Securing Federal Information Systems and Beyond: *NIST Activities and Plans*

Ed Roback

Chief, Computer Security Division

September 2004

National Institute of Standards and Technology

NIST

Cybersecurity at the NIST Information Technology Laboratory

Building Trust and Confidence in IT Systems -- The context of our Security Work

Do systems ---

Operate as intended?	**Conformity**
Meet user needs?	**Utility**
Provide reliable service	**Reliability**
Pose a threat to human life/limb?	**Safety**
Talk to other systems when needed?	**Interoperability**
Protect	**Security**
data against unauthorized change?	**Integrity**
confidential data against unauthorized disclosure?	**Confidentiality**
Operate when/where needed?	**Availability**
Protect personal privacy?	Privacy

NIST 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

Non-national security systems

Other Assignments

- HAVA – Security of Voting Systems
- Homeland Security Presidential Directive #12

U.S. Federal Security Roles

Congress/ OMB – Government-wide policy/oversight role

Unclassified Systems

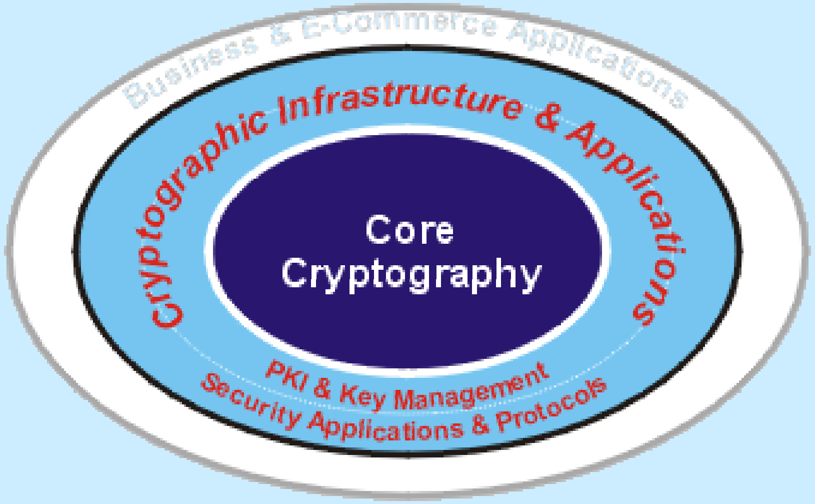
- NIST – standards, guidelines, security research (in-house and academic-industry partnerships)
  - Federal Information Security Management Act of 2002
  - Cyber Security Research and Development Act of 2002
- DHS – Day-to-day security alerts, operations, etc.
  - National Cyber Security Division in IAIP
- NSF – Academic research support
  - Cyber Security Research and Development Act of 2002

Classified Systems

A. National Security Systems – "Committee on National Security Systems"

B. Intelligence Systems – Director of Central Intelligence

Cryptographic Standards and Applications


Business & E-Commerce Applications
Cryptographic Infrastructure & Applications
Core Cryptography
PKI & Key Management
Security Applications & Protocols

Goals

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

Technical Areas

- Secure encryption, authentication, non-repudiation, key establishment, & random number generation algorithms.
- Standards & guidance for e-Gov & e-Authentication
- PKI standards, interoperability, assurance & scalability

Impacts

- Strong cryptography used in COTS IT products
- Standardized PKI & cryptography improves interoperability
- Availability of secure applications through cryptography

Collaborators

Industry: ANSI X9, IETF PKIX, Baltimore Technologies, Certicom, Cylink, Digital Signature Trust, RSA Security, Entrust Technologies, E-Lock Technologies, Getronics, IBM, ID Certify, Mastercard, Microsoft, Motorola, Netscape, Spyrus, Network Associates, VeriSign, Verizon, Visa, World Talk, public commenters

Federal: Department of Treasury**,** Agencies participating in Federal PKI Steering Committee and Bridge CA Project, FDIC, NSA

Projects

- ***Cryptographic Standards & Guidelines***
  - Cryptographic Standards Toolkit
  - Key Management Guidance
  - Modes for Block Cipher Algorithms
- ***Infrastructure & Applications***
  - Industry and Federal Security Standards
  - Identity Management and e-Authentication
  - Identity Management Infrastructure
  - Securing e-Gov Applications With Cryptography
  - Security Testing for e-Commerce Components

Some specifics…

Upcoming cryptographic-based standards activities

Key Management

- Recommendation on Key Establishment Schemes Using Discrete Logarithm Cryptography
  - Diffie-Hallman and MQV using Finite Field and Elliptic Curve Cryptography
  - Special Publication 800-56: public comment (1Q, FY2005); complete (2Q, FY2005); testing (4Q, FY2005?)

Tentative plans; budget permitting

Key Management (contd.)

