



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

FISMA, NIST and the Requirement for
Security Certification and Accreditation

Clayton Holland

Missing Link Security

**This white paper is made available by Missing Link Security...We find
your weakest links.**



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Abstract

The Federal Information Security Management Act of 2002 (FISMA) is directed to the heads of federal agencies. It requires development of agency-wide information security programs and delegation of responsibility and authority by the agency heads to Chief Information Officers and subordinates. FISMA also directs the National Institute of Standards and Technology to develop standards and guidelines for providing adequate information security for all agency operations and assets. Chief among these is NIST Special Publication 800-53, made mandatory by Federal Information Processing Standards 200 under the authority of FISMA. NIST SP 800-53 contains explicit requirements for security certification and accreditation of federal information systems.

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

FISMA, NIST and the Requirement for Security Certification and Accreditation

The Federal Information Security Management Act of 2002 (FISMA) is Title III of the E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President on December 17, 2002 . FISMA recognizes the significance of the security of federal information to the national security and economic interests of the United States. The Act (text available at, <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>) requires each federal agency to develop, document and implement an agency-wide information assurance program.

The act is directed to agency heads and requires each to ensure provision of:

...information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency... (§ 3544)

The Act seeks to mature the federal government's information assurance capabilities from being an attribute of individuals to an attribute of the organization at the agency level. The act contains explicit direction to agency heads to delegate responsibility and authority to Chief Information Officers and their subordinates to achieve this goal. It requires that information assurance programs be integrated with

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

agency strategic and operational planning processes, and that these programs operate on principals of risk management implemented through periodic assessments of risk associated with the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information or information systems. The Act directs implementation of policies and procedures to manage risk, and periodic testing of risk mitigation controls.

FISMA requires annual independent audits of agency information assurance programs to be reported to the White House Office of Management and Budget to directly tie FISMA compliance to agency program funding.

The Act directs the National Institute of Standards and Technology (NIST) to “...develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets.” (§ 11331)

Among the standards published by NIST under the authority and direction of FISMA is Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations. NIST SP 800-53 details 171 control requirements in 17 families of operational, managerial and technical controls. (Ross, 2007) The publication’s title is misleading. Although originally published as recommendations, Federal Information Processing Standards Publication number 200, Minimum Security Requirements for Federal Information and Information Systems (FIPS

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

200) published in March of 2006, made NIST SP 800-53 control recommendations mandatory.

FIPS 200 explicitly cites FISMA as its authority:

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

FIPS 200 is applicable to:

(i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2). (p. iv)

The text of FIPS 200 that invokes NIST SP 800-53 reads,

Federal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Publication 800-53, Recommended Security Controls for Federal Information Systems, as amended. (p.v)

This chain of authority is important because although the familiar assertion that FISMA does not require security certification and accreditation (C&A) of federal information systems is correct, NIST SP 800-53 is where requirements for C&A and associated documentation reside, and SP 800-53 became mandatory under FIPS 200 under the authority of FISMA.

The 17 families of controls, their identifiers and class described by SP 800-53 (2007, p. 6) are: Access Control (AC) (Technical,) Awareness and Training (AT) (Operational,) Audit and Accountability (AU) (Technical,) Certification, Accreditation, and Security Assessments (CA) (Management,) Configuration Management (CM) (Operational,) Contingency Planning (CP) (Operational,) Identification and Authentication (IA) (Technical,) Incident Response (IR) (Operational,) Maintenance (MA) (Operational,) Media Protection (MP) (Operational,) Physical and Environmental Protection (PE) (Operational,) Planning (PL) (Management,) Personnel Security (PS) (Operational,) Risk Assessment (RA) (Management,) System and Services Acquisition (SA) (Management,) System and Communications Protection (SC) (Technical,) and System and Information Integrity (SI) (Operational.) Note that only 4 of these families of controls are technical. The remaining 13 are either managerial or operational in class.

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

At the system level, “FISMA compliance” usually refers to compliance with NIST SP 800-53 and most especially that the system has been explicitly authorized to operate by an authority delegated that authority by the agency head. This authorization to operate (also known as accreditation) is described by control CA-1 of SP 800-53 and the process by which the system’s compliance with requirements is determined and risk is assessed toward making the accreditation decision is CA-4 of SP 800-53. CA-1 and CA-4 form the basis for information systems security certification and accreditation (C&A) requirements under the authority of FISMA.

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

Supplemental Guidance: The security assessment and certification and accreditation policies and procedures are consistent with applicable laws,

Executive Orders, directives, policies, regulations, standards, and guidance. The

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures (2007, p. F-19).

CA-4 SECURITY CERTIFICATION

Control: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Supplemental Guidance: A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

controls in an information system during the initial security accreditation...(2007, p. F-21)

FISMA is broad in scope. It does not explicitly require federal information systems security certification and accreditation. However, it directs NIST to develop standards and guidelines to including minimum requirements, for providing adequate information security for all agency operations and assets. NIST published Special Publication 800-53 in compliance with this directive. The Secretary of Commerce subsequently published Federal Information Processing Standards 200 under the authority of FISMA which made the control recommendations of SP 800-53 mandatory for all federal information systems and systems that process federal information. Included within the SP 800-53 controls made mandatory are those requiring information systems security certification and accreditation.

This white paper is made available by Missing Link Security...We find your weakest links.



Missing Link Security
A Veteran Owned Small Business
123 S Fayette Street
Alexandria, VA 22314
www.MissingLinkSecurity.com
SPACE@MissingLinkSecurity.com

Reference List

Federal Information Security Management Act of 2002, Pub. L. No. 107-347, Title III (2002).

U.S. Department of Commerce. National Institute of Standards and Technology. (2007, December). Recommended Security Controls for Federal Information Systems (Rev 2 ed.) (SP 800-53). Washington, DC: U.S. Government Printing Office. Retrieved February 24, 2009 from the World Wide Web:

<http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf>.

U.S. Department of Commerce. National Institute of Science and Technology. (2006, March 0). Minimum Security Requirements for Federal Information and Information Systems (FIPS 200). Washington, DC: U.S. Government Printing Office. Retrieved February 24, 2009 from the World Wide Web:

<http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>.

This white paper is made available by Missing Link Security...We find your weakest links.