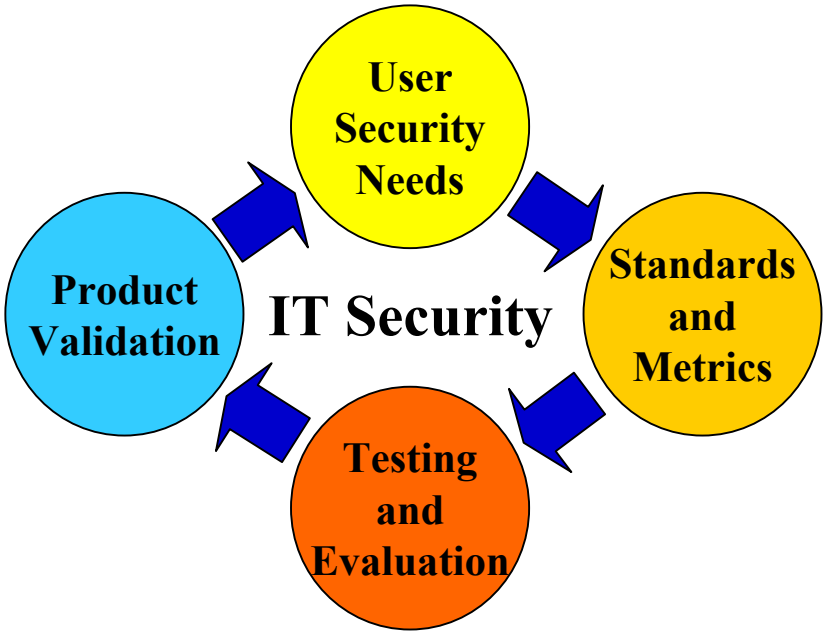
The Security Testing and Metrics Group

(CMVP, NIAP, and C&A)