- Recommendation for Key Management

  SP 800-57, Part 1: General (Guidance on using and handling cryptographic material)

  - Public comment (1Q, FY2005); complete (2Q, FY2005)

  SP 800-57, Part 2: Best Practices for Key Management Organizations

  - Public comment (1Q, FY2005); complete (2Q, FY2005)

  SP 800-57, Part 3: Application-Specific Key Management Guidance

  - Public comment (2Q, FY2005); complete (3Q, FY2005)

Tentative plans; budget permitting

Block Cipher Modes of Operation

- Authentication Mode (CMAC): SP 800-38B

  Public comment (1Q, FY2005); complete (2Q, FY2005); testing (3Q, FY2005)

- Key Wrapping: SP 800-38D

  Public comment (3Q, FY2005); complete (1Q, FY2006)

Tentative plans; budget permitting

Digital Signature Standard

- Revision of FIPS 186-2
- Public comments (1Q, FY2005); signed by Secretary of Commerce (3Q, FY2005?); testing (4Q, FY2005)

Tentative plans; budget permitting

Random Number Generation

- Working in conjunction with ANSI; considering how to recommend for Federal government use
- Complete drafts (4Q, FY2005?); public comments for NIST recommendation (1Q, FY2006?); complete (3Q, FY2006?); testing (4Q, FY2006?)

Tentative plans; budget permitting

Research & Emerging Technologies

Goals

- 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

Technical Areas

- Authorization Management, Access Control, System Management
- Vulnerability Analysis, Intrusion Detection, Attack Signatures
- Mobile Code, Agents, Aglets, Java, Smart Cards
- Models, Cost-models, Prototyping, Reference Implementations
- Automated Testing, Security Specification

Impacts

- Better cheaper and more intuitive methods of authorization management
- Creating internal competence in emerging technologies (i.e. mobile devices)
- World class vulnerability search engine
- RBAC Economic Impact Study

Collaborators

Industry: IBM, Microsoft, SUN, Boeing, Intel, Booz Allen, VDG, SCC, Sybase, SAIC, SUN, Lincoln Labs, Lucent, ISS, Symantec, 3Com, Interlink, Ford, CISCO, Lucent, Checkpoint, CIS, Oracle, MITRE, Network Access Consortium, Intel, SANS Institute

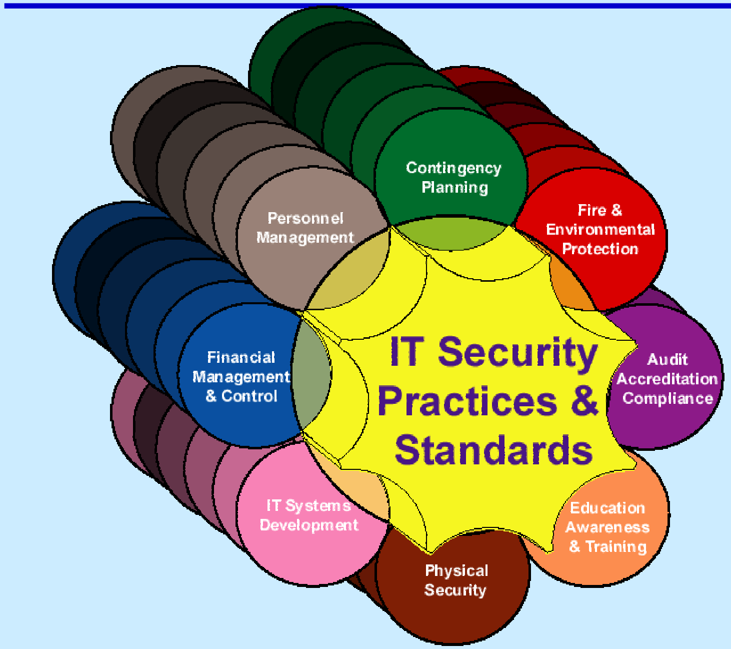
Academic: U Maryland, Ohio State, U Tulsa, George Mason, Rutgers U, Purdue , George Washington, U of W. Fla, UCSD, UMBC

Federal: NSA, DoD, NRL, DARPA, DoJ

Major Projects

- Smart Card Infrastructure
- Wireless/ Mobile Device Security
- Access Control & Authorization Management
- Technical Guidance
- ICAT Vulnerability/Patch Search Tool
- IPsec
- IDS
- Quantum Computing Support
- CIP Grants
- Checklists/Benchmarks

Security Management and Assistance


Contingency Planning
Fire & Environmental Protection
Personnel Management
IT Security Practices & Standards
Financial Management & Control
Audit Accreditation Compliance
IT Systems Development
Education Awareness & Training
Physical Security

