NIST Security Certification and Accreditation Project

An Integrated Strategy Supporting FISMA

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

Today's Climate

- Highly interactive environment of powerful computing devices and interconnected systems of systems across global networks
- Federal agencies routinely interact with industry, private citizens, state and local governments, and the governments of other nations
- The complexity of today's systems and networks presents great security challenges for both producers and consumers of information technology

The Advantage of the Offense

- Powerful attack tools now available over the Internet to anyone who wants them
- Powerful, affordable computing platforms to launch sophisticated attacks now available to the masses
- Little skill or sophistication required to initiate extremely harmful attacks

Result: The sophistication of the attack is growing, but the sophistication of the attacker is not.

Today's Challenges

- Adequately protecting information systems within constrained budgets
- Changing the current culture of:

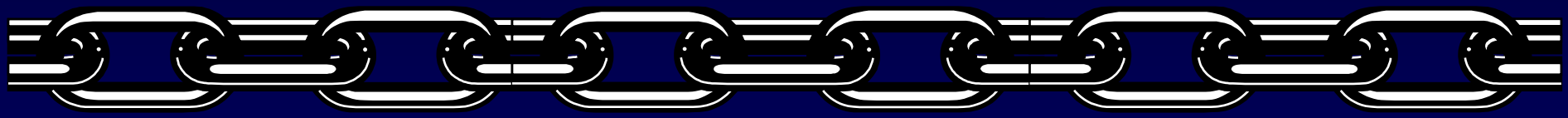
  "Connect first…ask security questions later"
- Bringing standards to:
  - Security controls for information systems
  - Verification procedures employed to assess the effectiveness of those controls

Assurance in Information Systems

Building more secure systems requires --

- Well defined system-level security requirements and security specifications
- Well designed component products
- Sound systems security engineering practices
- Competent systems security engineers
- Appropriate metrics for product/system testing, evaluation, and assessment
- Comprehensive system security planning and life cycle management

The Security Chain



Links in the Chain
(Non-technology based examples)

- ✓ Physical security
- ✓ Personnel security
- ✓ Procedural security
- ✓ Risk management
- ✓ Security policies
- ✓ Security planning
- ✓ Contingency planning

Links in the Chain
(Technology based examples)

- ✓ Access control mechanisms
- ✓ Identification and authentication devices
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls
- ✓ Smart cards
- ✓ Biometrics

Adversaries attack the weakest link…where is yours?

Supporting Tools and Programs

Building more secure systems is enhanced by --

- Standardized Security Requirements and Specifications
  - ✓ Government-sponsored protection profile development project
  - ✓ Private sector protection profile contributions
- Component-level Product Testing and Evaluation Programs
  - ✓ NIAP Common Criteria Evaluation and Validation Scheme
  - ✓ NIST Cryptographic Module Validation Program
- Security Implementation Guidance
  - ✓ NIST Special Publications
  - ✓ DoD Security Technical Implementation Guides
  - ✓ NSA Security Reference Guides
- System Certification and Accreditation

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 Tasks for NIST

- 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

Project Objectives

- Phase I: To develop standards and guidelines for:
  - ✓ Categorizing Federal information and information systems
  - ✓ Selecting and specifying security controls for Federal information systems; and
  - ✓ Verifying the effectiveness of security controls in Federal information systems

Phase II: To create a national network of accredited organizations capable of providing cost effective, quality security assessment services based on the NIST standards and guidelines

Significant Benefits

- More consistent and comparable specifications of security controls for information systems
- More consistent, comparable, and repeatable system-level evaluations of information systems
- More complete and reliable security-related information for authorizing officials
- A better understanding of complex information systems and associated risks and vulnerabilities
- Greater availability of competent security certification services

The Big Picture

Information Security Program

SP 800-30

Risk Assessment

Analyzes the threats to and vulnerabilities of information systems and the potential impact or magnitude of harm that the loss of confidentiality, integrity, or availability would have on an agency's operations and assets

SP 800-18

Security Planning

Documents the security requirements and security controls planned or in place for the protection of information and information systems

AGENCY INFORMATION AND INFORMATION SYSTEM

FIPS 199 SP 800-60

Categorization of Information and Information System

Defines categories of information and information systems according to levels of risk for confidentiality, integrity, and availability; maps information types to security categories

SP 800-37 SP 800-53A

Verification of Security Control Effectiveness (Certification)

Measures the effectiveness of the security controls associated with information systems through security testing and evaluation

SP 800-53 (Interim)

FIPS 200 (Final)

