

# *NIST Cyber Security: Resources and Update*

Ed Roback

Chief, Computer Security Division

[edward.robback@nist.gov](mailto:edward.robback@nist.gov)

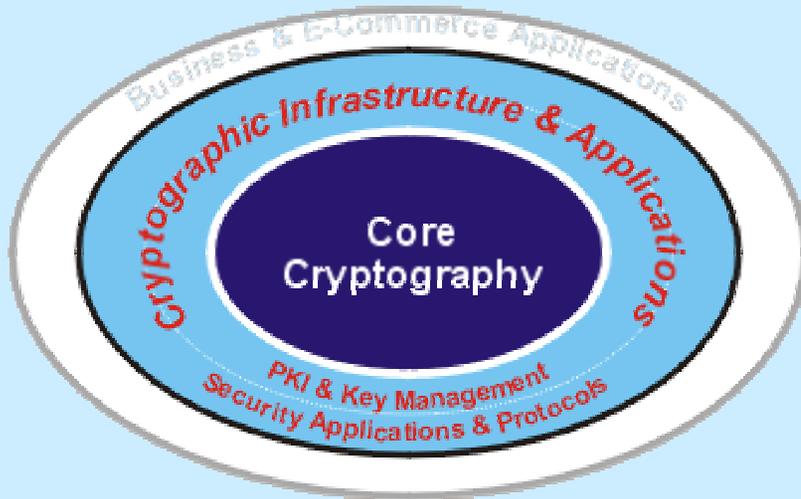
# NIST Security Mandates

- Develop standards and guidelines for the Federal government
- Improve the overall security of IT products and services
- Make the national infrastructures more secure

# Specific Focus Areas of NIST's Security Program

1. Cryptography
2. Research
3. Management Guidance and Assistance
4. Security Testing and Evaluation
5. Outreach

# Cryptographic Standards and Applications



## Goals

Establish secure cryptographic standards for storage and communications & enable cryptographic security services in applications through the development of PKI, key management protocols and secure application standards

## Technical Areas

- Secure encryption, authentication, non-repudiation, key establishment, & random number generation algorithms.
- PKI standards for protocols, standards and formats
- PKI interoperability, assurance & scalability

## Impacts

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

## Collaborators

- Industry:** ANSI X9, IETF PKIX, AES submitters, Baltimore Technologies, CertCo, Certicom, Cylink, Digital Signature Trust, RSA Labs, Entrust Technologies, E-Lock Technologies, Getronics, IBM, ID Certify, Mastercard, Microsoft, Motorola, Netscape, Spyrus, Network Associates, VeriSign, Verizon, Visa, World Talk
- Federal:** Department of Treasury, Agencies in Federal PKI Steering Committee and Bridge CA Project, FDIC, NSA, Army Corps of Engineers

## Projects

- ***Cryptographic Standards & Guidelines***
  - Cryptographic Standards Toolkit
  - Key Management Guidance
- ***Public Key Infrastructure & Applications***
  - Industry and Federal Security Standards
  - PKI and Client Security Assurance
  - Promoting PKI Deployment
  - Securing PKI Applications

**New advice re single DES now available.**

# Security Research / Emerging Technology



## 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, Active Networks
- 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 code, etc.)
- World class vulnerability search engine
- Increased security and interoperability of IPsec protocols via IPsec/Web tester

## Collaborators

**Industry:** IBM, Microsoft, SUN, Boeing, Intel, GTE, VDG, SCC, Sybase, SAIC, SUN, Lincoln Labs, Lucent, ISS, Symantec, 3Com, Interlink, Ford, CISCO, Lucent, Checkpoint, MCI, Oracle, MITRE, Open Group, 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

- Access Control & Authorization Management
- ICAT Vulnerability/Patch Search Tool
- National Smart Card Infrastructure
- Wireless/Device Security
- Mobile Agents
- IPSec/web interface testing
- Quantum Computing Support
- CIP Grants
- Benchmarks
- Technical Guidance



## Welcome to ICAT!

ICAT contains:  
**5234 vulnerabilities**  
 Last updated:  
**11/12/02**

ICAT is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information.

Enter your e-mail address and press "Add" to receive ICAT announcements.