Goals

- 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

Technical Areas

- Computer security policy/management guidance
- Computer Security Expert Assist Team (CSEAT) security support to Federal agencies
- Outreach to government, industry, academia, citizens

Impacts

- Agencies use standard, interoperable solutions
- Improved federal agency computer security programs
- Reduced costs to agencies from reduction of duplication of efforts
- Use of "Shared Security Practices" among federal agencies

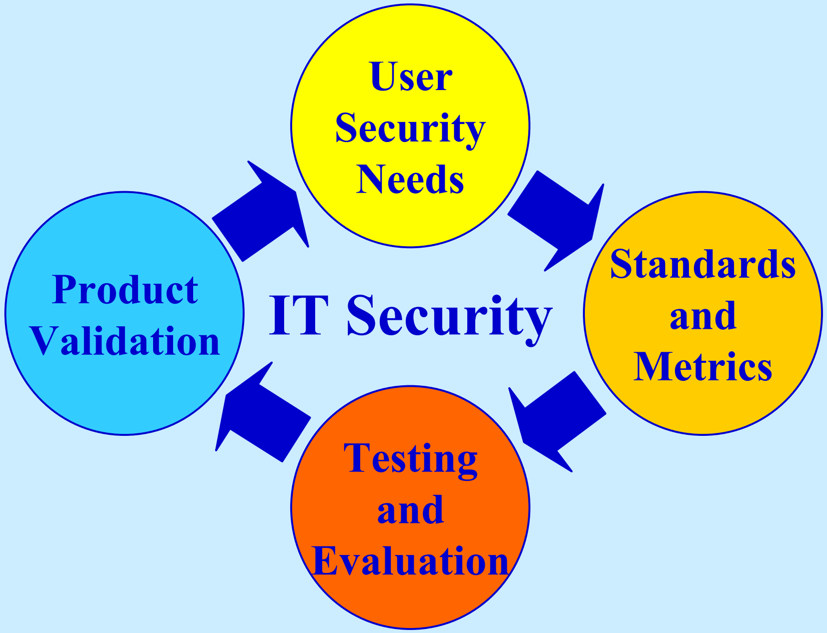
Collaborators

Federal: All Federal Agencies
Federal Computer Security Program Managers' Forum
OMB
GSA
NSA
Industry: Security Product Vendors
Academia: Major Universities with Computer Security curricula

Major Projects

- Computer security expert assist team (CSEAT)
- Federal computer security program managers forum
- Information security and privacy advisory board (ISPAB)
- Computer Security Resource Center (CSRC)
- Federal IT Security Self-Assessment Tool (ASSET)
- Selecting IT Security Products and Services; A User's Guide
- Federal Practices Web site (FASP)
- Procurement Guideline
- Private Sector Policies and Practices
- Security and Capital Planning

Security Testing and Metrics



User Security Needs

Standards and Metrics

Testing and Evaluation

Product Validation

IT Security

Goals

- 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

Technical Areas

- Provide Federal agencies, industry, and the public with a proven set of IT security testing methodologies and test metrics
- Promote joint work between NIST, the American National Standard Institute (ANSI) and the international standards community

Impacts

- Timely, cost-effective IT security testing
- Increased security in IT systems through availability of tested products
- Creates business opportunities for vendors of security products, testing laboratories, and security consultants

Collaborators

Federal: NVLAP, State Dept., DoC, DoD, GSA, NASA, NIST, NSA, DoE, OMB, SSA, USPS, Treasury, VA, DoT, DoJ, FAA

Industry: American National Standards Institute (ANSI), InfoGard Laboratories Inc., CygnaCom Solutions, DOMUS IT Security Laboratory, COACT, Inc. CAFÉ Lab, Atlan Laboratories, EWA, Logica Security Consulting, CORSEC Security Inc., Oracle, CISCO, Hewlett-Packard, Lucent, SAIC, Microsoft, Computer Sciences Corp., IBM, EDS, VISA, MasterCard, Amex, Checkpoint, Computer Assoc., RSA, Sun Microsystems, Network Assoc., Booz-Allen Hamilton, Entrust, Silicon Graphics, Arca, AEPOS Technologies Corporation

Global: Canada, United Kingdom, France, Germany, Korea

Major Projects

- Cryptographic Security Testing
- Cryptographic Module Validation Program (CMVP)
- Security Control Development and Information System Certification & Accreditation
- Laboratory Accreditation (Common Criteria and CMVP)
- Automated Security Testing and Test Suite Development
- Protection profile development effort with government/industry
- Industry Forums
- Testing, Education, Outreach Programs, Conferences and Workshops

Recently Completed NIST Security Guidelines

- 800-30, ***Risk Management Guide for Information Technology Systems***
- 800-31, *Intrusion Detection Systems*
- 800-32*, Intro to Public Key Technology and Federal PKI Infrastructure*
- 800-33, *Underlying Technical Models for Information Technology Security*
- 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*
- 800-44, *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***
- 800-55, *Security Metrics Guide for Information Technology Systems*

