NIST Computer Security Division Update

Ed Roback
Chief, Computer Security Division
December 2003

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.

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

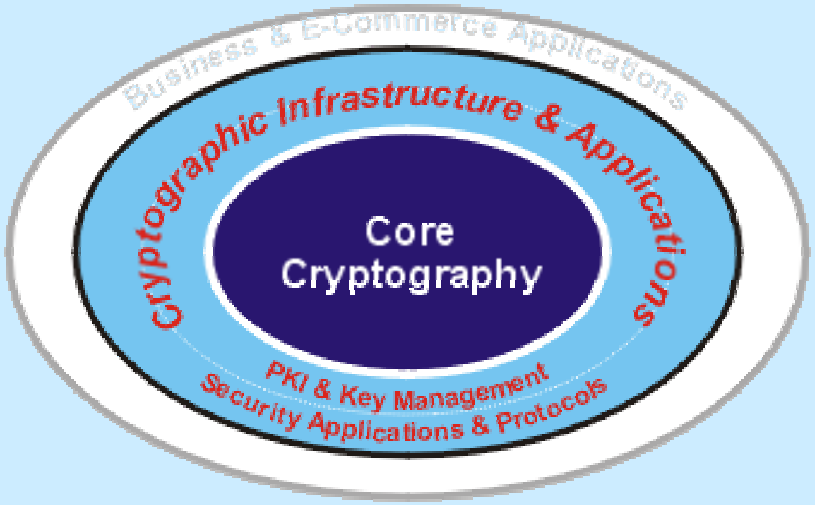
- Extramural research support
- Fellowships
- Intramural research
- Checklists
- NRC study support

Current NIST Security Activities

Focus Areas

- Cryptographic Standards and E-Authentication
- Emerging Technologies
  - Smart Cards, Wireless/PDAs, Authorization Management
- Management and Assistance
- Security Testing

Cryptographic Standards and Applications



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

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

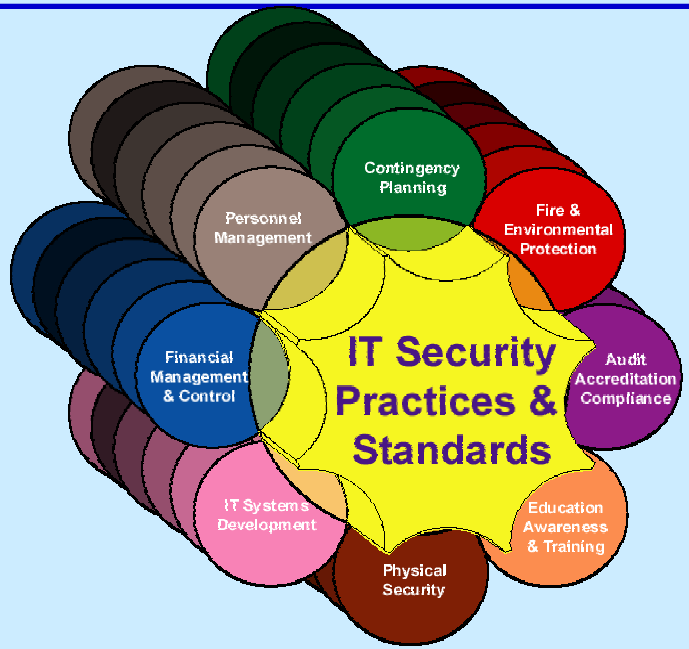
Academic: U Maryland, Ohio State, U Tulsa, George Mason, Rutgers U, Purdue , George Washington, U of W. Fla, UCSD, UMBC

