Federal Information Security Management Act (FISMA) Implementation

Federal Demonstration Partnership

January 13, 2012

Kevin Stine

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

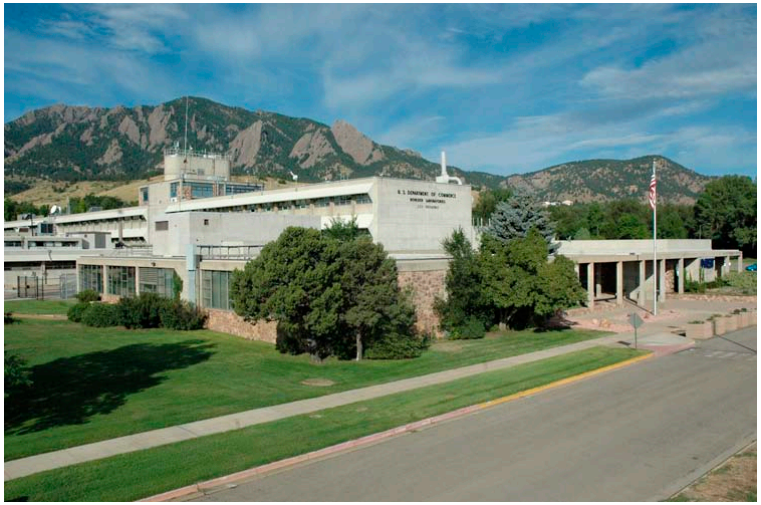
A Few Questions …

- What is FISMA?
- Who is NIST, and what does NIST have to do with FISMA and information security?
- Does FISMA apply to me?
- What does FISMA tell me to do?
- What is Risk Management, and how does it fit into FISMA?

NIST's Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology …

Credit: R. Rathe



Credit: NIST

… in ways that enhance economic security and improve our quality of life.