Available at http://csrc.nist.gov/publications/nistpubs/index.html

Future guidelines*

- Checklists and Configuration/Hardening Guides (DHS)
- Media Destruction/Sanitization (DHS)
- Risk Management (DHS)
- Incident Exercises (DHS)
- Malware (DHS)
- VOIP
- Forensics Handbook
- Sensor Deployment
- Penetration Testing & Vulnerability Management
- Technical Security Metrics
- Web Services
- IP/Telephony Convergence
- Trust frameworks
- RFID
- Embedded Systems
- Governance

*funding permitting, except as noted

3 High Visibility Projects

- FISMA Trilogy - #3 - Minimum Standards for all Federal Systems
- CSRDA - Checklists
- HSPD #12 - Personal Identity Verification

1. FISMA Specific Tasks

- FIPS 199 (completed)
- Mapping Guideline (completed)
- *Minimum Standards (draft)*
- Identifying National Security Systems (completed)
- Incident Handling (completed)
- Annual Report (completed)

Mandatory Standards for all Federal IT systems

- FISMA set 3 year requirement (12-2005)
- Mandatory
- All Federal systems
- Requirements for each category in FIPS 199
- Guideline in development first (800-53); mandatory standard to follow
- Full range of IT security topics, but fairly high-level

2. NIST Tasked to Develop a Cyber Security Checklist Program

- Cyber Security Research and Development Act of 2002 directs NIST to:

  Develop, and revise as necessary, a checklist 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 would set priorities for development

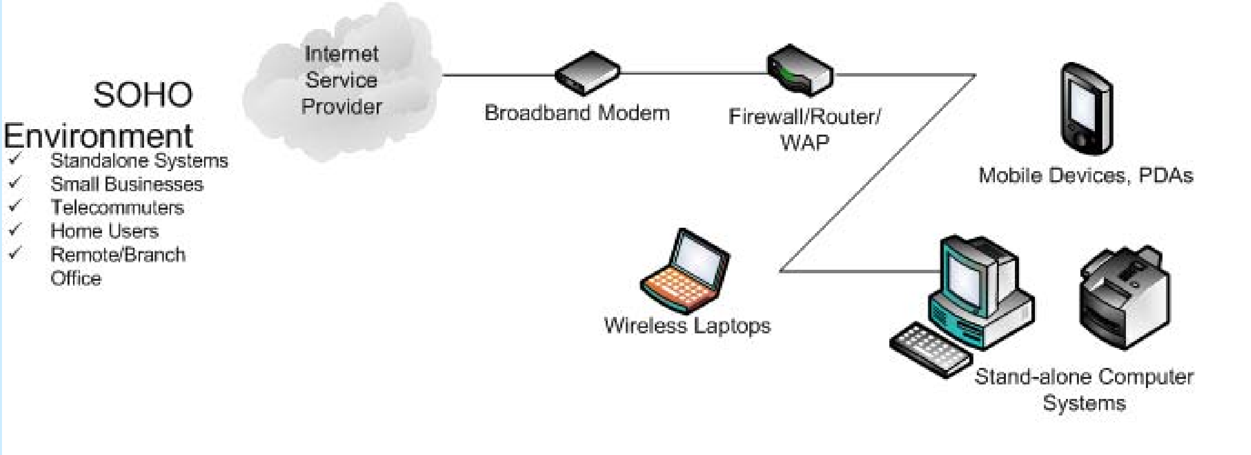
Cyber Security Summit

- **Common Configuration Working Group Report** of the Technical Standards and Common Criteria Task Force, formed at the Department of Homeland Security's first National Cyber Security Summit in 2003, recommended ***government promotion of the use of a NIST central repository for IT security configuration checklists.***

NIST’s Response:

- Write guideline for developers and users (800-70)
- Build the repository; populate with current checklists from NIST, NSA, DISA, CIS
- Get participation agreements from vendors and major users
- Assist agencies in using the repository to share and acquire configuration checklists

Operational Environments



SOHO Environment

- ✓ Standalone Systems
- ✓ Small Businesses
- ✓ Telecommuters
- ✓ Home Users
- ✓ Remote/Branch Office