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



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

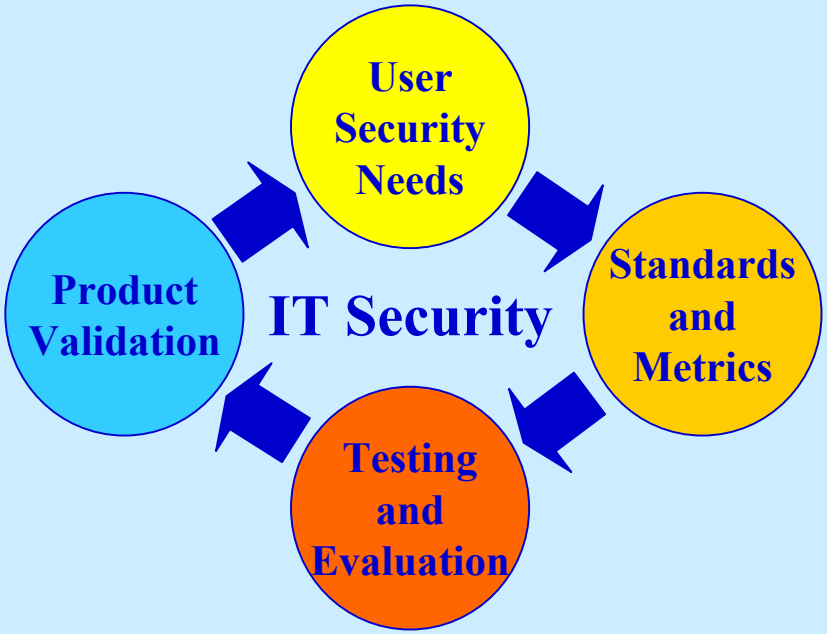
Industry: Security Product Vendors

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



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

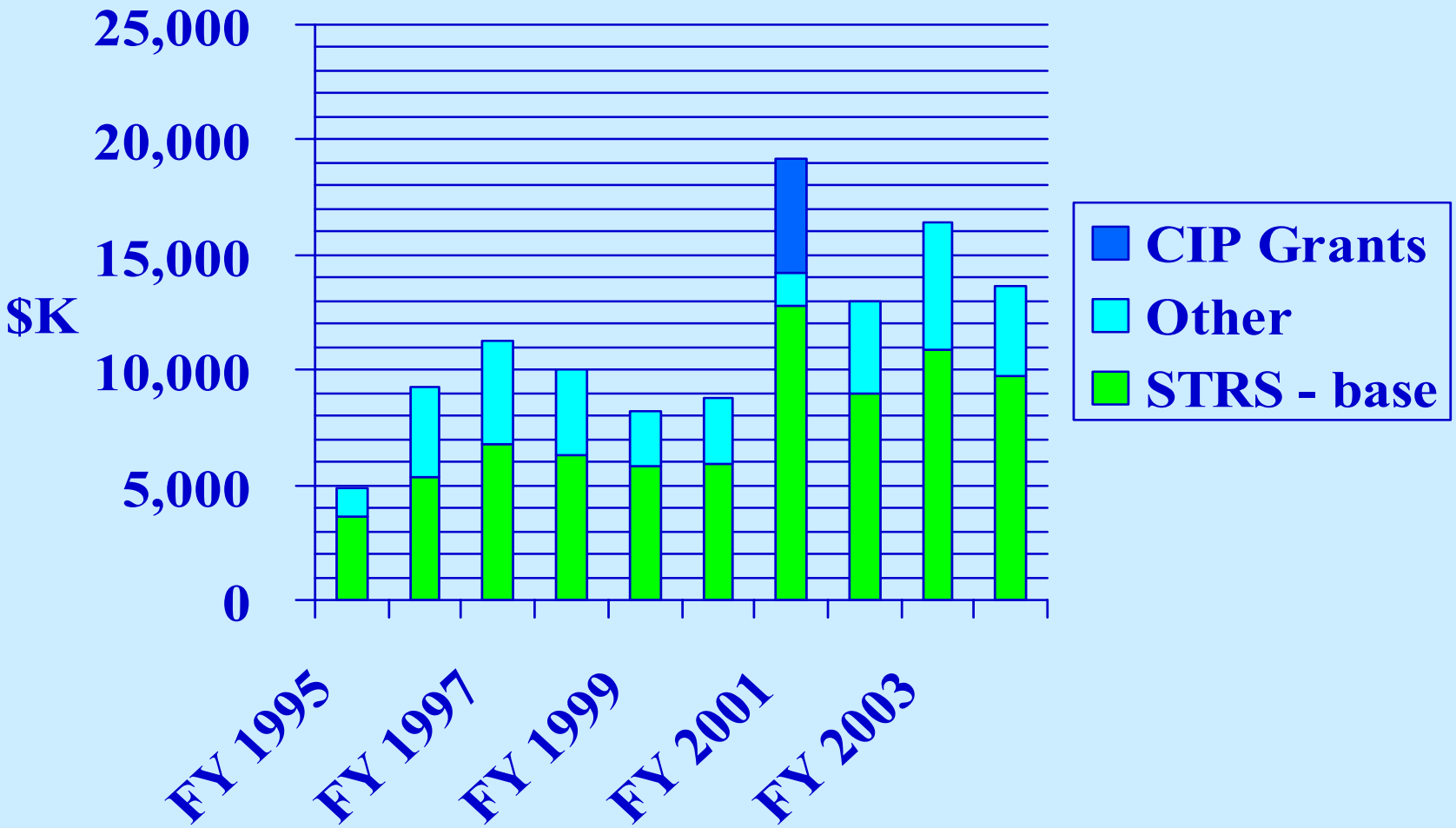
Industry: American National Standards Institute (ANSI), InfoGard Laboratories Inc., CygnaCom Solutions, DOMUS IT Security Laboratory, COACT, Inc. CAFÉ Lab, Atlan Laboratories, EWA, Logica Security Consulting, CORSEC Security Inc., Oracle, CISCO, Hewlett-Packard, Lucent, SAIC, Microsoft, Computer Sciences 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