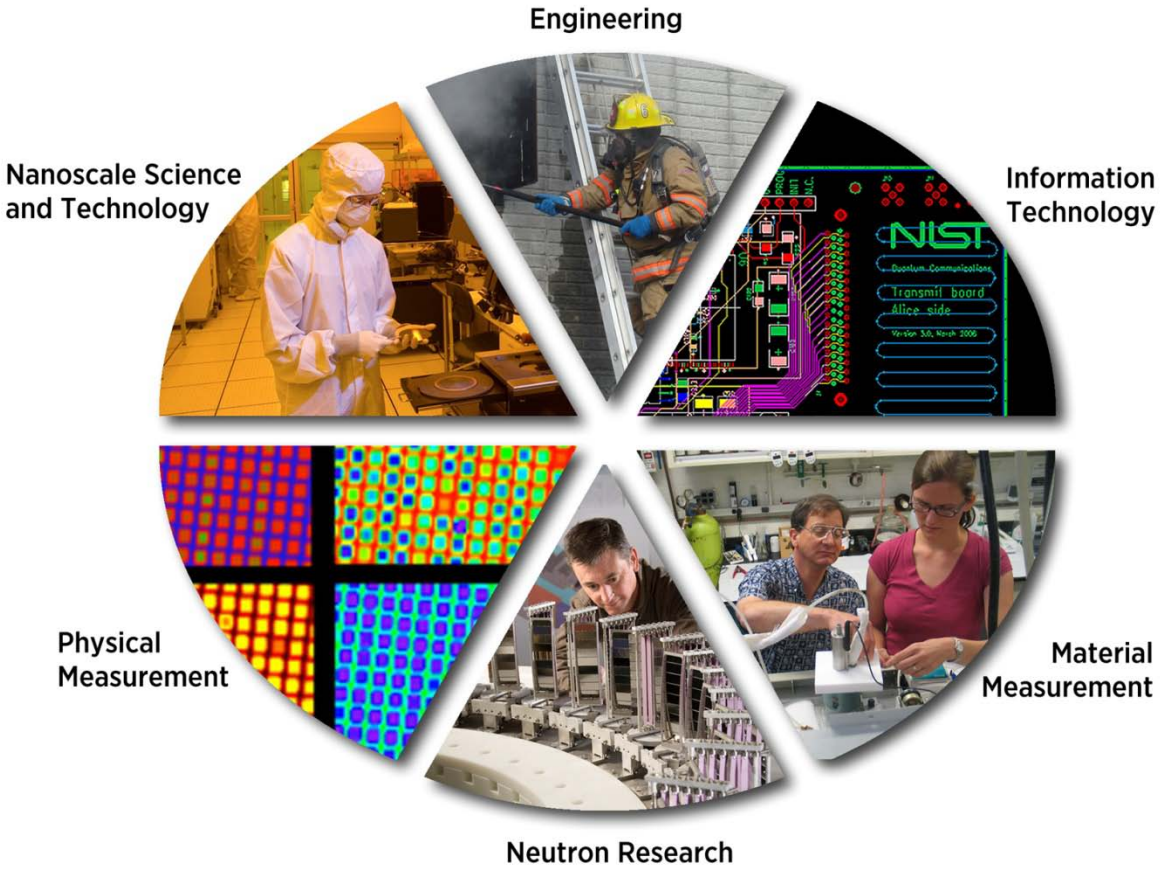
NIST Laboratories

NIST's work enables

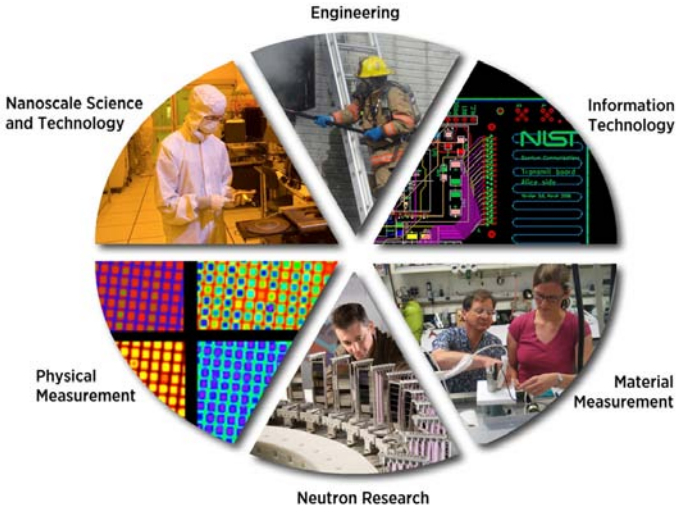
- Science
- Technology innovation
- Trade
- Public benefit

NIST works with

- Industry
- Academia
- Government agencies
- Measurement labs
- Standards organizations



Computer Security Division



A division within the Information Technology Lab, CSD conducts research, development and outreach necessary to provide standards and guidelines, mechanisms, tools, metrics and practices to protect information and information systems.

Some Major Activities
Cryptographic Algorithms, Secure Hash Competition, Authentication, Key Management, Crypto Transitions, DNSSEC, Post-Quantum Crypto, BIOS Security
FISMA, Health IT, Smart Grid, Supply Chain, NICE, Crypto Validation Programs, Outreach and Awareness, Cyber Physical Systems, Voting
Identity Management, Access Control, Biometric Standards, Cloud and Virtualization Technologies, Security Automation, Infrastructure Services and Protocols

Types of NIST Publications

- Federal Information Processing Standards (FIPS)
  - Developed by NIST; Approved and promulgated by Secretary of Commerce
  - Per FISMA, compulsory and binding for all federal agencies; not waiverable
  - Voluntary adoption by non-Federal organizations (e.g., state, local, tribal governments; foreign governments; industry; academia)

- Special Publications (SP 800 series)
  - Per OMB policy, Federal agencies must follow NIST guidelines
  - Voluntary adoption by non-Federal organizations

- Other security-related publications
  - NIST Interagency Reports

So, what is FISMA?