Internet Service Provider

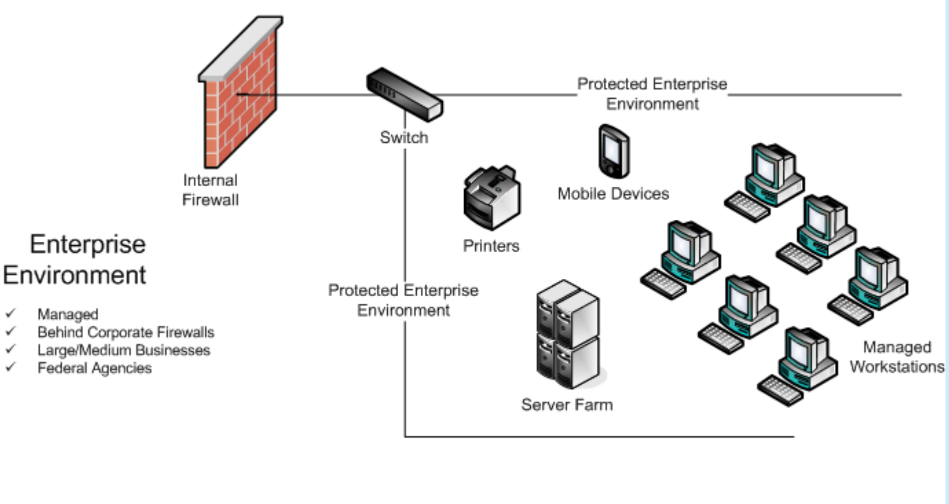
Broadband Modem

Firewall/Router/ WAP

Mobile Devices, PDAs

Wireless Laptops

Stand-alone Computer Systems



Internal Firewall

Switch

Protected Enterprise Environment

Mobile Devices

Printers

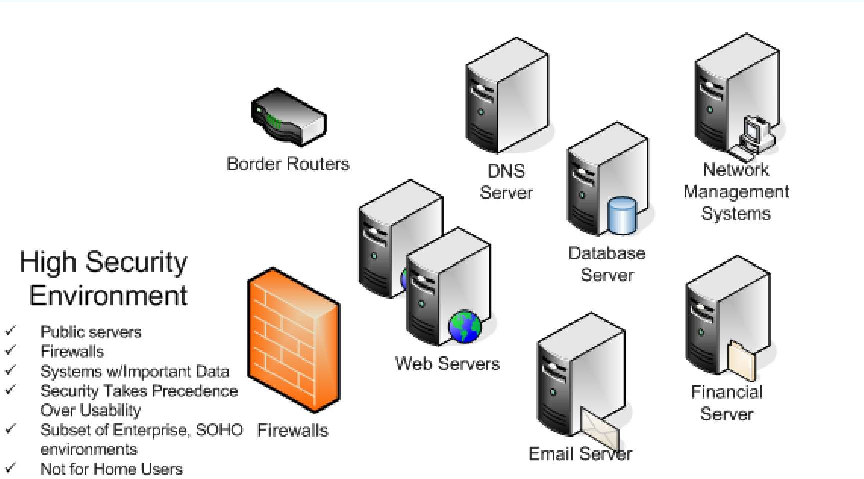
Enterprise Environment

- ✓ Managed
- ✓ Behind Corporate Firewalls
- ✓ Large/Medium Businesses
- ✓ Federal Agencies

Protected Enterprise Environment

Server Farm

Managed Workstations



Border Routers

DNS Server

Network Management Systems

Database Server

High Security Environment

- ✓ Public servers
- ✓ Firewalls
- ✓ Systems w/Important Data
- ✓ Security Takes Precedence Over Usability
- ✓ Subset of Enterprise, SOHO environments
- ✓ Not for Home Users