The ICAT team appreciates the contributions and support of the following organizations: [CERIAS](#), [FedCIRC](#), [ISS X-Force](#), [NIAP](#), [SANS Institute](#), and [Security Focus](#).

The ICAT Metabase is a product of the [Computer Security Division](#) at the

### Search tips:

**All drop down menus are ANDed together to create a query.**  
**Click a link below to look up vulnerabilities by vendor or product name**  
**'\_' represents non-alphabetic characters**

Search->

Vendor [\\_..A..B](#) [C..E](#) [F..H](#) [I..K](#) [L..N](#) [O..Q](#) [R..T](#) [U..W](#) [X..Z](#) [All](#)  
 Product [\\_..A..B](#) [C..E](#) [F..H](#) [I..K](#) [L..N](#) [O..Q](#) [R..T](#) [U..W](#) [X..Z](#) [All](#)  
 Version ^ --- Choose a Vendor or Product --- ^  
 Keyword search   
 (try a CVE or CAN name)  
 Severity

### General Filters:

Common Sources   
 Related exploit range   
 Vulnerability consequence   
 Vulnerability type   
 Exposed component type   
 Entry type   
 Entries since the following date

The ICAT Metabase is a product of the [Computer Security Division](#) at the [National Institute of Standards and Technology](#).

ICAT Creator: Peter Mell

ICAT Developers: Kathy Ton-Nu and Michael Reilly.

ICAT Database Support: Susan Nourbakhsh, Christina Kingsberry, Rachel Glenn

Past Developers: Derek Dye, Elizabeth Boteler, Angela Huh, David Marks, Mark McLamon, Jorge Armenta, Benjamin Van Durne

Send Feedback to: [icat@nist.gov](mailto:icat@nist.gov)

# Security Management and Assistance



## 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
- Increased 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
- Computer system security and privacy advisory board (CSSPAB)
- 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 Guidelines
- EBISS Guidelines/Support
- Metrics

# Recently Completed NIST Security Guidance

- 800-27, *Engineering Principles for IT Security*
- 800-28, *Mobile Code and Active Content*
- 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*
- 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*
- 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*
- 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*
- 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*

# NIST Security Guidance in Draft

(Available now)

- 800-37, *Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems*
- 800-55, *Security Metrics Guide for Information Technology Systems*
- 800-38B, *Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode*
- 800-36, *Guide to Selecting IT Security Products*
- 800-35, *Guide to IT Security Services*
- 800-4A, *Security Considerations in Federal Information Technology Procurements*
- 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*
- 800-50, *Building an Information Technology Security Awareness and Training Program*
- 800-43, *System Administration Guidance for Windows 2000 Professional*
- 800-42, *Guideline on Network Security Testing*

# Federal Agency Security Practices

Federal Computer Security Program Manager's Forum


[HOME](#)
[FASP Areas](#)
[Pilot BSPs](#)
[FAQ](#)
[Submit FASP](#)
[Other Security  
Practice Sites](#)
[Federal Computer  
Security Program  
Managers' Forum](#)
[Points of Contacts](#)


FASP Areas	Date
<p>There are some FASP in the listing below that do not reference an agency affiliation. These examples are provided in a generic format. The original BSP submissions are identified below by an asterisk (*) behind their title. The original BSP submissions marked by * are in .html format. The new FASP links are in MS Word format (without *).</p>	

## AUDIT TRAILS -

**maintains a record of system activity by system or application processes and by user activity.**

[Sample Generic Policy and High Level Procedures for Audit Trails](#)

08/02/00

## AUTHORIZE PROCESSING (C&A) -

**provides a form of assurance of the security of the system.**

[Certification and Accreditation -- DLA \\*](#)

03/12/01

[C&A of Core Financial System -- USAID \\*](#)

02/05/01

[How to Accredit Information Systems for Operation -- DOD/NSWC \\*](#)

05/11/01

[Sample Generic Policy and High Level Procedures for Certification/Accreditation](#)

08/02/00

## CONTINGENCY PLANNING -

**how to keep an organization's critical functions operating in the event of disruption, large and small.**

[Continuity of Operations -- Treasury \\*](#)

05/19/00

[Contingency Planning Template - DOJ](#)

no date

# Cryptographic Module Validation Program

# CMVP



*Conformance through Testing*

## Goals

- Improve the security and quality of cryptographic products
- Provide U.S. and Canadian Federal agencies with a security metric to use in procuring cryptographic equipment
- Promote the use of tested and validated cryptographic algorithms, modules, and products