Division Budget Trends



FY-04 -- Note that NIST funding is on a continuing resolution; budget figures are thus not "final."

Specific NIST Resources…

Security Publications

- Guidelines
  - Technical, Management and Operational Controls
  - http://csrc.nist.gov/publications/nistpubs/index.html
- NIST Information Technology Laboratory Bulletins
  - Topics vary
  - http://csrc.nist.gov/publications/nistbul/index.html
- Standards
  - Usually Highly technical – e.g., cryptographic algorithms
  - http://csrc.nist.gov/publications/fips/index.html

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***
- 800-40, *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***
- 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*
- 800-55, *Security Metrics Guide for Information Technology Systems*

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

NIST ITL Bulletins

2003

- IT Security Metrics
- Testing Intrusion Detection Systems
- ASSET: Security Assessment Tool For Federal Agencies
- Security For Wireless Networks And Devices
- Secure Interconnections for Information Technology Systems

2002

- Security Of Electronic Mail
- Security of Public Web Servers
- Security For Telecommuting And Broadband Communications
- Security Patches And The CVE Vulnerability Naming Scheme: Tools To Address Computer System Vulnerabilities
- Cryptographic Standards and Guidelines: A Status Report
- Overview: The Government Smart Card Interoperability Specification
- Contingency Planning Guide For Information Technology Systems
- Techniques for System and Data Recovery
- Risk Management Guidance For Information Technology Systems
- Guidelines on Firewalls and Firewall Policy

Information Technology Laboratory
Computer Security Division (CSD) & Computer Security Resource Center (CSRC)
NIST National Institute of Standards and Technology

Federal Agency Security Practices

Federal Computer Security Program Manager's Forum

search

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

FASP Areas	Date
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 *).	

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

HOME

Federal Agency Security Practices (FASP)

Pilot BSPs

FAQ

Federal Computer Security Program Managers' Forum

Public/Private Security Practices

Checklists / Implementation Guides

Submit Practices & Checklists/ Implementation Guides

Points of Contacts

Information Technology Security

Practices & Checklists / Implementation Guides

Computer Security Resource Center - CSD

Public / Private Security Practices	File Format	Date
Some security practices in the listing below may not reference an organization's affiliation. These practices are provided in a generic format. The second column specifies the type of file format (Ex. MS Word, pdf, Text file, etc.) that the file is available in. The third column contains the date when the file was posted to this page.		

NIST invites public and private organizations to submit their information security practices as nominated candidates for inclusion in its Computer Security Resource Center. With the recognition that protection of the Nation's critical infrastructure is dependent upon effective information security solutions and to minimize vulnerabilities associated with a variety of threats, the broader sharing of such practices will enhance the overall security of the nation. Today's federal networks and systems are highly interconnected and interdependent with non-federal systems. Access to information security practices in the public and private sector can be applied to enhance the overall performance of Federal information security programs.

Nominated candidate policies and procedures may be submitted to NIST in any area of information security including, but not limited to: accreditation, audit trails, authorization of processing, budget planning and justification, certification, contingency planning, data integrity, disaster planning, documentation, hardware and system maintenance, identification and authentication, incident handling and response, life cycle, network security, personnel security, physical and environmental protection, production input/output controls, security policy, program management, review of security controls, risk management, security awareness training, and education (to include specific course

Address http://icat.nist.gov/icat.cfm

ICAT METABASE

Your CVE Vulnerability Search Engine

SEARCH DOWNLOAD NOTIFICATION CONTACT INFO TOP TEN LIST STATISTICS

Welcome to *ICAT*!

