FISMA Implementation Project

The Associated Security Standards and Guidelines

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

National Institute of Standards and Technology

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

National Institute of Standards and 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 <u>attack</u> is growing, but the sophistication of the <u>attacker</u> is not.

National Institute of Standards and Technology

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)

- ✓ Security policies and procedures
- ✓ Risk management
- ✓ Security planning
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Physical security
- ✓ Personnel security

Links in the Chain
(Technology based examples)

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

Adversaries attack the weakest link…where is yours?

National Institute of Standards and Technology

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**

National Institute of Standards and Technology

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
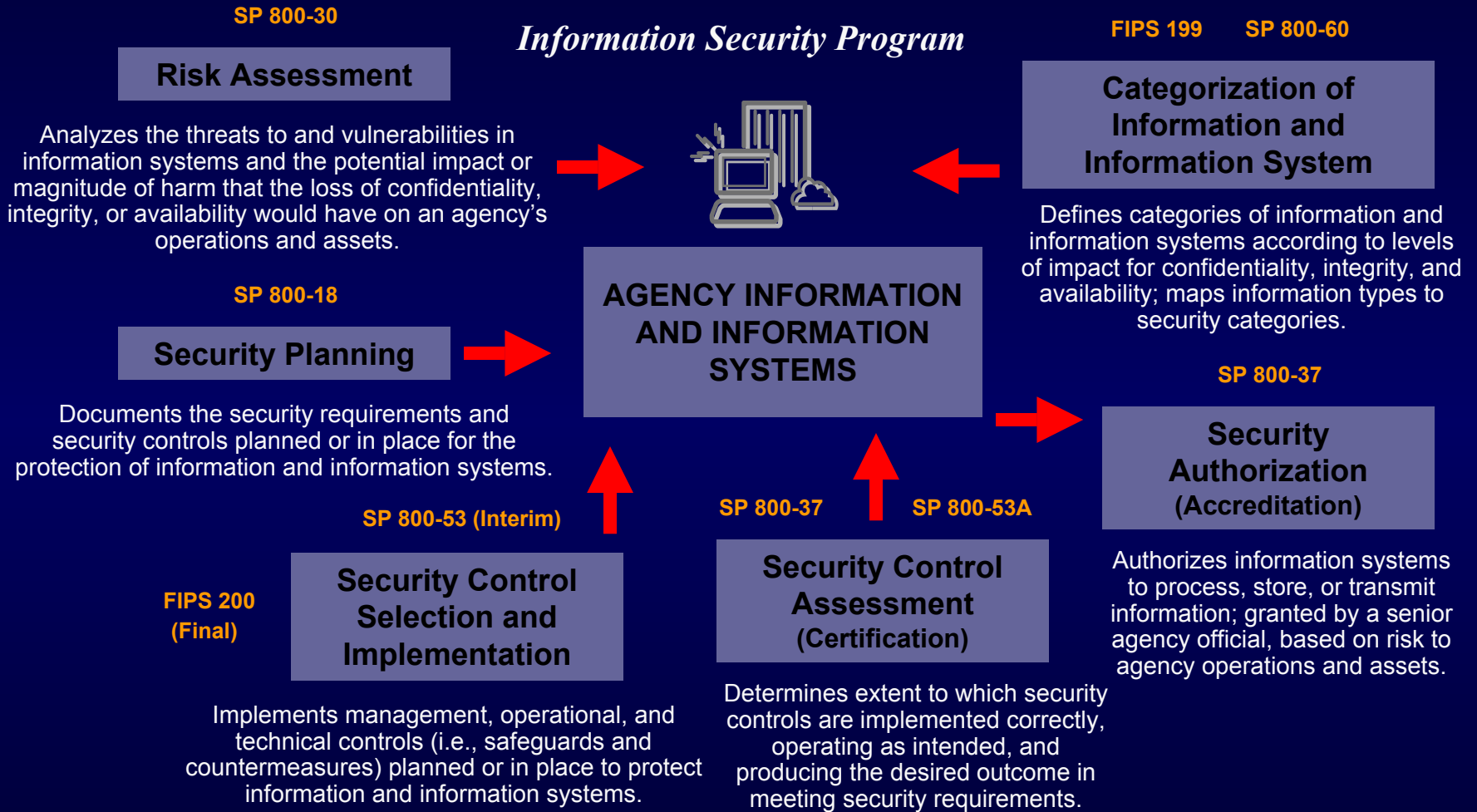
Project Objectives