Ray Snouffer
Manager, Security Testing and Metrics Group

National Institute of Standards and Technology
December 16, 2003

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

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

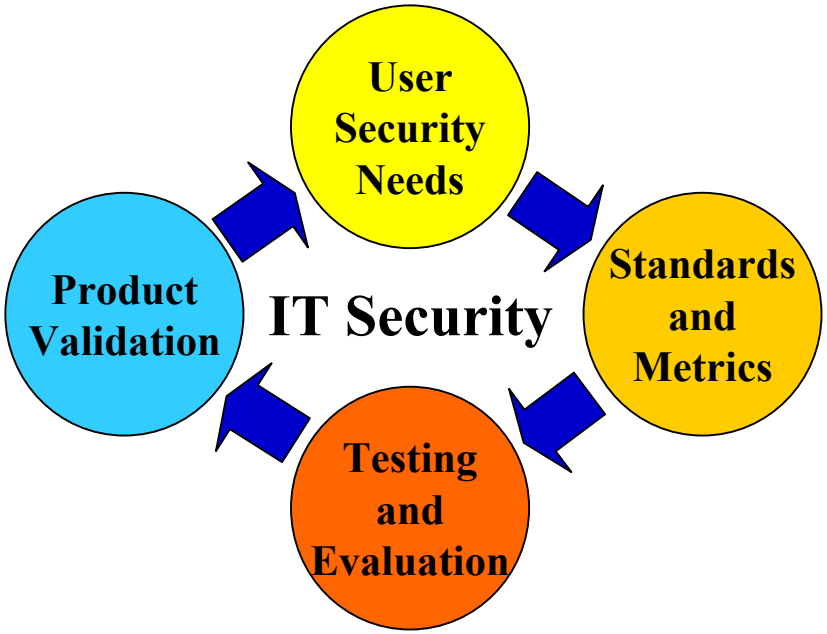
Impacts

•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

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

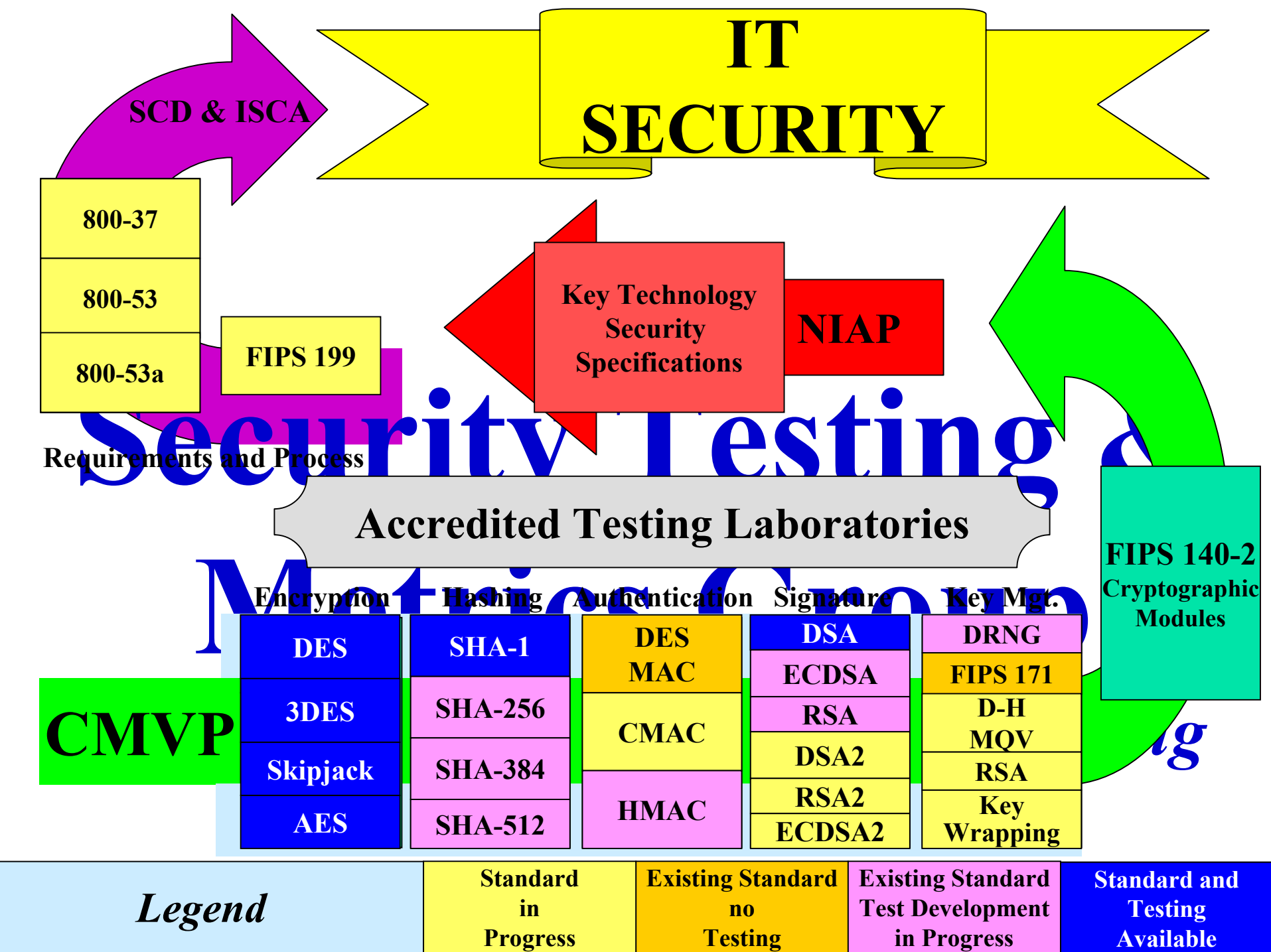
Global: Canada, United Kingdom, France, Germany, Korea

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

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


IT SECURITY
SCD & ISCA
800-37
800-53
800-53a
FIPS 199
Key Technology Security Specifications
NIAP
Requirements and Process
Accredited Testing Laboratories
FIPS 140-2 Cryptographic Modules
CMVP
Encryption
Hashing
Authentication
Signature
Key Mgt.
DES
3DES
Skipjack
AES
SHA-1
SHA-256
SHA-384
SHA-512
DES MAC
CMAC
HMAC
DSA
ECDSA
RSA
DSA2
RSA2
ECDSA2
DRNG
FIPS 171
D-H MQV
RSA
Key Wrapping
Legend
Standard in Progress
Existing Standard no Testing
Existing Standard Test Development in Progress
Standard and Testing Available

… Making a Difference

- Cryptographic Modules Surveyed (during testing)
  - 48.8% Security Flaws discovered
  - 96.3% Documentation Errors

- Algorithm Validations (during testing)
  (DES, Triple-DES, DSA and SHA-1)
  - 26.5% Security Flaws
  - 65.1% Documentation Errors

Cryptographic Module Validation Program

Goals

- Improve the security and technical quality of cryptographic products
- Provide U.S. Canadian, and U.K. 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
- Joint work between NIST, ANSI and international standards bodies

Impacts

- Provide Federal agencies (U.S., Canada, and UK) with confidence that a validated cryptographic product meets a claimed level of security
- Supply a documented methodology for conformance testing of cryptographic algorithms and modules
- 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
Logica Security Consulting
CORSEC Security Inc.
AEPOS

Global: Communications Security Establishment (CSE) - Canada
Communications-Electronics Security Group (CESG) – UK
National Security Research Institute (NSRI) – South Korea
France
Germany

FY 2003

- Validated 160+ crypto modules and 275+ crypto algorithm implementations
- Designed and developed Cryptographic Algorithm Validation System
- Developed AES test suite and enhanced DES/TDES validation tests

FY 2004

- FIPS 140-2 validations: 160+ certificates
- Cryptographic algorithm validations: 600+ certificates
- FIPS 140-2 as an ISO standard (ISO 19790)
- Third Cryptographic Module Validation Program Workshop/Conference
- Key Establishment and Key Transport validation test suites
- Develop Validation Test Suites for new algorithms/protocols
- Research into new technology areas (e.g. wireless, JAVA, FIPS 140-2 Level 5)

