

NIST Cyber Security Activities

Dr. Alicia Clay

Deputy Chief, Computer Security Division

NIST Information Technology Laboratory

U.S. Department of Commerce

September 29, 2004

The background of the slide is a photograph of a large, modern, multi-story office building with a grid-like facade of windows. The building is set against a sky with soft, white and grey clouds. In the foreground, there are some trees and a paved area. The overall lighting is bright, suggesting a clear day.

NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's primary mission is to promote economic growth by working with industry to develop and apply technology, measurements, and standards.

NIST carries out its mission through a portfolio of four programs:

Measurement and Standards Laboratories

provides technical leadership for the Nation's measurement and standards infrastructure, and assures the availability of essential reference data and measurement capabilities

Advanced Technology Program

stimulates U.S. economic growth by developing high risk and enabling technologies through industry-driven cost-shared partnerships

Manufacturing Extension Partnership

strengthens the global competitiveness of smaller U.S.-based manufacturing firms by assisting in the adoption of advanced technologies, techniques, and business practices

National Quality Program

enhances U.S. competitiveness, quality, and productivity, manages the Malcolm Baldrige National Quality Award, and provides global leadership in promoting quality awareness

Computer Security Division Mission

Mission: To improve information systems security by:

- Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;
- Developing standards, metrics, tests and validation programs:
 - to promote, measure, and validate security in systems and services
 - to educate consumers and
 - to establish minimum security requirements for Federal systems
- Developing guidance to increase secure IT planning, implementation, management and operation.

Cyber Security Statutory Mandates

Federal Information Security Management Act of 2002

Federal security standards and guidelines

Minimum requirements;
categorization standards,
incident handling,
NSS identification, ...
Support of ISPAB

Cyber Security Research and Development Act of 2002

Extramural research support
Fellowships
Intramural research
Checklists
NRC study support

Current NIST Computer Security Activities

Cryptographic Standards and E-Authentication

- Establish secure cryptographic standards for storage and communications & enable cryptographic security services in e-Government applications through electronic authentication and key management protocols

Emerging Technologies

- Identify & exploit emerging technologies especially infrastructure niches
- Develop prototypes, reference implementations, and demonstrations
- Transition new technology and tools to public & private sectors
- Develop the tests, tools, profiles, methods, and implementations for timely, cost effective evaluation and testing

Management and Assistance

- Provide computer security guidance to ensure sensitive government information technology systems and networks are sufficiently secure to meet the needs of government agencies and the general public
- Serve as focal point for Division outreach activities
- Facilitate exchange of security information among Federal government agencies

Security Testing

- Improve the security and quality of IT products
- Foster development of test methods, tools, techniques, assurance metrics, and security requirements
- Promote the development and use of tested and validated IT products
- Champion the development and use of national/international IT security standards

Recently Completed NIST Security Guidelines

- 800-30, *Risk Management Guide for Information Technology Systems*
- 800-31, *Intrusion Detection Systems*
- 800-34, *Contingency Planning Guide for Information Technology System*
- 800-37, *Security Certification and Accreditation*
- 800-40, *Procedures for Handling Security Patches*
- 800-41, *Guidelines on Firewalls and Firewall Policy*
- 800-42, *Guideline on Network Security Testing*
- 800-44, *Guidelines on Securing Public Web Servers*
- 800-45, *Guidelines on Electronic Mail Security*
- 800-46, *Security for Telecommuting and Broadband Communications*
- 800-47, *Security Guide for Interconnecting Information Technology Systems*
- 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*
- 800-63, *Electronic Authentication Guideline*
- 800-67, *Recommendation for the Triple Data Encryption Algorithm Block Cipher*