- **F**ederal **I**nformation **S**ecurity **M**anagement **A**ct

- Public Law 107-347: E-Government Act of 2002, Title III

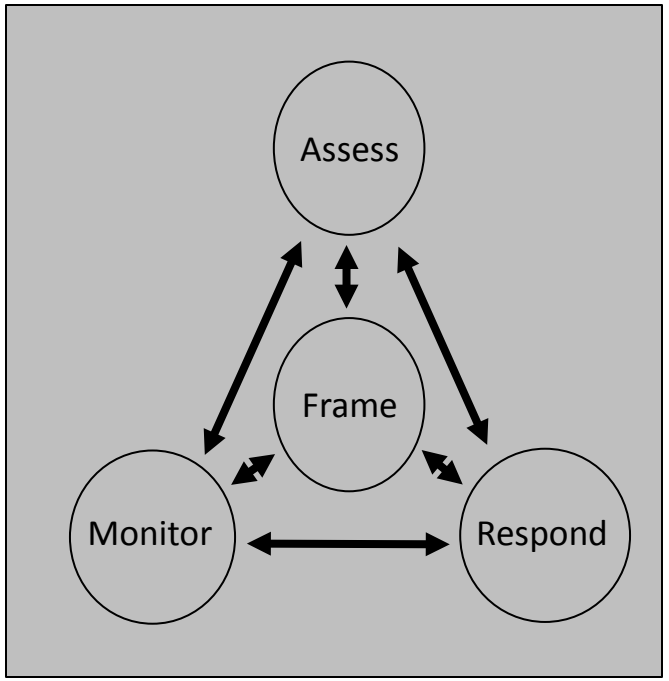
- "… provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets"

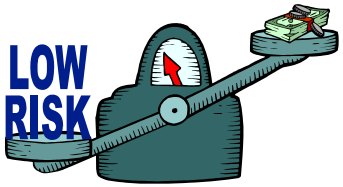
Risk Management is Central to FISMA

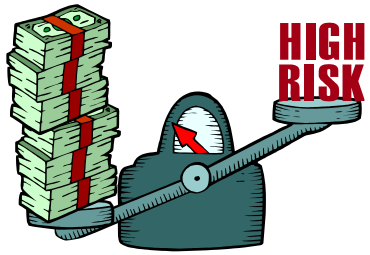
(and every other security framework)

- Determine risk tolerance
- Identify and assess risks
- Respond to risks
- Monitor risks over time

- No risk can be completely eliminated







Who has FISMA responsibilities?

- Office of Management and Budget
- Federal Agencies
  - Agency Head
  - CIO
- Inspectors General
- Comptroller General
- NIST

FISMA applies to …

- Federal agencies

- Organizations operating "on behalf of" federal agencies

Important Point – FISMA requirements follow agency information into any system which uses it or processes it on behalf of the agency.

What does FISMA require of Agencies?

- Among other things, develop and maintain an agency-wide information security program
  - Periodic assessment of risk and magnitude of harm to information and information systems
  - Risk-based, cost-effective policies and procedures that are compliant with OMB policies and promulgated standards
  - Security plans for networks, facilities, systems/groups of systems
  - Security awareness training (personnel and contractors)
  - Periodic testing and evaluation of security control effectiveness (management, operational, technical controls)
  - Procedures for managing remediation to address deficiencies and security incidents
  - Continuity of operations for information systems

What are NIST's FISMA Responsibilities?

- … developing standards, guidelines, and associated methods and techniques for information systems;

- … develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or other organization on behalf of an agency, other than national security systems …