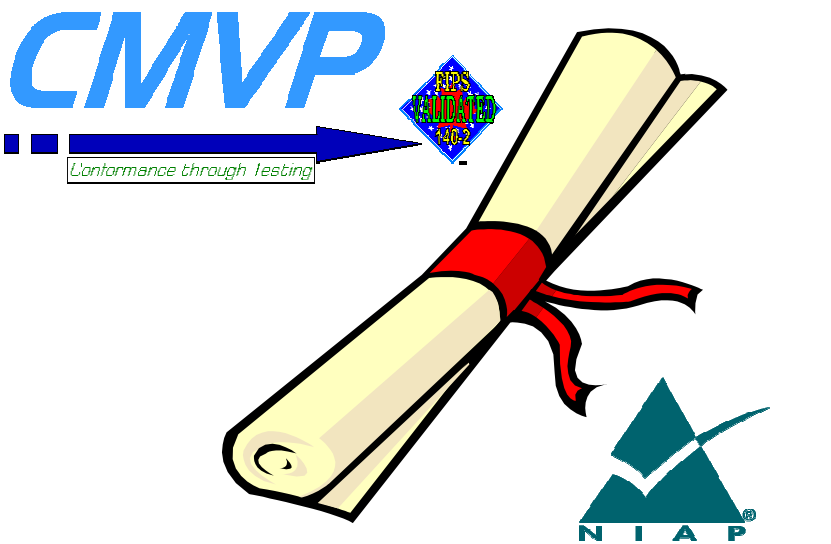
FY 2003

- Validated 160+ crypto modules and 275+ crypto algorithm implementations
- Designed and developed Cryptographic Algorithm Validation System
- Developed AES test suite and enhanced DES/TDES validation tests

FY 2004

- FIPS 140-2 validations: 160+ certificates
- Cryptographic algorithm validations: 600+ certificates
- FIPS 140-2 as an ISO standard (ISO 19790)
- Third Cryptographic Module Validation Program Workshop/Conference
- Key Establishment and Key Transport validation test suites
- Develop Validation Test Suites for new algorithms/protocols
- Research into new technology areas (e.g. wireless, JAVA, FIPS 140-2 Level 5)

Laboratory Accreditation



Goals

- To accredit fully qualified Common Criteria Testing and Cryptographic Module Testing laboratories.
- Promote the technical competence of accredited and applicant laboratories.

Technical Areas

- Development of new methods of proficiency testing for accreditation and re-accreditation.
- Development of continuous training opportunities for laboratories.

Impacts

- Highly qualified accredited laboratories for Common Criteria and Cryptographic Module Testing.
- Consistent evaluations and validations for use by Federal agencies and private sector.
- Pool of technical experts in Common Criteria and Cryptographic Module testing.

Collaborators

Federal: National Voluntary Laboratory Accreditation Program (NVLAP), NSA

Industry: 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; Logica Security Consulting; Booz Allen Hamilton Common Criteria Testing Laboratory; Cable and Wireless Common Criteria Testing Laboratory; Computer Sciences Corporation; SAIC Common Criteria Testing Laboratory; CORSEC Security Inc.

Global: Communications Security Establishment (CSE) – Canada
Communications-Electronics Security Group (CESG) – UK

FY 2003

- Accredited 1 Cryptographic Module Testing (CMT) Laboratories
- Accredited 2 Common Criteria (CC) Testing Laboratories
- 8 Re-accreditations (5 CMT, 3 CC)
- Revised Handbook 150-17
- FIPS 140-2 Level 3 Hardware testing artifact

FY 2004

- Cryptographic Module Testing Laboratories
  - o New North American: 2
  - o New International: 2
  - o Re-accreditation: 6
- Common Criteria Testing Laboratories
  - o New Domestic: 3
  - o Re-accreditation: 5

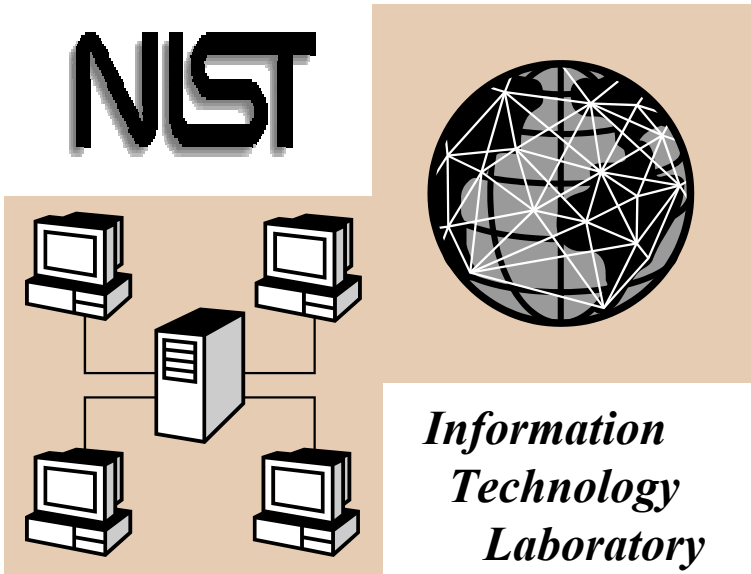
FY 2003

- Accredited 1 Cryptographic Module Testing (CMT) Laboratories
- Accredited 2 Common Criteria (CC) Testing Laboratories
- 8 Re-accreditations (5 CMT, 3 CC)
- Revised Handbook 150-17
- FIPS 140-2 Level 3 Hardware testing artifact

