Protecting Federal Information Systems

The NIST Strategy for Implementing Key Provisions of the Federal Information Security Management and the Cyber Security R&D Acts

Ed Roback, Chief
Computer Security Division

March 2003

Topics

1. Federal Information Security Management Act
2. Cyber Security Research and Development Act

FISMA Legislation

Overview

"Each Federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"

-- Federal Information Security Management Act of 2002

FISMA Legislation

Requirements Part I

In accordance with the provisions of FISMA, agency information security programs must include—

- Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate

FISMA Legislation

Requirements Part II

In accordance with the provisions of FISMA, agency information security programs must include—

- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including the management, operational, and technical controls of every agency information system identified in their inventory) to be performed with a frequency depending on risk, but no less than annually
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency

FISMA Legislation

Requirements Part III

In accordance with the provisions of FISMA, agency information security programs must include—

- Procedures for detecting, reporting, and responding to security incidents (including mitigating risks associated with such incidents before substantial damage is done and notifying and consulting with the Federal information security incident response center, and as appropriate, law enforcement agencies, relevant Offices of Inspector General, and any other agency or office, in accordance with law or as directed by the President
- 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

Key NIST Specific Responsibilities Under FISMA

NIST tasked to develop:

- Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Guidelines recommending the types of information and information systems to be included in each category
- Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category

Categorization Standards

NIST FISMA Requirement #1

- Develop standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels—
- Planning underway by NIST to develop:

  Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"

  Final Publication NLT December 2003

Mapping Guidelines

NIST FISMA Requirement #2

- Develop guidelines recommending the types of information and information systems to be included in each category described in FIPS 199—
- Planning underway by NIST to develop:

  Special Publication 800-60, "Guide for Mapping Types of Federal Information and Information Systems to Security Categories"

  Final Publication NLT June 2004 (by law)

✓ Public workshop planned

Minimum Security Requirements

NIST FISMA Requirement #3

- Develop minimum information security requirements (i.e., management, operational, and technical security controls) for information and information systems in each such category—
- Planning underway by NIST to develop:
  - Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Controls for Federal Information and Information Systems"*
  - Final Publication NLT December 2005 (by law)

