Procedures.** Risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each computer system.
- **Security Plans.** Plans describing security measures that address specific system requirements and comply with policies and procedures, as well as guidance issued by NIST. Such plans must cover security professionals and user training, incident response capabilities, contingency plans, remediation and system configuration standards.
- **Security Awareness Training.** Training must be offered to users of agency computer systems and cover the risks associated with handling critical data and the responsibilities involved in providing effective security.
- **Annual Security Testing.** Periodic testing and evaluation of the effectiveness of information security policies, procedures and practices, performed with a frequency depending on risk (no less than annually), and including testing of management, operations and technical controls for every computer system identified in the agency's required inventory of major information systems.
- **Remediation Procedures.** A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency, through plans of action and milestones.
- **Incident Response Procedures.** Sufficient detection and response capabilities within each agency, including the ability to mitigate attacks in progress. FISMA directs agencies to report all attacks to US-CERT.
- **Contingency Plans.** Every computer system must be included in annually-tested plans containing procedures to ensure continuity of operations in the event of infrastructure failure.

What do critics say about FISMA?

Different entities, including Government Accountability Office (GAO) and NIST have voiced concerns over FISMA. The major criticisms can be grouped into four categories: inefficiency, clarity of guidance, consistency and adoption rate.

- **Inefficiency.** The SANS Institute and *Government Computer News* are concerned that FISMA diverts critical resources away from implementing information network security. Instead, time, energy and money are spent fulfilling the paperwork requirements of FISMA.
- **Clarity of Guidance.** The GAO and OMB disagree on whether the OMB's FISMA guidance to agencies is useful for Congressional oversight purposes.
- **Consistency.** The GAO also is critical because auditors use different evaluation criteria in different agencies. Results vary widely, and it is not clear what the benchmark is, or whether one standard of security control is feasible across agencies.

- **Adoption Rate.** It will take time for agencies to adopt FISMA as a risk management framework. Federal agencies are at various levels of maturity with respect to assimilating the security standards and guidance.

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is the only advocacy group dedicated exclusively to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Led by CEOs from the world's top security providers, CSIA believes a comprehensive approach to information system security is vital to the stability of the global economy. Visit our web site at www.csialliance.org.

Members of the CSIA include Application Security, Inc.; CA, Inc. (NYSE: CA); Citadel Security Software Inc. (CDSS:OTC); Citrix Systems, Inc. (NASDAQ: CTXS); Entrust, Inc. (NASDAQ: ENTU); F-Secure Corporation (HEX: FSC1V); Fortinet, Inc.; Internet Security Systems Inc. (NASDAQ: ISSX); iPass Inc. (NASDAQ: IPAS); McAfee, Inc. (NYSE: MFE); Mirage Networks; PGP Corporation; Qualys, Inc.; RSA Security Inc. (NASDAQ: RSAS); Secure Computing Corporation (NASDAQ: SCUR); Surety, Inc.; SurfControl Plc (LSE: SRF); Symantec Corporation (NASDAQ: SYMC); TechGuard Security, LLC; and Vontu, Inc.

Cyber Security Industry Alliance
2020 North 14th Street, Suite 750 • Arlington, VA 22201 • (703) 894-CSIA • www.csialliance.org