- Phase I: To develop standards and guidelines for:
  - Categorizing Federal information and information systems
  - Selecting and specifying security controls for Federal information systems; and
  - Assessing 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 assessments 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 Framework

Information Security Program

SP 800-30

Risk Assessment

Analyzes the threats to and vulnerabilities in 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.

FIPS 199   SP 800-60

Categorization of Information and Information System

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

AGENCY INFORMATION AND INFORMATION SYSTEMS

SP 800-37

Security Authorization (Accreditation)

Authorizes information systems to process, store, or transmit information; granted by a senior agency official, based on risk to agency operations and assets.

SP 800-53 (Interim)

FIPS 200 (Final)

Security Control Selection and Implementation

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

SP 800-37   SP 800-53A

Security Control Assessment (Certification)

Determines extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome in meeting security requirements.

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

- Publication status:
  - ✓ 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 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

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

- Publication status:
  - ✓ NIST Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories"
  - ✓ Initial Public Draft (December 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—

- Publication status:
  - ✓ Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Controls for Federal Information Systems"*
  - ✓ Final Publication December 2005

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

National Institute of Standards and Technology

Special Publication 800-53
Recommended Security Controls for Federal Information Systems

- Provides a master catalog of security controls for information systems (incorporated from many sources including 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

National Institute of Standards and Technology

Applicability

- Applicable to all Federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542

- Broadly developed from a technical perspective to complement similar guidelines issued by agencies and offices operating or exercising control over national security systems

Security Controls

- The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

  -- [FIPS Publication 199, December 2003]

Key Questions

- What security controls are needed to adequately protect an information system that supports the operations and assets of the organization?

- Have the selected security controls been implemented or is there a realistic plan for their implementation?

- To what extent are the security controls implemented correctly, operating as intended, and producing the desired outcome?

National Institute of Standards and Technology

Catalog of Security Controls

- Contains 166 entries currently

- Organized by classes and families

- Includes three levels of security control strength (basic, enhanced, and strong) when appropriate and technically feasible

- Dynamic in nature allowing revisions and extensions to security controls to meet changing requirements and technologies

National Institute of Standards and Technology

Security Control Structure

- Section I: *Control Objective*
  - Provides the overall objective for the particular security control when applied to an information system
- Section II: *Control Mapping*

  - Lists source documents considered during development of the control catalog that have similar security controls, (e.g., FISCAM, DoD 8500, ISO 17799, NIST SP 800-26, DCID 6/3, HHS CMS)

- Section III: *Control Description*
  - Provides the specific control requirements and details of each control

National Institute of Standards and Technology

Security Control Example

Class: Management   *Family: Security Control Review*

CR-2   **VULNERABILITY SCANNING**

Control objective: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically scan for vulnerabilities in the information system.

Control mapping: [NIST 800-26: 2.1.4; ISO-17799: 12.2.2; DCID 6/3: SysAssur3-b; DOD 8500: VIVM-1]

CR-2.b   Basic control: Vulnerability assessment tools are implemented by the organization and personnel are trained in their use. The organization conducts periodic testing of the security posture of the information system by scanning the system with vulnerability detection tools every [*Assignment: time period (e.g., every 6 months)*].

National Institute of Standards and Technology

Security Control Example

Class: Management   *Family: Security Control Review*

CR-2   **VULNERABILITY SCANNING**

Control objective: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically scan for vulnerabilities in the information system.