Security Control Selection and Implementation

Management, operational, and technical controls (i.e., safeguards and countermeasures) planned or in place to protect information and information systems

SP 800-37

Security Authorization (Accreditation)

The authorization of information systems to process, store, or transmit information, granted by a senior agency official, based on the effectiveness of security controls and residual risk

National Institute of Standards and Technology

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
- Project underway at NIST to develop:
  - ✓ Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"
  - ✓ Public Review Period: May 16th—August 16th 2003
  - ✓ Final Publication NLT December 2003

FIPS Publication 199

- Establishes 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
- Will be linked to the Federal Enterprise Architecture to show ***security traceability*** through reference models

Result

- Agencies will have a standard means of determining what *baseline security controls* are needed to adequately protect the information and information systems that support the operations and assets of the agency in order to:
  - ✓ accomplish its assigned missions
  - ✓ protect its assets
  - ✓ maintain its day-to-day functions
  - ✓ fulfill its legal responsibilities
  - ✓ protect individuals

Applicability

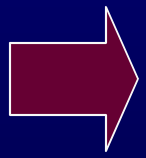
The standard shall apply to:

- All information within the Federal government other than that information that has been determined pursuant to Executive Order 12958 as amended by E.O. 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
- 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)

Security Categorization

Example: Mission Critical Information and Information System

Mapping Types of Information and Information Systems to FIPS Pub 199 Security Categories



	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

National Institute of Standards and Technology

Security Categorization

Example: Mission Critical Information and Information System

Mapping Types of Information and Information Systems to FIPS Pub 199 Security Categories

	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Baseline Security Controls for High Impact Systems

National Institute of Standards and Technology

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 Publication 199—
- Project underway at NIST to develop:
  - ✓ Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categorization Levels"
  - ✓ Initial Public Draft (Projected for publication, Fall 2003)

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—
- Project underway at NIST to develop:
  - ✓ Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Controls for Federal Information Systems"*
  - ✓ Final Publication NLT December 2005

* NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems", (Initial public draft projected for publication, October 2003), will provide interim guidance until completion and adoption of FIPS Publication 200.

Special Publication 800-53

Guide for the Selection and Specification of Security Controls for Federal Information Systems

- Provides a master catalog of security controls for information systems (incorporated from many sources (NIST SP 800-26, DoD Policy 8500, D/CID 6-3, ISO/IEC 17799, GAO FISCAM, HHS-CMS)
- Recommends baseline (minimum) security controls for information systems in accordance with security categories in FIPS Publication 199
- Provides guidelines for agency-directed tailoring of baseline security controls

Certification and Accreditation

- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical controls)
- Project underway at NIST to develop:
  - ✓ Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"
  - ✓ Special Publication 800-53A, "Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems"

Special Publication 800-37

Guide for the Security Certification and Accreditation of Federal Information Systems

- Establishes guidelines (including tasks and subtasks) to certify and accredit information systems supporting the executive branch of the Federal government
- Applicable to non-national security information systems as defined in the Federal Information Security Management Act of 2002
- Replaces Federal Information Processing Standards (FIPS) Publication 102

Special Publication 800-53A

Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems

- Provides standardized techniques and procedures for independent certification agents to verify the effectiveness of security controls
- Provides a single baseline verification procedure for each security control in SP 800-53
- Allows additional verification techniques and procedures to be applied at the discretion of the agency

NIST Standards and Guidelines

Are intended to promote and facilitate—

- More consistent, comparable specifications of security controls for information systems
- More consistent, comparable, and repeatable system evaluations of information systems
- More complete and reliable security-related information for authorizing officials
- A better understanding of complex information systems and associated risks and vulnerabilities
- Greater availability of competent security certification services

Key Milestones

- NIST Special Publication 800-53
  Initial Public Draft: October 2003
- NIST Special Publication 800-60
  Initial Public Draft: Fall 2003
- FIPS Publication 199
  Final: December 2003
- NIST Special Publication 800-37
  Pre-Publication Final: December 2003
- NIST Special Publication 800-53A
  Initial Public Draft: Spring 2004

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Manager
Dr. Ron Ross
(301) 975-5390
rross@nist.gov

Assessment Scheme
Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Special Publications
Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Organization Accreditations
Patricia Toth
(301) 975-5140
patricia.toth@nist.gov

Gov't and Industry Outreach
Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Technical Advisor
Gary Stoneburner
(301) 975-5394
gary.stoneburner@nist.gov

Comments to: sec-cert@nist.gov
World Wide Web: http://csrc.nist.gov/sec-cert