## Technical Areas

- Development of Implementation Guidelines, metrics and test methods
- Validation of test results
- Accreditation of testing laboratories
- Joint work between NIST, ANSI and international standards bodies

## Impacts

- Provide Federal agencies with confidence that a validated cryptographic product meets a claimed level of security
- Supply a documented methodology for conformance testing
- Create business opportunities for vendors of cryptographic products, testing laboratories, and security consultants

## Collaborators

**Federal:** National Voluntary Laboratory Accreditation Program

**Industry:** American National Standards Institute (ANSI)  
 InfoGard Laboratories Inc.  
 CygnaCom Solutions  
 DOMUS IT Security Laboratory, a Division of LGS  
 COACT, Inc. CAFÉ Lab  
 Atlan Laboratories  
 EWA-Canada LTD, IT Security Evaluation Facility  
 CORSEC Security Inc.

**Global:** Communications Security Establishment (CSE) of the Government of Canada

## FY 2002

- Implemented Cost Recovery Plan June 2002
- Completed FIPS 140-2 Derived Test Requirements and automated test tool
- Validated 120+ crypto modules and 150+ crypto algorithm implementations
- Accredited second non-U.S. laboratory (EWA Canada), first non-North American laboratory accreditation scheduled July 2002
- Designed and developed Cryptographic Algorithm Validation System Developed AES test suite and enhanced DES/TDES validation tests
- Conducted second CMVP workshop
- UK announces recognition of FIPS 140-2

## FY 2003

- Continue FIPS 140-2 validations
- Accredit 2-3 additional CMT Laboratories, including international
- Expand the agreement with CSE to include additional countries
- FIPS 140-2 as an ISO standard
- Plan third Cryptographic Module Validation Program Workshop/Conference
- Develop Validation Test Suites for new algorithms/protocols
- Interpretations of new technology areas for existing standards (e.g. JAVA)

[Cryptographic Module Validation Program](#)

**Standards and Their Related Documents:**

- [FIPS 140-1](#)
- [FIPS 140-2](#)
- [T-DES, DES, Skipjack](#)
- [DSA, RSA, ECDSA](#)
- [SHA-1](#)

- [MAC](#)
- [X9.17](#)

**Announcements and Notices**

Updated 02/04/2002

[Validation Lists](#)

[Testing Laboratories](#)

[FAQs](#)

Updated 03/11/2002

[Helpful Documentation](#)

[Contacts](#)

[Computer Security](#)

# Validation Lists for Cryptographic Standards

\*\*\*

All questions regarding the implementation and/or use of any module/product located on the following lists should first be directed to the appropriate *VENDOR point of contact* (listed for each entry). Thank you.

\*\*\*

NIST maintains validation lists for all of its cryptographic standards testing programs (past and present). All of the following lists are updated as new products/implementations receive validation certificates from NIST and CSE. Items on the FIPS 140-1 and FIPS 140-2 validation list include validated algorithm implementations that appear on the algorithm validation lists.