CR-2.e   Enhanced control: Vulnerability assessment tools are implemented by the organization and personnel are trained in their use. The organization conducts periodic testing of the security posture of the information system by scanning the system with vulnerability detection tools every [*Assignment: time period (e.g., every 6 months)*]. Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. The list of vulnerabilities scanned is updated periodically, at least prior to each periodic scan. Vulnerability scanning procedures include vulnerability list update and vulnerability scan when a significant, new vulnerability is announced. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

National Institute of Standards and Technology

Security Control Example

Class: Management   *Family: Security Control Review*

CR-2 **VULNERABILITY SCANNING**

<u>Control objective</u>: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically scan for vulnerabilities in the information system.

CR-2.s <u>Strong control</u>: Vulnerability assessment tools are implemented by the organization and personnel are trained in their use. The organization conducts periodic testing of the security posture of the information system by scanning the system with vulnerability detection tools every [*Assignment: time period (e.g., every 6 months)*]. Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. The list of vulnerabilities scanned is updated periodically, at least prior to each periodic scan. Vulnerability scanning procedures include vulnerability list update and vulnerability scan when a significant, new vulnerability is announced. Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

National Institute of Standards and Technology

Security Controls

- ## Management Controls

  - Safeguards and countermeasures employed by an organization to manage the security of the information system and the associated risk to the organization's assets and operations

- ## Operational Controls

  - Safeguards and countermeasures employed by an organization to support the management and technical security controls in the information system (typically executed by people, not systems)

- ## Technical Controls

  - Safeguards and countermeasures (typically described as security mechanisms) employed within the information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction

National Institute of Standards and Technology

Management Controls

Families of Controls

- Risk Assessment

- Security Planning

- System and Services Acquisition

- Security Control Review

- Processing Authorization

Operational Controls

Families of Controls

- Personnel Security

- Physical and Environmental Protection

- Contingency Planning and Operations

- Configuration Management

- Hardware and Software Maintenance

National Institute of Standards and Technology

Operational Controls

Families of Controls

- System and Information Integrity

- Media Protection

- Incident Response

- Security Awareness and Training

National Institute of Standards and Technology

Technical Controls

Families of Controls

- Identification and Authentication

- Logical Access Control

- Accountability (Including Audit)
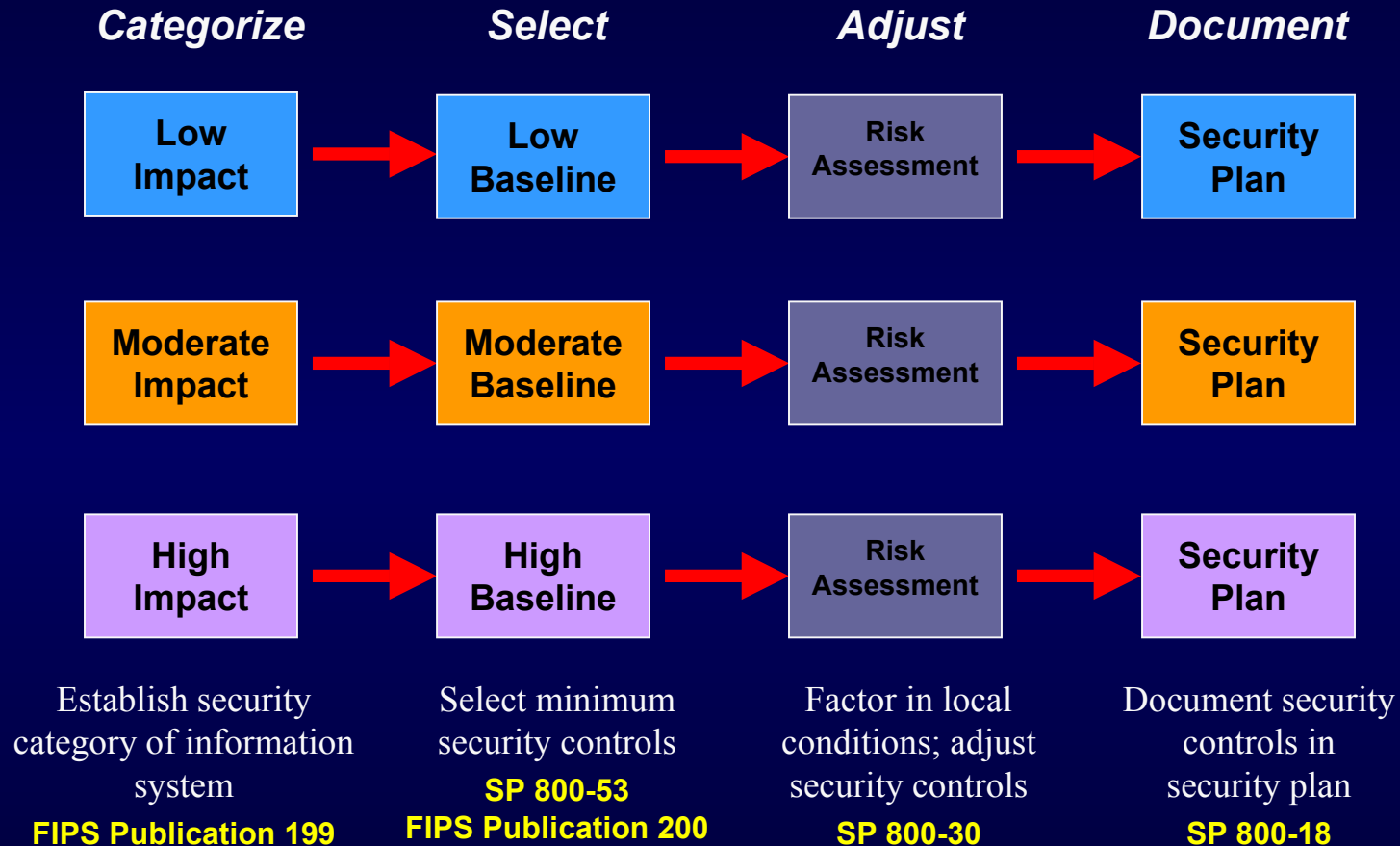
- System and Communications Protection