Firewalls

Web Servers

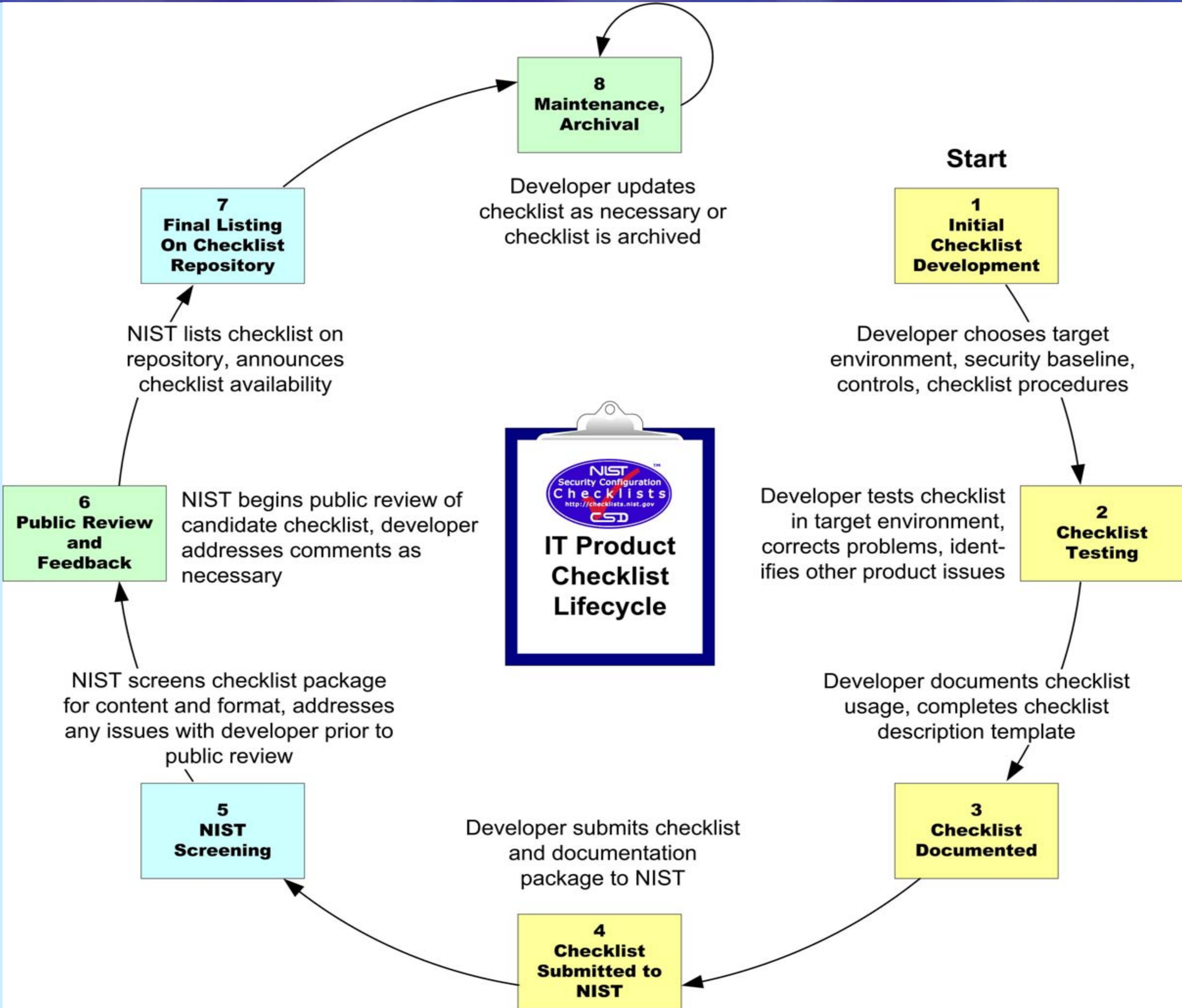
Financial Server

Email Server

How will the Program Work?

- Developers follow NIST guidance in creating checklists, e.g., targeted operational environments
- After submission to NIST and initial screening, checklists are publicly reviewed
- Issues are addressed, checklist is listed in repository and maintained by developer
- Developers can use our logo on their products
- Users can provide feedback to NIST and developers

Developer Steps Overview



Start

1
Initial Checklist Development

Developer chooses target environment, security baseline, controls, checklist procedures

2
Checklist Testing

Developer tests checklist in target environment, corrects problems, identifies other product issues

3
Checklist Documented

Developer documents checklist usage, completes checklist description template

4
Checklist Submitted to NIST

Developer submits checklist and documentation package to NIST

5
NIST Screening

NIST screens checklist package for content and format, addresses any issues with developer prior to public review

6
Public Review and Feedback

NIST begins public review of candidate checklist, developer addresses comments as necessary

7
Final Listing On Checklist Repository

NIST lists checklist on repository, announces checklist availability

8
Maintenance, Archival

Developer updates checklist as necessary or checklist is archived

IT Product Checklist Lifecycle

NIST Security Configuration Checklists
http://checklists.nist.gov
CSD

Screening Checklists Prior to Public Review

- NIST screens for applicability, technical merit based on established criteria
- NIST posts candidates for public review
- Comments are provided to the developer
- Issues addressed by the developer before final posting of the checklist
- As necessary, NIST uses independent qualified reviewers

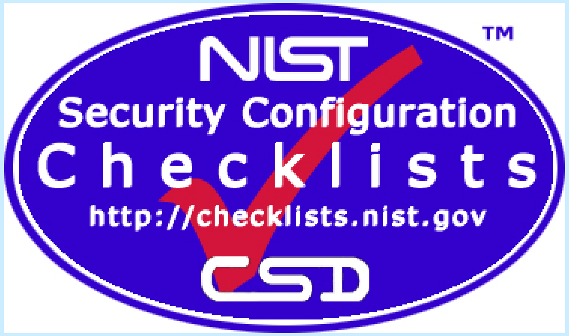
Final Listing of Checklists on Repository

- After all issues get addressed, checklist is listed on repository
- NIST continues to receive user feedback, passes on to developer
- Checklist owner can use the logo on product material with conditions
- Users get advised to test and back up before applying checklists