Select Guidelines Under Development

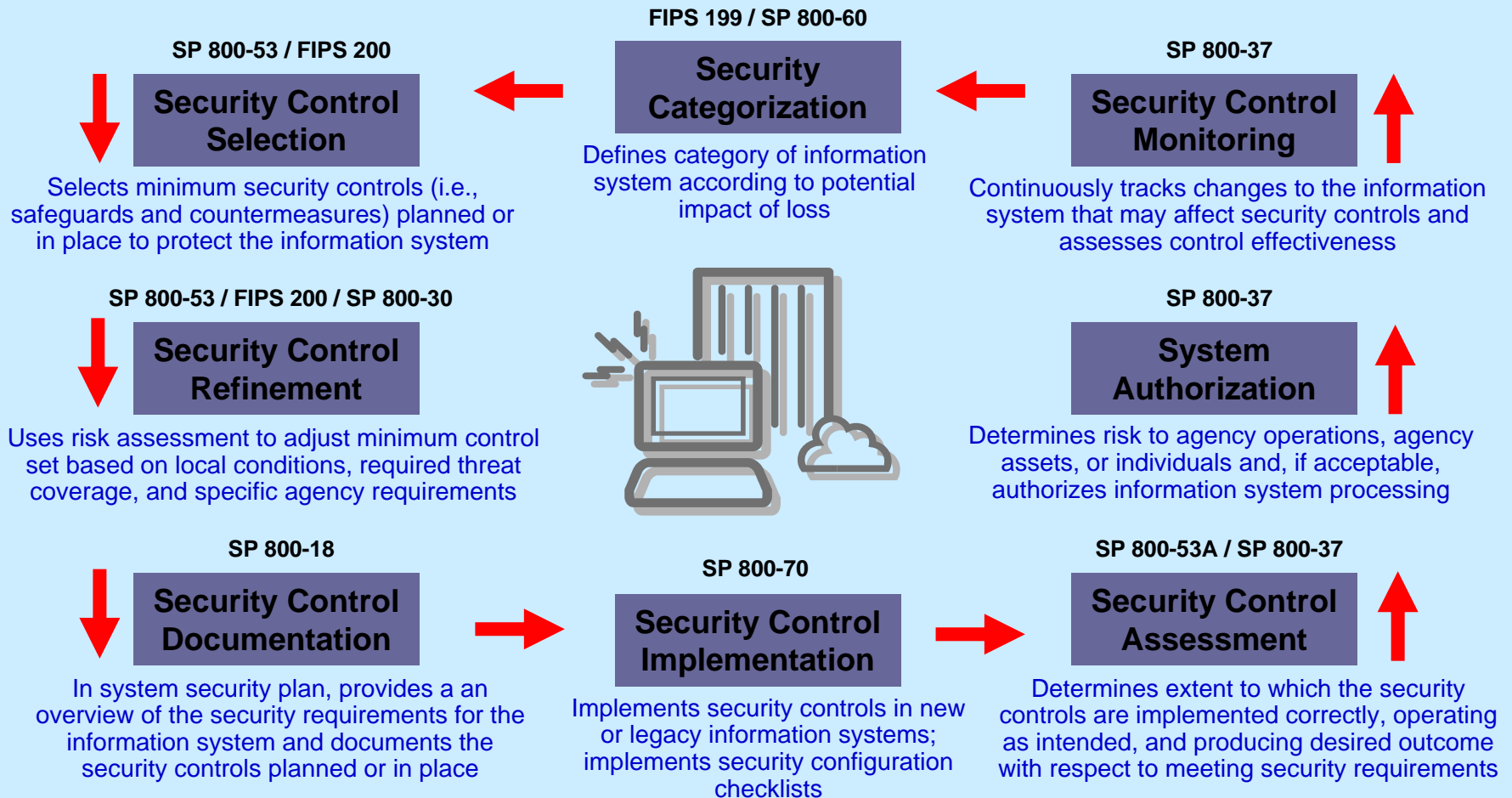
- 800-53, *Security Controls for Federal Information Systems (DRAFT)*
- 800-56, *Recommendation on Key Establishment Schemes (DRAFT)*
- 800-57, *Recommendation on Key Management (DRAFT)*
- 800-58, *Security Considerations for Voice Over IP (DRAFT)*
- 800-61, *Computer Security Incident Handling Guide (DRAFT)*
- 800-65, *Integrating Security into the Capital Planning and Investment Control Process (DRAFT)*
- 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (DRAFT)*
- 800-68, *Securing Microsoft Windows XP Systems for IT Professionals (DRAFT)*
- 800-70, *The NIST Security Configuration Checklists Program (DRAFT)*
- 800-72, *Guidelines on PDA Forensics (DRAFT)*

-
- *Media Destruction/Sanitization*
 - *Penetration Testing & Vulnerability Management*
 - *Trust frameworks*

3 High Visibility Projects

- Minimum Standards for all Federal Systems
- Cyber Security Checklists
- Personal Identity Verification

Risk Management Framework



Cyber Security Checklists

- Task to NIST ... Develop checklists:
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 developing web-based database
- DHS Support
- FISMA requirements for agencies
- 800-70 out for comment
- ~December 2004 – Target for Launch
- Outreach – NCSP, CISWG, ITAA, BSA, etc.

Personal Identity Verification

HSPD #12 – Six Month Deadline to create a secure and reliable automated system that may be used Government-wide to:

- 1) Establish the authentic true identity of an individual;
- 2) Issue an identity credential token to each authenticated individual containing an “electronic representation” of the identity and the person to whom it is issued which can later be verified using appropriate technology when access to a secure Federal facility or information system is requested;
- 3) Provide graduated criteria that provide appropriate levels of assurance and security to the application;
- 4) Be strongly resistant to identity fraud, counterfeiting, and exploitation by individuals, terrorist organizations, or conspiracy groups;
- 5) Initiate development and use of interoperable automated systems meeting these requirements.

Deployment of Outcomes

What

- Guidelines and standards

How

- Buy-in through collaboration
- Bulletins and brochures
- Workshops (examples)
- Strong Web Presence
<http://csrc.nist.gov>
- PRISM
- Direct agency support
- Voluntary standards participation
- Sharing information with other National Bodies

Objectives

NIST's cyber security work provides:

- Increased protection against cyber security disruptions;
- Increased trust and confidence in the security of the IT infrastructure leading to increased usage for transactions, increased productivity, and enhanced flexibility of use;
- Improved cyber security for government information systems enhancing the ability of agencies to deliver services electronically and ensuring continuity of operations; and
- Decreased life-cycle costs of government IT