NIST Security Certification and Accreditation Project

An Integrated Strategy Supporting FISMA

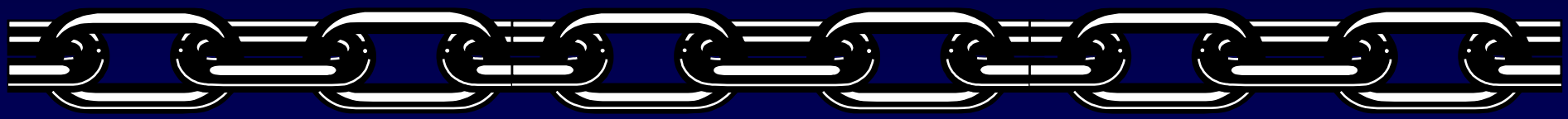
Dr. Ron Ross

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 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?

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

National Policy

Office of Management and Budget Circular A-130, *Management of Federal Information Resources* requires Federal agencies to:

- Plan for security
- Ensure that appropriate officials are assigned security responsibility
- Authorize system processing prior to operations and periodically, thereafter.

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

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

AGENCY INFORMATION AND INFORMATION SYSTEM

SP 800-18

Security Planning

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

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