FY 2004

- Cryptographic Module Testing Laboratories
    - o New North American: 2
    - o New International: 2
    - o Re-accreditation: 6
- Common Criteria Testing Laboratories
    - o New Domestic: 3
    - o Re-accreditation: 5

Security Certification and Accreditation Project



Goals

- To develop standards and guidelines for conducting security certifications and accreditations of federal information systems
- To facilitate the development of a national network of accredited organizations capable of providing cost effective, quality security certification services based on the standards and guidelines

Technical Areas

- Techniques and procedures for system level security evaluations

Impacts

- More consistent, comparable, and repeatable system-level evaluations of federal information systems
- More complete, reliable technical information for information system authorizing officials—leading to better understanding of complex systems and associated risks and vulnerabilities
- Greater availability of competent certification services for public and private sector customers

Collaborators

Federal: Departments of Defense, Homeland Security, Energy, Justice, State, Treasury, Veterans Affairs, Transportation, Commerce, Health and Human Services, NSA, OMB, GSA, GAO, state and local governments

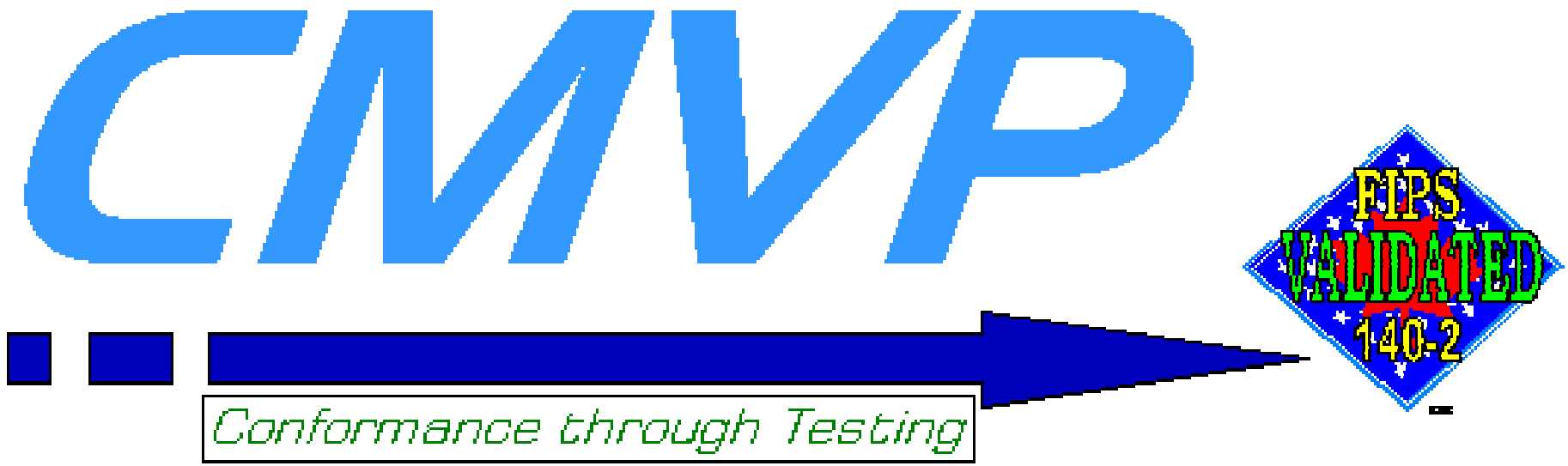
Industry: Audit, insurance, healthcare industry consortia, IT trade associations, IT developers, systems integrators

FY2003

- First draft NIST Special Publication 800-37 (1st QTR FY03)
- Second draft NIST Special Publication 800-37 (3rd QTR FY03)

FY2004

- Final draft NIST Special Publication 800-37 (1st QTR FY04)
- Assessment Scheme Concept of Operations (2nd QTR FY04)
- Public workshop and C&A conference (3rd QTR FY04)
- First draft NIST Special Publication 800-53A (2nd QTR FY04)
- Second draft NIST Special Publication 800-53A (4th QTR FY04)
- Development of approval criteria and proficiency tests for certification service providers (4th QTR 04)


CMVP
FIPS
VALIDATED
140-2
Conformance through Testing

Cryptographic Module Validation Program (CMVP)

- Established by NIST and the Communications Security Establishment (CSE) in 1995
- Original FIPS 140-1 requirements and updated FIPS 140-2 requirements developed with industry input
  - Four increasing levels of security
- Seven NVLAP-accredited testing laboratories
  - True independent 3rd party accredited testing laboratories
  - Can not test and provide design assistance
  - Several potential new labs

CMVP: Applicability of FIPS 140-2

- U.S. Federal organizations must use validated cryptographic modules
- With the passage of the Federal Information Security Management Act of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards.
- GoC departments are recommended by CSE to use validated cryptographic modules
- International recognition

CMVP Status (as of October 31, 2003)