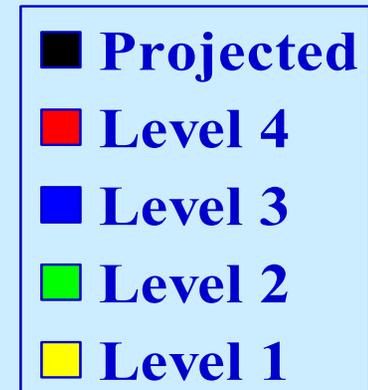
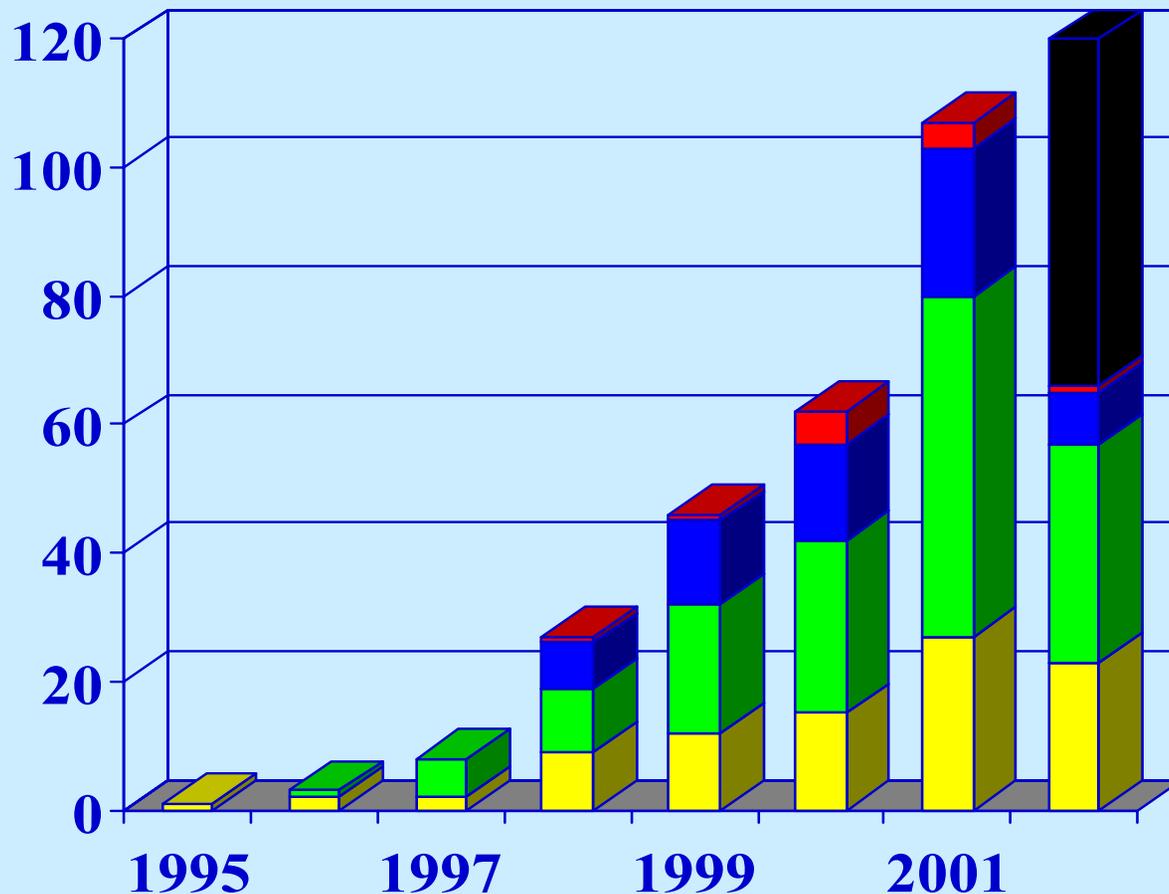
Users in Federal Government organizations are advised to refer to the FIPS 140-1 and FIPS 140-2 validation list.

- [FIPS 140-1 and FIPS 140-2 Vendor List](#) - alphabetical list of vendors with validated cryptomodules.
- [FIPS 140-1 and FIPS 140-2 Cryptographic Module Validation List](#) [MS Access (ZIP)] - contains detailed cryptomodule information.
- [Triple DES Validation List](#) [MS Access (ZIP)]
- [DES Validation List](#) [MS Access (ZIP)]
- [Skipjack Validation List](#) (PDF)
- [DSA Validation List](#)
- [SHA-1 Validation List](#)
- [MAC Validation List](#)
- [FIPS 171 \(ANSI X9.17 Key Management\) Validation List](#)

**FIPS 140-2, Security Requirements for Cryptographic Products, is a mandatory standard for Federal sensitive systems. If cryptography is needed, agencies must use validated products (250+ now exist).**

# FIPS 140-1 and FIPS 140-2 Validations by Year and Level

(May 24, 2002)



# National Information Assurance Partnership



*Building More Secure Systems for the New Millennium* <sup>(sm)</sup>

## Goals

- Promote the development and use of evaluated and validated IT products
- Champion the development and use of national/international IT security standards
- Develop state-of-the-art test methods, tools, techniques and assurance metrics
- Support a framework for international recognition of testing results
- Foster development of IT security requirements in key technology areas

## Technical Areas

- Development of implementation Guidelines, requirements, metrics and test methods
- Validation of test results and accreditation of testing laboratories
- Joint work among NIST, NSA and international partners