Checklist Maintenance

- NIST schedules a periodic review of the checklist with developer – typically 1 year
- If major update, then checklist is rescreened/resubmitted for public review
- NIST or checklist owner can decide to “delist” the checklist
- Or, checklist can be frozen, i.e., archived, but remain on repository

NIST Checklist Program Logo



- To show participation in NIST Checklist Program and ownership of a checklist on repository
- Available to checklist producers who meet the NIST program requirements
- Producer must provide end-user checklist-related support
- Does not convey NIST endorsement

Developer Participation Requirements

- Agree to requirements of program
- Create a checklist and submit all materials
- Agree to public review of checklist
- Agree to respond to comments
- For certain checklists, agree to timely updates or withdraw the checklist

Security Checklists for Commercial IT Products

About Checklists

Under the Cyber Security Research and Development Act, NIST is charged with developing security checklists. These checklists describe security settings for commercial IT products.

Security Environment

Security environments are SOHO, Enterprise, High Security, or Custom. Checklists can also be associated with the security as contained in FIPS 199.

Partners

The checklists provided on this website are provided by a wide variety of vendors, government agencies, consortia, non-profit organizations, and user organizations. For a complete list, click here. NIST gratefully acknowledges their contributions and assistance in providing this security service.

Disclaimer

The contents of each checklist is the responsibility of the submitting organization. We encourage users to send comments on specific checklists to the appropriate author.

NIST™
Security Configuration
Checklists
http://checklists.nist.gov
CSD

Search the Security Checklist Database

Search

By specific product name	Microsoft Windows 2000
By security environment	High Security
By product type	Operating System

Results

(list of checklists)

NIST Windows 2000 Special Publication
NSA Windows 2000 Security Guide
DISA Windows 2000 Security Configuration Guide
CIS Windows 2000 Guide – Level 2

Concept

Please Participate!

- NIST encourages vendors to participate
- NIST will encourage agencies to use the checklist repository
- Raise awareness of the program

Current Status

- 800-70 out for comment
- December 1, 2004 – Target date for Launch
- Outreach Underway– NCSP, CISWG, ITAA, BSA, etc.

See chart

Checklist Program Contact Info

- Tim Grance, grance@nist.gov
- Murugiah Souppaya, murugiah.souppaya@nist.gov
- John Wack, john.wack@nist.gov