Baseline Security Controls

- Three sets of baseline (minimum) security controls defined for security categories in accordance with FIPS Publication 199

- Each set of security controls in the respective baselines (i.e., low, moderate, high) provides an estimated threat coverage

- For identifiable threat sources, security controls in the baselines provide: (i) full coverage; (ii) partial coverage; or (iii) no coverage

Baseline Security Controls

- Baseline security controls provide a *starting point* for organizations and communities of interest in their security control selection process

- The security control set can be tailored by organizations based on results of risk assessments and/or specific security requirements (e.g., HIPAA, Gramm-Leach-Bliley)

- The final agreed upon set of security controls is documented in the system security plan

Control Selection Process

Categorize	Select	Adjust	Document
Low Impact →	**Low Baseline** →	**Risk Assessment** →	**Security Plan**
Moderate Impact →	**Moderate Baseline** →	**Risk Assessment** →	**Security Plan**
High Impact →	**High Baseline** →	**Risk Assessment** →	**Security Plan**
Establish security category of information system **FIPS Publication 199**	Select minimum security controls **SP 800-53** **FIPS Publication 200**	Factor in local conditions; adjust security controls **SP 800-30**	Document security controls in security plan **SP 800-18**

National Institute of Standards and Technology

Certification and Accreditation

- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical controls)

- Publication status:
  - ✓ NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"
  - ✓ NIST Special Publication 800-53A, "Assessing the 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

National Institute of Standards and Technology

Special Publication 800-53A

Assessing the Security Controls in Federal Information Systems

- Provides standardized assessment methods and procedures to determine the extent to which the security controls in an information system are:

  - Implemented correctly

  - Operating as intended

  - Producing the desired outcome with respect to meeting system security requirements

- Allows additional methods procedures to be applied at the discretion of the agency

National Institute of Standards and Technology

FISMA Implementation Project
Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- NIST Special Publication 800-37 (C&A)
- NIST Special Publication 800-53 (Security Controls)
- NIST Special Publication 800-53A (Assessment)
- NIST Special Publication 800-59 (National Security)
- NIST Special Publication 800-60 (Category Mapping)
- FIPS Publication 200 (Minimum Security Controls)

National Institute of Standards and Technology

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

Contact Information

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

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

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

Special Publications
Joan Hash
(301) 975-3357
joan.hash**@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

National Institute of Standards and Technology