## Impacts

- More timely, cost-effective IT security evaluations with greater consistency
- Less duplication of security testing globally
- New test methods for specific information technologies
- Increased security in IT systems and networks through greater availability of evaluated and validated products
- Greater availability of common security requirements and specifications for key technologies and sectors

## Collaborators

- Federal:** State Dept., DoC, DoD, GSA, NIST, NSA, DoE, OMB
- Industry:** Oracle, CISCO, Hewlett-Packard, Lucent, SAIC, Microsoft, Computer Sciences Corp., Cygnacom, Arca, IBM, EDS, VISA, MasterCard, Amex, Checkpoint, Computer Assoc., RSA, Sun Microsystems, Network Assoc., Booz-Allen, Seculab, Entrust, Silicon Graphics, COACT
- Global:** United Kingdom, France, Germany, Japan, Korea, Canada, The Netherlands, Australia, Italy, Spain, New Zealand, Finland, Sweden, Norway, Greece, Israel, Russia, ECMA, JCB, Europay, Mondex, Austria, India
- Forums:** Healthcare, Information Assurance, Process Control, Smart Card

## FY 2002

- Accredited 2 Common Criteria (CC) Testing Laboratories
- Expanded CC Recognition Arrangement to 15 nations adding Sweden
- Conducted Federal Information Assurance Conference with industry partner
- Organized Second National Summit on Security Requirements for Critical Information Systems (Scheduled October 2002)
- Briefed at two workshops in Moscow, Russia for Minatom, Russia & DoE, USA
- Common Criteria Seminar in Japan
- Authored Protection Profile Development Process in coordination with NSA
- Supported the third International Common Criteria Conference in Ottawa
- Validated 11 security products and 11 protection profiles (projected)

## FY 2003

- Accredited 1-2 additional CC Testing Laboratories
- Common Criteria Evaluation and Validation Scheme
- Develop technology-based lab accreditation program with smart card prototype
- Continue cooperative protection profile development effort with government/industry
- Enhance outreach program and activities

**NIST guidance to Federal agencies on the use of evaluated products (for sensitive systems) is contained in NIST 800-23.**



# Common Criteria

## Evaluation and Validation Scheme



SCHEME HOME

NIAP VALIDATION BODY

CC TESTING LABORATORIES

NIAP VALIDATED PRODUCTS LIST

PROTECTION PROFILE REGISTRY

PRODUCTS / PPS IN EVALUATION

GUIDANCE DOCUMENTS

EVENTS

COMMON CRITERIA (ISO/IEC 15408)

COMMON METHODOLOGY



### NIAP VALIDATED PRODUCTS LIST

The following information technology evaluated and certified/validated Common Criteria Evaluation and Recognition Arrangement (CCRA) evaluated at accredited and license of the other countries participating Criteria for IT Security Evaluation (IS

Common Criteria certificates issued the specific versions and releases in conjunction with complete certification only to the IT product tested, or described in the certification/validation certification/validation information certification/validation report and when using the certified/validated tested environment; and is responsible results to see if the testing conducted

Certificates are not endorsements of any other organization that recognizes



FREQUENTLY ASKED QUESTIONS  
TRUST TECHNOLOGY ASSESSMENT PROGRAM

#### From the United States:

NIAP Common Criteria Evaluation and Validation Scheme  
National Institute of Standards and Technology (NIST)  
National Security Agency (NSA)

#### Check Point Software Technologies, Inc.

- [Check Point FireWall-1 Version, Version 4.0 \(SP 5\)](#) - Compliant with U.S. Government Protection Profile

#### Cisco Systems, Inc.

- [Cisco PIX Firewall520](#) - Compliant with U.S. Government Protection Profile

#### Electronic Engineering Systems, Inc. (EESI)

- [SuperNet 2000 EAL4/r1](#) -

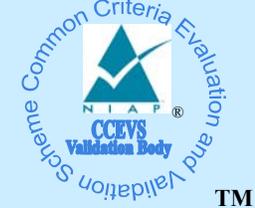
#### Finjan Software Incorporated

- [Finjan SurfinGate Version 5.6](#)