ICAT contains:
6108 vulnerabilities
Last updated:
08/27/03

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.

Add

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

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
Double-quotes are ignored in text-search; Individual words are ANDed together.

Search-> All entries | 1 Year | 6 Months | 3 Months | Reset values

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	Any

General Filters:

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

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

Advanced Encryption Standard Algorithm Validation List

Last Update: August 28, 2003

The page provides technical information about implementations that have been validated as conforming to the **Advanced Encryption Standard (AES) Algorithm**, as specified in Fe Information Processing Standard Publication 197, *Advanced Encryption Standard*.

The list below describes implementations which have been validated as correctly implementing the AES algorithm, using the tests found in The Advanced Encryption Standard Algorithm Validation Suite (AESAVS). This testing is performed by NVLAP accredited Cryptographic Module Testing (CMT) laboratories.

The implementations below consist of software, firmware, hardware, and any combination thereof. The National Institute of Standards and Technology (NIST) has made every atte provide complete and accurate information about the implementations described in this document. However, due to the possibility of changes made within individual companies, N cannot guarantee that this document reflects the current status of each product. It is the responsibility of the vendor to notify NIST of any necessary changes to its entry in the following list. A validation certificate issued to each vendor also indicates 1) the CMT laboratory that tested the implementation, and 2) the operating environment used to test the implementation (if software or firmware).

This list is ordered in reverse numerical order, by certificate number. Thus, the more recent validations are located closer to the top of the list. Also indicated after the date of valid are the **modes** (e.g., ECB, CFB, etc.), **states** (encryption(e) and/or decryption(d)), and **key sizes** (128-bit, 192-bit, and/or 256-bit) for which the implementation was validated. For Co (CTR) mode, the **counter source** (internal(int) and/or external(ext)) is also indicated:

Advanced Encryption Standard (AES) Algorithm Validated Implementations

Cert#	Vendor	Implementation	Val. Date	Modes/States/Key sizes/ Description
89		rary	8/27/2003	**ECB(e/d; 128,192,256); CBC(e/d; 128,192,256); CFB128(e/d; 128,192,256) OFB(e/d; 128,192,256); CTR(ext only; 128,192,256)** "The F-Secure Cryptographic Library for Windows is a 140-2 Level 2 compliar software module, implemented as a 32-bit Windows compatible DLL. The mod provies an assortment of cryptographic services to client processes that atta instances of the module DLL."
				CBC(e/d; 128,256)

NIAP

Operating Systems <-- click here for definition

Product Name	Manufacturer	Conformance Claim	Valid. Date	CC Scheme
AIX 5L for Power V5.2, Program Number 5765-E62	IBM Corporation	EAL 4 Augmented ALC_FLR.1 PP	Apr 02	
B1/EST-X, V2.0.1 with AIX, V 4.3	Bull S.A. and IBM Informationsysteme DeutschlandGmbH	EAL 4 Augmented ALC_FLR.2	Nov 99	
Hewlett-Packard HP-UX (11i) Version 11.11	Hewlett-Packard Ltd.	EAL 4	Sep 01	
IRIX v 6.5.13, with patches 4354, 4451, 4452	Silicon Graphics, Inc.	EAL 3 PP	Apr 02	
NOKIA IPSO 3.5 and 3.5.1	Nokia Internet Communications	EAL 4	Jul 03	
Trusted IRIX/CMW v 6.5.13, with patches 4354, 4451, 4452, 4373, 4473	Silicon Graphics, Inc.	EAL 3 PP	May 02	
Solaris 8 2/02	Sun Microsystems, Inc.	EAL 4 PP	Apr 03	
Sun Trusted Solaris, v 8 4/01	Sun Microsystems, Inc.	EAL 4	Jun 02	
Sun Solaris Version 8 with AdminSuite v3.0.1	Sun Microsystems, Inc.	EAL 4	Nov 00	
SuSE Linux Enterprise Server V8 (BSI-DSZ-CC-0216-2003).	SuSE Linux AG	EAL 2 Augmented ALC_FLR.1	Feb 02	
Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886	Microsoft Corporation	EAL 4 Augmented ALC_FLR.3 PP	Oct 02	

Back to Top

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

What's ahead from NIST?