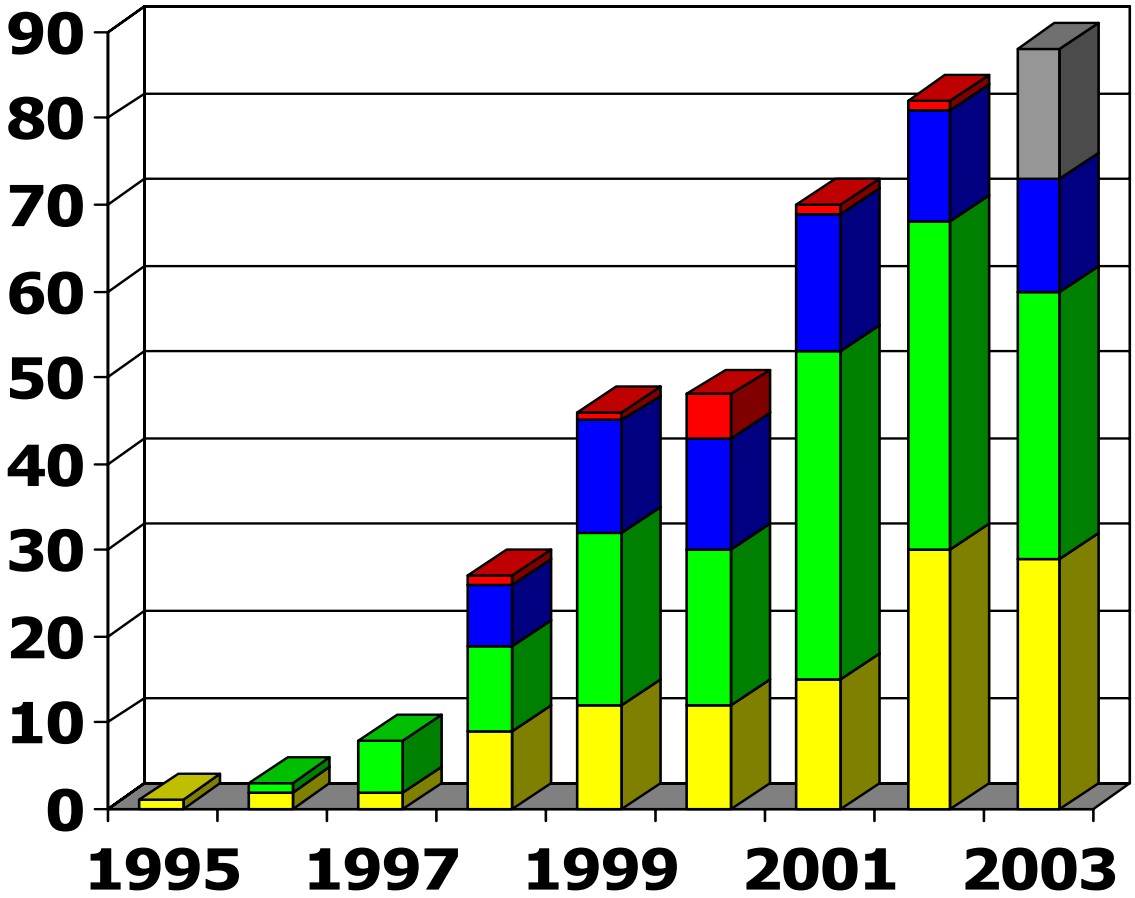
- Continued record growth in the number of cryptographic modules validated
  - Over 350 Validations representing over 750 modules
- All four security levels of FIPS 140-1 represented on the Validated Modules List
- Over 100 participating vendors

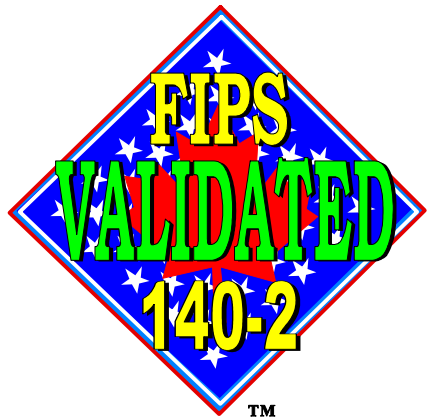
Participating Vendors

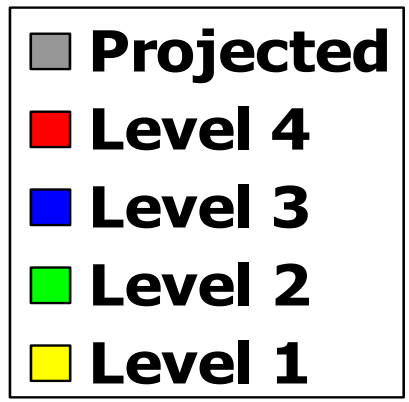
(October 30, 2003)