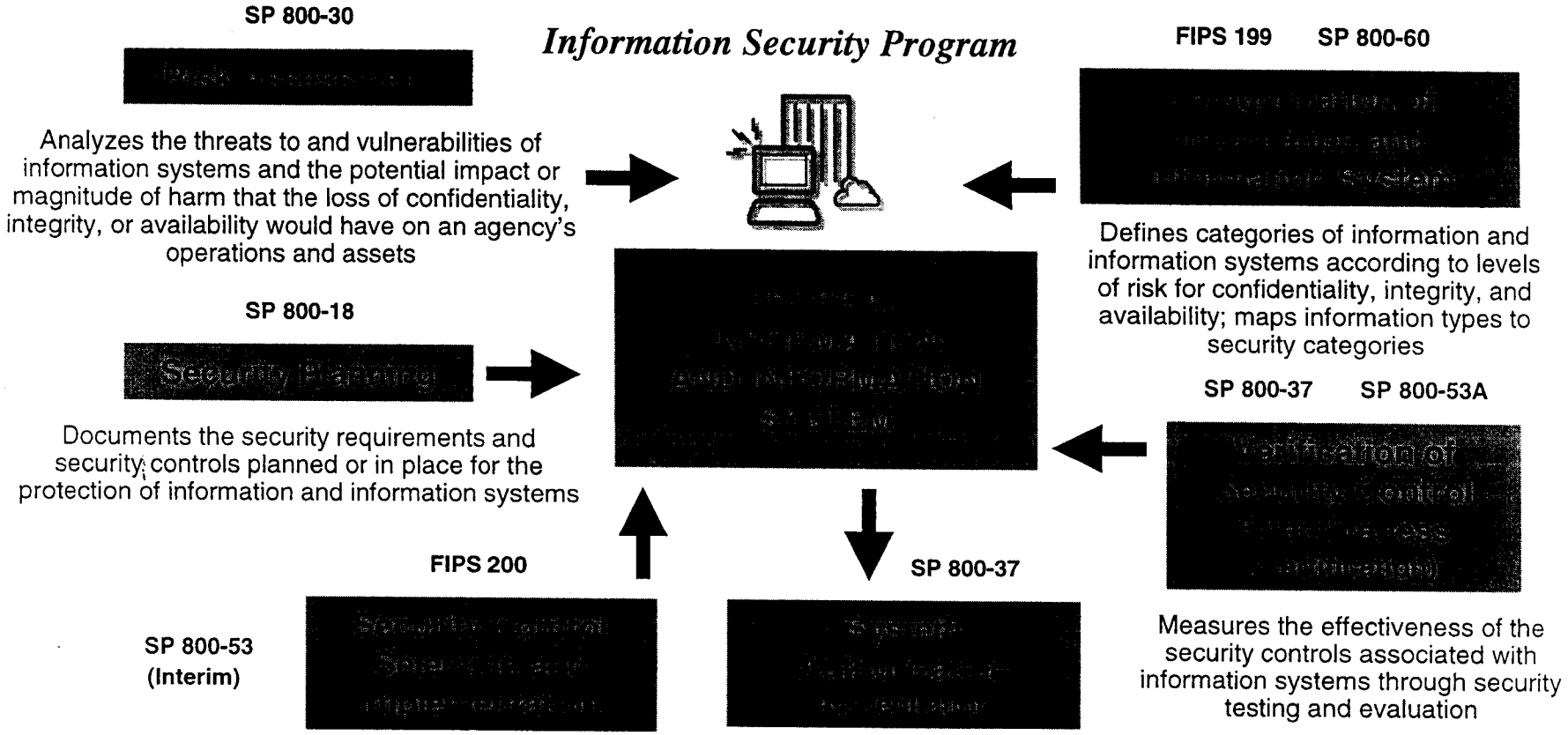
* NIST Special Publication 800-53, "Minimum Security Controls for Federal Information and Information Systems," projected for final publication in Spring 2004, will provide interim guidance until completion and adoption of FIPS 200.

Certification and Accreditation

General FISMA and OMB Requirement

- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical controls)
- Planning underway by NIST to develop:
  - Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"
  - Special Publication 800-53A, "Guide for Verifying the Effectiveness of Security Controls in Federal Information Systems"
  - Final Publication NLT Fall 2003 and Summer 2004 respectively
- Planning underway by NIST to update:
  - Special Publication 800-26, "Security Self-Assessment Guide for Information Systems"
  - Bring into alignment with security controls in SP 800-53

The Big Picture



Cyber Security Research and Development Act

Signed into Law by President Bush on 11-27-2002

Cyber Security Research and Development Act

- National Science Foundation
  - grants for basic research
  - support for higher education (many variants)
- NIST
  - research grants
  - cyber security checklists
  - in-house research:
    - Composability; SCADA; long-term/high-risk
  - Advisory Board and NRC study

Research Support

- to institutions of higher education that enter into partnerships with for-profit entities to support research to improve the security of computer systems

- Grants or Cooperative Agreements

Fellowships

- Post-Doctoral Research
  - engaged in research activities related to the security of computer systems

- Senior Research
  - individuals seeking research positions at institutions, including NIST
  - for established researchers at institutions of higher education who seek to change research fields and pursue studies related to the security of computer systems

Cyber Security Checklists

- Definition –

  a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal government.

- NIST would set priorities for development

Agency Use of Checklists (1)

- The Act does **NOT:**
  - require agencies to select the specific settings or options recommended by the checklist for the system;
  - establish conditions or prerequisites for Federal agency procurement or deployment of any such system;
  - represent an endorsement of any such system by NIST ; nor
  - preclude agencies from procuring or deploying other computer hardware or software systems for which no such checklist has been developed.

Agency Use of Checklists (2)

- If an agency uses a system for which a checklist is issued, the agency:
  - shall include in their program plan an explanation of how the agency has considered such checklist in deploying that system; (except for national security systems) and
  - may treat the explanation as if it were a portion of the agency's annual performance plan properly classified under criteria established by an Executive Order (within the meaning of section 1115(d) of title 31, United States Code).

Questions?