Categorization Standards

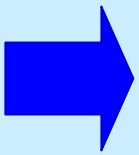
- Develop standard to categorize information and information systems
- Draft *Federal Information Processing Standards (FIPS) Publication 199, "Standard for Security Categorization of Federal Information and Information Systems"*
- Draft available

  http://csrc.nist.gov/publications/drafts/FIPS-PUB-199-ipd.pdf

Security Categorization

DRAFT

Mapping Types of Information and Information Systems to FIPS Pub 199 Security Categories



	Low	Moderate	High
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Mapping Guidelines

- Develop guidelines recommending the types of information and information systems to be included in each category described in FIPS 199
  - Writing in progress. (Special Publication 800-60, *"Guideline for Mapping Types of Federal Information and Information Systems to Security Categories")*
- Interagency Workshop held July 31, 2003
- Publication due Summer 2004

Minimum Security Requirements

- Develop minimum information security requirements (i.e., management, operational, and technical security controls) for information and information systems in each such category—
- Project underway at NIST to develop:

  Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Controls for Federal Information Systems"*

  Final Publication NLT December 2005

* NIST Special Publication 800-53 will provide interim guidance until completion and adoption of FIPS Publication 200.

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 (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

Certification and Accreditation

- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical controls)
- Project underway at NIST to develop:
  - Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"
  - Special Publication 800-53A, "Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems"

Special Publication 800-53A

Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems

- Provides standardized techniques and procedures for independent certification agents to verify the effectiveness of security controls
- Provides a single baseline verification procedure for each security control in SP 800-53
- Allows additional verification techniques and procedures to be applied at the discretion of the agency

Some of the Guidelines in Development

- Incident detection and handling
  - Comments were due 10-15
- Border Gateway Protocol
- Security in the Capital Planning Process
- Domain Name System (DNS) Security
- Voice over Internet Protocol
- Procurement – Services and Products

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 to set priorities for development
- NIST Workshop held September 25-26, 2003
- http://csrc.nist.gov/checklists/
- DHS S&T support

Many challenges remain…

Some* examples…

*** Following presentations will elaborate and provide others…**

3 Stoplight Charts

- Specific Technology guidelines, specifications, testing requirements, & guidance for settings of specific products and scanning tools
- Comprehensive Guidance Suite
- Expanding cryptographic toolkit and related testing

Security Product Specifications and Testing

- Problem
  - Many of today's commercially available technology products do not have the level of security appropriate to protect the nation's critical infrastructures.
  - Moreover, we do not have a sense whether vendors' claims of security in a product is actually present and functional.
- Solution
  - consensus-based security requirements ("protection profiles") for key families of information technology products;
  - corresponding detailed testing procedures to accompany each set of requirements; and
  - advisory guideline for each technology area

Finding Hidden Malicious Code

- Problem
  - Hidden malicious code may be buried in software
  - No cost-effective means to uncover
- Solution
  - More research needed in automated scanning tools
  - Need for ways to measure effectiveness of tools
  - Software test data set

Cryptographic Security for Constrained Environments

- Problem:
  - Devices with constrained processing and storage power (e.g., sensor embedded systems) cannot incorporate traditional cryptography because of high-overhead processing costs.
  - Risks from amateur attempts to 'tailor' existing standards to fit.
- Solution:
  - Expand the NIST cryptographic toolkit to accommodate these limited power, small-sized computing environments;
  - Develop and promulgate guidance on where the new standards are technically appropriate; and
  - Develop the next generation of agile cryptographic security standards for process control, embedded systems, and mobile applications.

Security Composability

- Problem:
  - In the end, we operate systems, not components, BUT –
  - We do not have technical means to understand the resulting security properties of connecting individually understood components.
- Solution:
  - Develop models to better understand security associated with assembling a networked computer system from components; and
  - Develop advanced methods to express security requirements for integrated systems, and metrics to enable rapid testing.

Wireless Security

- Problem:
  - Little security exists to protect the ever-growing array of mobile and wireless systems now being deployed.
  - Wireless deployment is inexorable.
  - Temporary security standards “band-aids” are inadequate for long-term.
- Solution:
  - Work with industry to speed the improvement of wireless security standards and ensure that insecure “interim fixes” do not become entrenched;
  - Study and report on new security issues and properties appropriate for wireless intrusion detection systems; and
  - Develop means for location-based security policy enforcement.

Protocol Security

- Problem:
  - Flaws in protocols allow exploitation.
    e.g., Distributed Denial of Service attacks
  - Continued development of protocols without attention to security.
- Solution:
  - Design security tools and guidance for protocol designers; and
  - Develop and provide automated web-based testing for implementers of widely used protocols with security consequences.

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
- Many challenges remain.