#### IBM Corporation

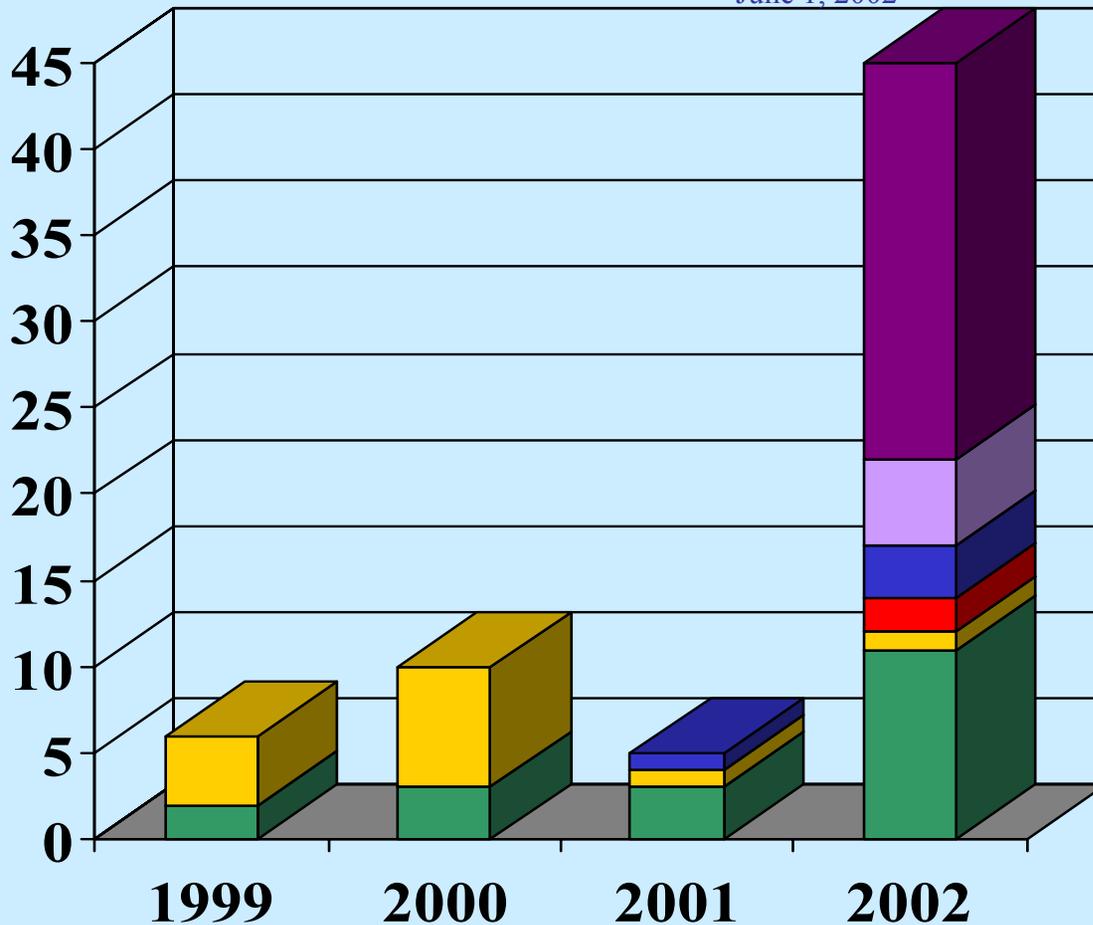


# NIAP CCEVS



## Validations by Year and Level

June 1, 2002



- In Evaluation**
- Expected**
- EAL 4**
- EAL 3**
- EAL 2**
- EAL 1**
- PP's**

# Beyond IT product testing...

- Homeland Security/Cybersecurity needs demand attention beyond just security evaluation of IT products
- Complementing the current NIAP focus on *product* evaluation, NIST plans to use its unique position to focus on Federal *system certifications* by:
  - Developing unified Federal procedures and guidelines for system certification (draft NIST Special Publication 800-37).
  - Developing minimum security requirements for federal systems – and validation techniques. (800-53 and –53A; drafts expected Spring 2003).
  - Exploring utility/costs of developing a voluntary accreditation program to validate organizational competence to conduct security certifications for Federal agencies (and also available for use by to State/Local governments and private sector).
  - Exploring utility/costs of a project to validate commercial automated tools as correctly supporting the 800-37 security certification methodology.

