

Federal Information Security Management Act of 2002

From Wikipedia, the free encyclopedia

For a factual analysis of FISMA and its flaws, see the "Discussion" section.

The **Federal Information Security Management Act of 2002** ("FISMA", 44 U.S.C. § 3541, *et seq.*) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The Act was meant to bolster computer and network security within the Federal Government and affiliated parties (such as government contractors) by mandating yearly audits.

FISMA has brought attention within the Federal Government to cybersecurity, which had previously been much neglected. As of February 2005, many government agencies received extremely poor marks on the official report card, with an average of 67.3% for 2004, an improvement of only 2.3 percentage points over 2003.^[1] This shows a marginal increase in how federal agencies prioritize cybersecurity, but experts warn that this system of measurement is misleading. Many argue that in actual implementation across Federal departments and agencies, FISMA measures the wrong things. Thus, it is entirely possible that an agency with a high grade can be less secure than an agency with a lower grade, and a high grade is no guarantee of actual security. Despite its value for increasing awareness and bringing attention to such an important issue, there are some who feel that FISMA is fatally flawed and will never get Federal information systems, networks and information to the point where they are safe from those who wish to do them harm. Those detractors are correct to a degree, namely that FISMA alone is not the solution to Federal information security challenges.

Contents

- 1 FISMA Compliance Process for an Information System
 - 1.1 Determine the Boundaries of the System
 - 1.2 Determine the Information Types in System and Perform FIPS-199 Categorization
 - 1.3 Document the System
 - 1.4 Performing Risk Assessment
 - 1.5 Select and Implement a Set of Security Controls for System
 - 1.6 Certification of System
 - 1.7 Accreditation of System
 - 1.8 Continuous Monitoring
- 2 Issues With FISMA
- 3 Sources
- 4 References
- 5 See also

FISMA Compliance Process for an Information System

FISMA imposes a mandatory set of processes that must be followed for all information systems used or operated by a US Government federal agency or by a contractor or other organization on behalf of a US Government agency. These processes must follow a combination of Federal Information Processing

standards (FIPS) documents, the special publications SP-800 series issued by NIST, and other legislation pertinent to federal information systems, such as the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act. Unfortunately, following these mandates only results in "compliance" and not "security." The flaws of the current process are addressed in the "Discussion" section.

Determine the Boundaries of the System

The first step is determining what constitutes the "information system" in question. There is not a direct mapping of computers to information system; rather an information system can be a collection of individual computers put to a common purpose and managed by the same system owner. NIST SP 800-18 revision 1 provides guidance on determining system boundaries. In actual practice, no two agencies apply the guidance the same way, and the Office of Management and Budget has yet to provide useful clarification. Moreover, no two agency inspectors general evaluate the definition of system boundaries the same way either. Therefore, no two departments or agencies are applying the same approaches to defining systems, applications, interconnections or controls.

Determine the Information Types in System and Perform FIPS-199 Categorization

The next step is to determine the information types resident in the system and categorize each according to the magnitude of harm resulting were the system to suffer a compromise of Confidentiality, Integrity, or Availability. NIST SP 800-60 provides a catalog of information types, and FIPS-199 provides a rating methodology and a definition of the three criteria.

The overall FIPS-199 system categorization is the high water mark of the impact rating of any of the criteria for any information types resident in the system. So if one information type in the system has a rating of *Low* for *confidentiality*, *integrity*, and *availability*, and another one has a rating of *Low* for *confidentiality* and *availability* but a rating of *Moderate* for *integrity*, the entire system has a FIPS-199 categorization of *Moderate*.

Document the System

Pertinent system information such as system boundaries, information types, constituent components, responsible individuals, description of user communities, interconnections with other systems and implementation details for each security control need to be documented in the system security plan.

A critical part of the system documentation is a hardware and software inventory of the systems and major applications that reside within the defined boundaries of the system. This inventory should include hardware make and model numbers, software version numbers, patch levels, and a functional description of the component such as "database", "webserver," "fileserver," "directory server," etc.

NIST SP 800-18 Rev 1 gives guidance on documentation standards. Additional documentation such as a contingency plan for the system also needs to be prepared at this stage. Guidance on contingency planning can be found in NIST SP 800-34.