3e Technologies International, Inc.
3S Group Incorporated
ActivCard
Admiral Secure Products, Ltd.
AEP Systems
Aladdin Knowledge Systems, Ltd.
Alcatel
Algorithmic Research, Ltd.
Atalla Security Products of Hewlett Packard Corporation
Altarus Corporation
Attachmate Corp.
Avaya, Inc.
Blue Ridge Networks
Bodacion Technologies
Certicom Corp.
Check Point Software Technologies Ltd.
Chrysalis-ITS Inc.
Cisco Systems, Inc.
Colubris Networks, Inc.
Communications Devices, Inc.
Control Break International Corp.
Corsec Security, Inc.
Cranite Systems, Inc.
Cryptek Inc.
CTAM, Inc.
CyberGuard Corporation
Cylink Corporation
Dallas Semiconductor, Inc.
Datakey, Inc.
Ensuredmail, Inc.
Entrust Inc.
Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd.
Entrust CygnaCom
F-Secure Corporation
Fortress Technologies, Inc.
Francotyp-Postalia
Gemplus Corp. and ActiveCard Inc.
GTE Internetworking
Hasler, Inc.
Information Security Corporation
IBM Corporation
IBM® Zurich Research Laboratory
Intel Network Systems, Inc.
IP Dynamics, Inc.
IRE, Inc.
ITT
Kasten Chase Applied Research
L-3 Communication Systems
Lipman Electronic Engineering Ltd.
Litronic, Inc.
Lucent, Inc.
M/A-Com, Inc.
Microsoft Corporation
Motorola, Inc.
Mykotronx. Inc
National Semiconductor Corp.
nCipher Corporation Ltd.
Neopost
Neopost Industrie
Neopost Ltd.
Neopost Online
Netscape Communications Corp.
NetScreen Technologies, Inc.
Nortel Networks
Novell, Inc.
Oberthur Card Systems
Oracle Corporation
Palm Solutions Group
PGP Corporation
Phaos Technology Corporation
Pitney Bowes, Inc.
Pointsec Mobile Technologies
PrivyLink Pte Ltd
PSI Systems, Inc.
Rainbow Technologies
RedCreek Communications
Research In Motion
RSA Security, Inc.
SafeNet, Inc.
SchlumbergerSema
Securit-e-Doc, Inc.
Sigaba Corporation
Simple Access Inc.
SingleSignOn.Net, Inc.
SonicWALL, Inc.
Spyrus, Inc.
Stamps.com
Standard Networks, Inc.
StoneSoft Corporation
Sun Microsystems, Inc.
Symbol(Columbitech)
Technical Communications Corp.
Thales eSecurity
TimeStep Corporation
Transcrypt International
Tumbleweed Communications Corp.
Ultra Information Systems, Inc.
ValiCert, Inc.
V-ONE Corporation, Inc.
Wei Dai
WinMagic Incorporated

FIPS 140-1 / FIPS 140-2 Validations by Year / Level
(Certificates Issued – December 15, 2003)