**About CSD:**

- [Mission Statement](#)
- [Projects / Focus Areas](#)
- [CSD staff](#)
- [Location](#)

**CSRC Website:**

- **New!** [System Certification & Accreditation Guidelines](#)
- **New!** [ASSET](#)
- [Awareness, Training and Education](#)
- [Encryption](#)
- [Federal Agencies Security Practices](#)
- [ICAT Vulnerability Database](#)
- [News](#)
- [Policies](#)
- [Publications](#)
- [Public Key Infrastructure](#)
- [Return on Investments \(ROI\)](#)
- [Security Events](#)
- [Site Map](#)
- [Small Business Computer Security Workshops](#)
- **New!** [Small Business Corner](#)

**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 \(NIAP\)](#)

**CSRC Website Highlights**

- \*\* Receive immediate e-mail notification when new NIST computer security publications or news are available by subscribing to the NIST computer security publications e-mail list. To subscribe to this list send e-mail to: [listproc@nist.gov](mailto:listproc@nist.gov) . In the body of the e-mail message type:

subscribe compsecpubs your first and last name

Once you subscribe to the list, you will receive a confirmation letter. You will not be able to post anything to compsecpubs. This is a private and non-interactive list. You will only receive notification whenever a new NIST draft or other computer security publication has been posted to CSRC.

To unsubscribe to this list type in the body of the e-mail message:

**unsubscribe compsecpubs**

[October ITL Bulletin \(.pdf\)](#)

**Security Patches And The CVE Vulnerability Naming Scheme: Tools To Address Computer System Vulnerabilities**

**Failure to keep operating system and application software up to date is a common mistake made by IT professionals. Despite extensive testing, all operating systems and applications are released with bugs (errors in the software) that affect security, performance, and stability. As software programs expand, the potential number of bugs grows. Many security-related bugs are generally discovered only after a large number of users start using the software, and hackers and independent testers start attempting to compromise it. Once a bug is discovered, the software manufacturer often releases a**

# What else is ahead?

- Cyber Security Research and Development bill**
- Federal Information Security Management Act**
  - (2 versions)**

# Cyber Security Research and Development Act

- National Science Foundation
  - grants for basic research
  - support for higher education (many variants)
- NIST
  - research grants
  - cyber security checklists
  - in-house research:
    - Composability; SCADA; long-term/high-risk
  - Advisory Board and NRC study

# Cyber Security Checklists

- Definition –  
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

# Agency Use of Checklists (1)

- The Act does **NOT**:
  - require agencies to select the specific settings or options recommended by the checklist for the system;
  - establish conditions or prerequisites for Federal agency procurement or deployment of any such system;
  - represent an endorsement of any such system by NIST ;  
nor
  - preclude agencies from procuring or deploying other computer hardware or software systems for which no such checklist has been developed.

# Agency Use of Checklists (2)

- If an agency uses a system for which a checklist is issued, the agency:
  - shall include in their program plan an explanation of how the agency has considered such checklist in deploying that system; (except for national security systems) and
  - may treat the explanation as if it were a portion of the agency's annual performance plan properly classified under criteria established by an Executive Order (within the meaning of section 1115(d) of title 31, United States Code).

# Federal Information Security Management Act (HR 2458)

Title III of E-Government bill  
(HR 2458; passed House and Senate 11-15)

# Purpose

- Provide Leadership in Promoting Electronic Government
- Promote Interagency Collaboration
- Utilize Best Practices From Public and Private Sector Organizations
- Promote Enhanced Access to Government Information Consistent With Required Protections

# NIST Role

FISMA Establishes an Information Technology Framework Based on NIST Standards

## KEY AREAS:

- Information categorization based on levels of sensitivity
- Minimum security requirements by category
- Incident Handling
- Agency Assistance
- Performance Indicators/Metrics
- Security Policy

# Summary & Conclusions

## ***NIST is improving security by:***

- Raising awareness of the need for cost-effective security
- Engaging in key U.S. voluntary standards activities
- Developing standards and guidelines to secure Federal systems (often adopted voluntarily by private sector)
  - Cryptographic algorithms
  - Policy, management, operations, and best practices guidance
  - PKI
- Providing National leadership role for security testing and evaluation
  - Cryptographic Module Validation Program
  - National Information Assurance Partnership