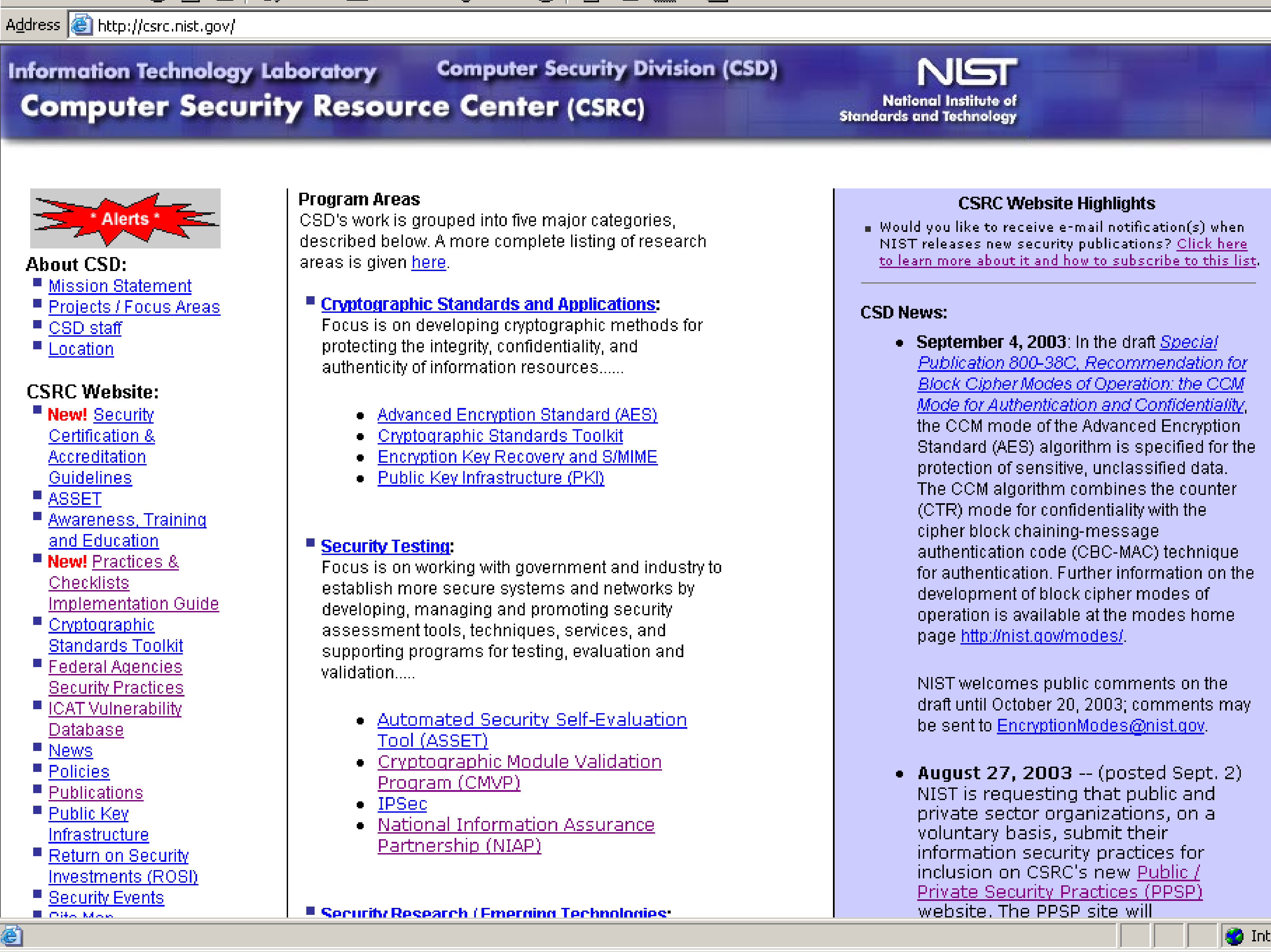
- Web site: http://checklists.nist.gov

3. Developing the PIV FIPS

- 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 technical 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.

PIV FIPS Development

- PIV TIWG being established
  - OMB/NIST to co-chair
  - Call to CIOs for Participation 9-7-04
- Phase I – Initial PIV FIPS – Framework
  (will need fleshing out)
- Phase II – Implementation Acceleration Support
- Phase III – Interoperability Maintenance Support



Information Technology Laboratory

Computer Security Division (CSD)

Computer Security Resource Center (CSRC)

NIST National Institute of Standards and Technology

About CSD:

- Mission Statement
- Projects / Focus Areas
- CSD staff
- Location

CSRC Website:

- **New!** Security Certification & Accreditation Guidelines
- ASSET
- Awareness, Training and Education
- **New!** Practices & Checklists Implementation Guide
- Cryptographic Standards Toolkit
- Federal Agencies Security Practices
- ICAT Vulnerability Database
- News
- Policies
- Publications
- Public Key Infrastructure
- Return on Security Investments (ROSI)
- Security Events
- Site Map

Program Areas

CSD's work is grouped into five major categories, described below. A more complete listing of research areas is given here.

- **Cryptographic Standards and Applications**:
  Focus is on developing cryptographic methods for protecting the integrity, confidentiality, and authenticity of information resources.....
  - Advanced Encryption Standard (AES)
  - Cryptographic Standards Toolkit
  - Encryption Key Recovery and S/MIME
  - Public Key Infrastructure (PKI)
- **Security Testing**:
  Focus is on working with government and industry to establish more secure systems and networks by developing, managing and promoting security assessment tools, techniques, services, and supporting programs for testing, evaluation and validation.....
  - Automated Security Self-Evaluation Tool (ASSET)
  - Cryptographic Module Validation Program (CMVP)
  - IPSec
  - National Information Assurance Partnership (NIAP)
- **Security Research / Emerging Technologies**:

CSRC Website Highlights

- Would you like to receive e-mail notification(s) when NIST releases new security publications? Click here to learn more about it and how to subscribe to this list.

CSD News:

- **September 4, 2003**: In the draft *Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, the CCM mode of the Advanced Encryption Standard (AES) algorithm is specified for the protection of sensitive, unclassified data. The CCM algorithm combines the counter (CTR) mode for confidentiality with the cipher block chaining-message authentication code (CBC-MAC) technique for authentication. Further information on the development of block cipher modes of operation is available at the modes home page http://nist.gov/modes/.

  NIST welcomes public comments on the draft until October 20, 2003; comments may be sent to EncryptionModes@nist.gov.

- **August 27, 2003** -- (posted Sept. 2) NIST is requesting that public and private sector organizations, on a voluntary basis, submit their information security practices for inclusion on CSRC's new Public / Private Security Practices (PPSP) website. The PPSP site will

Many Challenges Ahead

- Security Specifications and Testing (PPs/DTRs)
- FIPS for PP Assurance Levels – map to FIPS 199
- Finding Malicious Code
- Cryptographic Security for Constrained Environments
- Security Composability
- Protocol security
- Wireless
- Comprehensive Guidance Suite
- Expanded Testing Services
- Certification and Accreditation, Phase II, III

Some examples…

Summary

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