Performing Risk Assessment

A risk assessments starts by identifying potential threats and vulnerabilities, and maps implemented

controls to individual vulnerabilities. One then determines risk by calculating the likelihood and impact of any given vulnerability being exploited, taking into account existing controls. The culmination of the risk assessment shows the calculated risk for all vulnerabilities, and describes whether the risk is to be accepted or mitigated. If mitigated by the implementation of a control, one needs to describe what additional SP 800-53 controls will be added to the system. NIST SP 800-30 provides guidance on the risk assessment process.

Select and Implement a Set of Security Controls for System

If the system in question is in the design or implementation life-cycle phase, a set of security controls must be selected and incorporated into the system implementation. Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST Special Publication 800-53 revision 1, *Recommended Security Controls for Federal Information Systems*, which contains the management, operational, and technical safeguards or countermeasures prescribed for an information system. The controls selected or planned must be documented in the system security plan. Perhaps the area where inconsistencies prevail most across the Federal computing enterprise is in this area. The concept behind "controls" is to mitigate risk, so that resulting risk can be accepted and the system can be accredited to operate. No two agencies interpret this concept the same way or apply controls the same way. Thus, it is possible for a system owner to accept infinite risk to operate a system, document the decision correctly and accredit the system to operate. Here is where FISMA has its soft underbelly. Theoretically, 100% of all Federal information systems can be certified and accredited, thus receiving full FISMA credit. However, it is possible (even probable) that all 100% cannot be considered "secure." The myth of FISMA is that the annual grades have something to do with security; in actuality, the grades are about the acceptance of massive amounts of risk.

Certification of System

Once the system documentation and risk assessment is complete, the system needs to have its controls assessed and certified to be functioning appropriately. For systems with a FIPS-199 categorization of Low, a self assessment is sufficient for certification. For systems categorized at higher FIPS-199 levels, a certification performed by an independent 3rd party is required. NIST SP 800-26 provides guidance on the self assessment process. NIST SP 800-53A provides guidance on the assessment methods applicable to individual controls.

Accreditation of System

Once a system has been certified, the security documentation package is reviewed by an accrediting official, who, if satisfied with the documentation and the results of certification, accredits the system by issuing an authorization to operate (ATO). This authorization is usually for a 3 year period, and may be contingent on additional controls or processes being implemented. NIST SP 800-37 provides guidance on the certification and accreditation of systems.

Continuous Monitoring

All accredited systems are required to monitor a selected set of security controls for efficacy, and the system documentation is updated to reflect changes and modifications to the system. Significant changes to the security profile of the system should trigger an updated risk assessment, and controls that are

significantly modified may need to be re-certified. Guidance on continuous monitoring can be found in NIST SP 800-37 and SP 800-53A.

Issues With FISMA

Security experts such as Bruce Brody, a former Federal CISO, and Alan Paller, Director of Research for the SANS Institute have described FISMA as "fundamentally flawed" and argued that the compliance and reporting methodology mandated by FISMA may be primarily a paperwork exercise that doesn't necessarily improve information security. ^[2] ^[3] ^[4]

Many other Federal officials believe FISMA can be improved, but Congress does not appear to have FISMA high on its agenda prior to the 2008 elections.

Sources

- [1] FCW: Security experts fault FISMA paperwork
- [2] GCN: Interview with Bruce Brody
- [3] GCN: Experts: It's time to fix FISMA

References

- NIST SP 800 Series Special Publications Library
- NIST FISMA Implementation Project Home Page
- Full text of FISMA
- NIST Computer Security Resource Center
- Security Certification and Accreditation 101
- Report on 2004 FISMA scores

See also

- System Security Authorization Agreement (SSAA)
- ACART - FISMA Compliance Assessment & Reporting Solution

Retrieved from

"http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002"

Categories: All articles with unsourced statements | Articles with unsourced statements since March 2007 | 2002 in law | United States federal government administration legislation | Computer law

- This page was last modified 02:54, 13 July 2007.
- All text is available under the terms of the GNU Free Documentation License. (See **Copyrights** for details.)
Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a U.S. registered 501(c)(3) tax-deductible nonprofit charity.