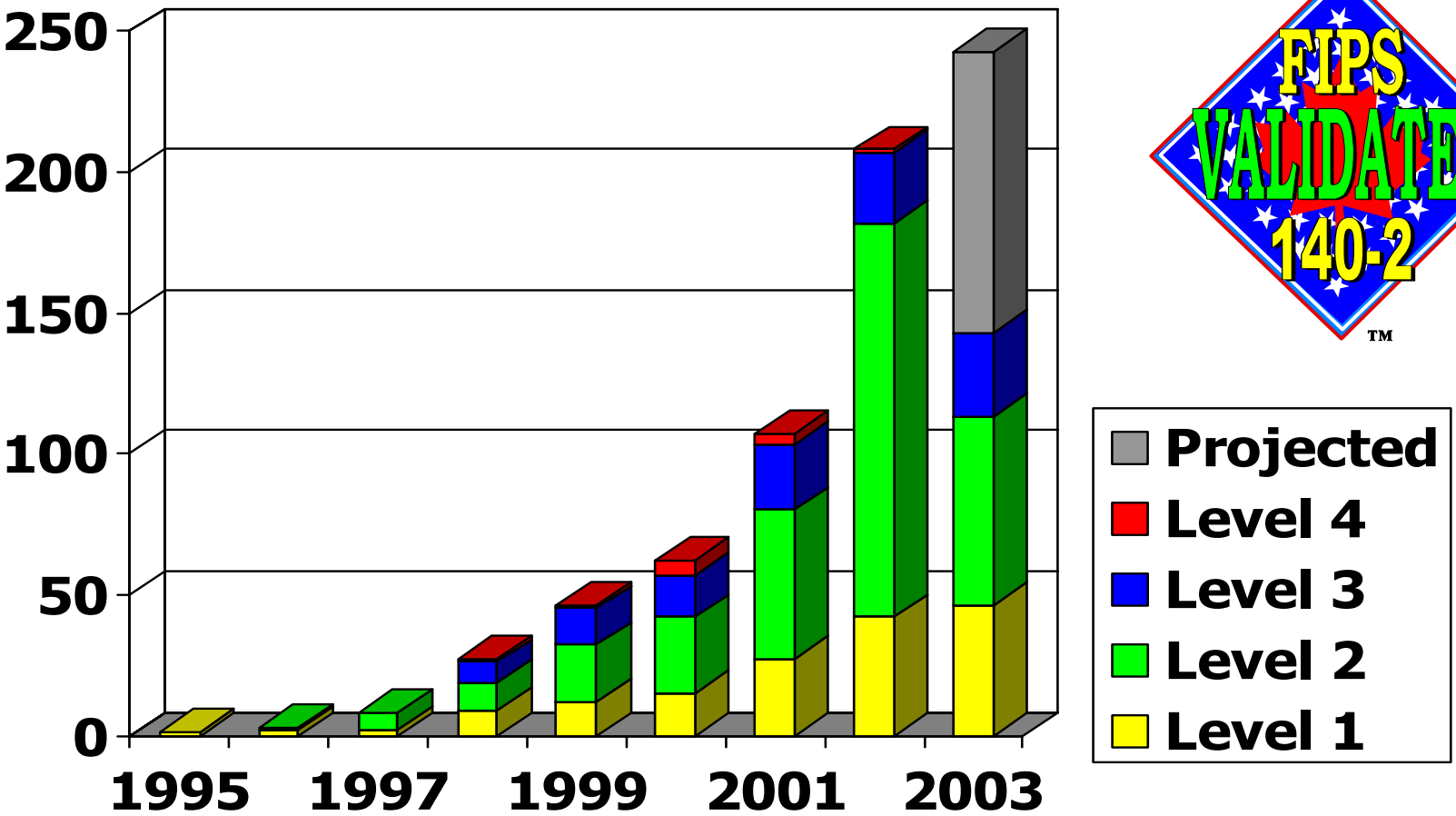




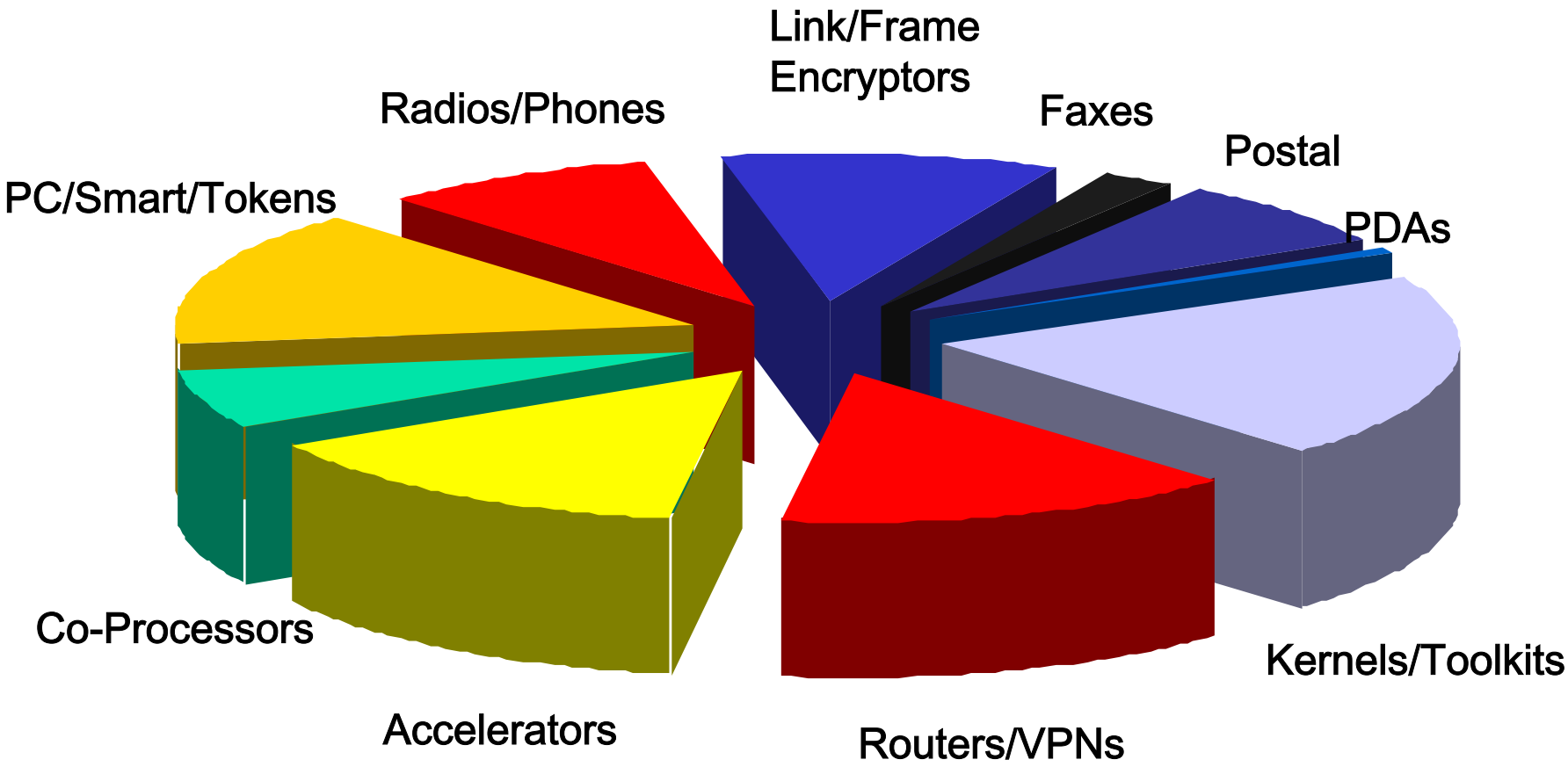


FIPS 140-1 / FIPS 140-2 Validations by Year / Level
(Modules Validated – December 15, 2003)