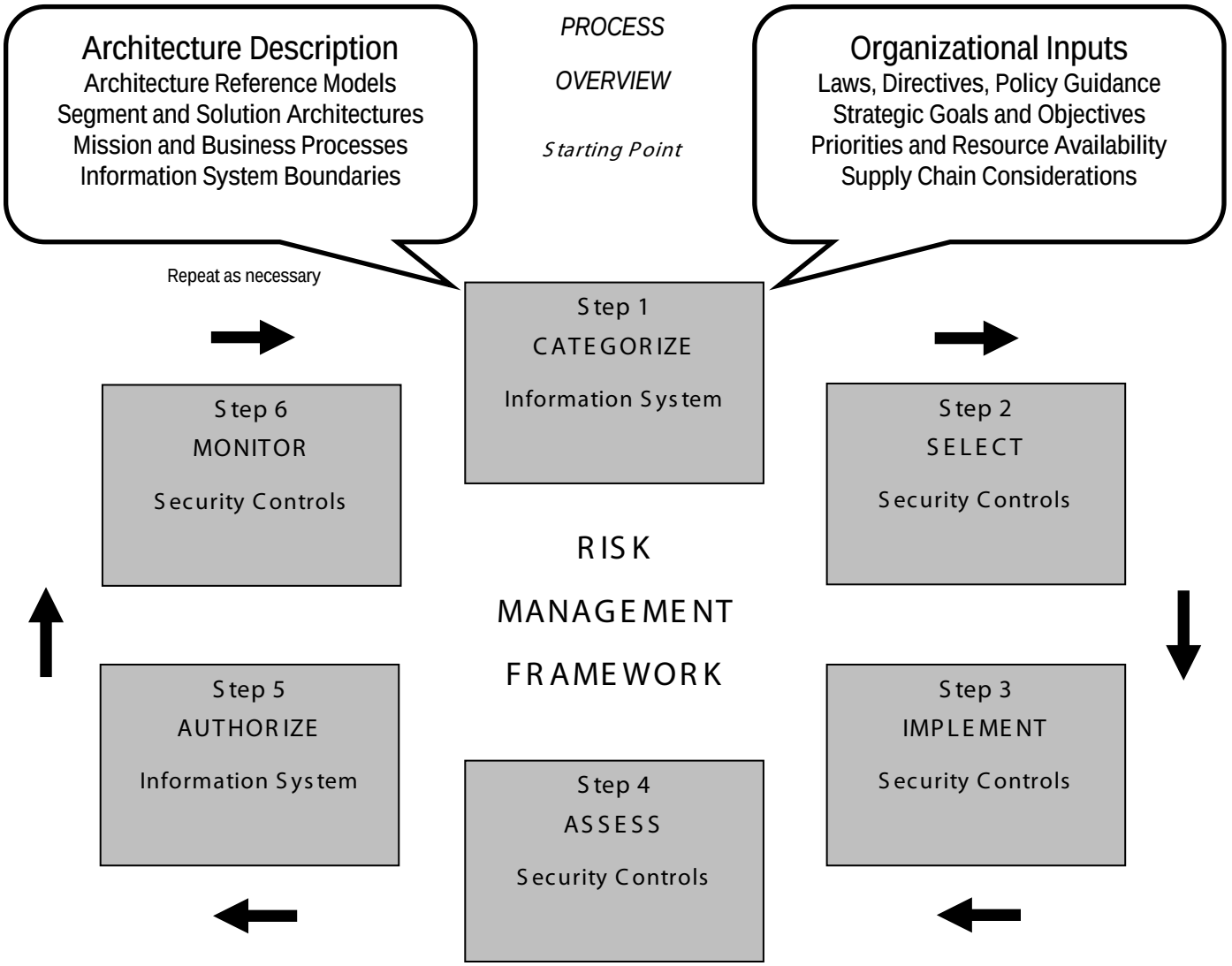
- … develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, …

Key FISMA Standards and Guidelines

- Standards
  - FIPS 199, Standards for Security Categorization of Federal Information and Information Systems *
  - FIPS 200, Minimum Security Requirements for Federal Information Systems *
- Guidelines
  - SP 800-30 (Risk Assessment)
  - SP 800-39 (Managing Information Security Risk)
  - SP 800-53 (Security Controls) *
  - SP 800-53A (Assessing Security Controls)
  - SP 800-60 (Security Categorization) *
  - SP 800-137 (Information Security Continuous Monitoring)

* *Called for in FISMA*

A Framework for Managing Risk



Some Closing Thoughts …

- Risk Management is essential.
- Don’t fear FISMA.
- Consider NIST Standards and Guidelines.
- Reach out to NIST – sec-cert@nist.gov

Questions…

Kevin Stine

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

Kevin.Stine@nist.gov