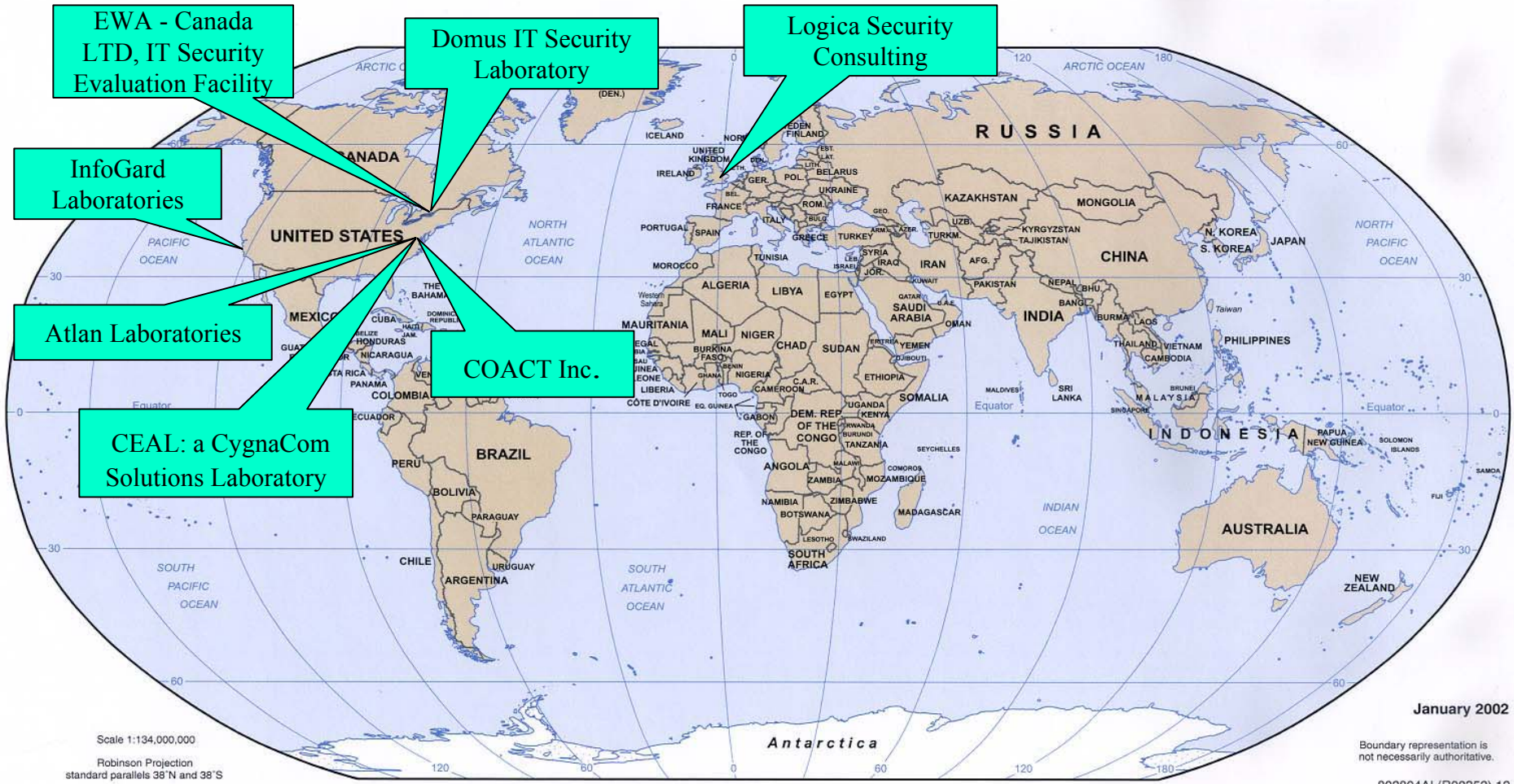
Program To Date: Over 750 Modules Validated !



Validated Modules By Type



CMVP: Accredited Laboratories



Seventh CMT laboratory added in 2002

International Acceptance

Communications-Electronics Security Group (CESG) - UK

- December 28, 2001
  - CESG proposes the use of FIPS 140 as the basis for the evaluation of cryptographic products used in a number of UK government applications and encourages the setting up of accredited laboratories in the UK to perform these evaluations.

FIPS 140-2 to ISO/IEC…..

- FIPS 140-2 is the *de facto* international standard for cryptographic module security requirements
  - Cryptographic modules on the Validated Modules List developed by vendors from around the world
    - Australia, Israel, Singapore, U.K., France, Finland, Germany, Canada
  - Protection Profiles developed throughout the world reference FIPS 140-1 and FIPS 140-2
- FIPS 140-2 developed to facilitate conversion to an ISO standard

ISO, *Security Requirements for Cryptographic Modules*

- Overview of changes
  - Inclusion of ISO terms and definitions
  - Inclusion of ISO references
  - Deletion of EMI/EMC section (a US FCC requirement)
  - Revisions based on proposed modifications to FIPS 140-2 (primarily "clean up")
  - Revision of random number generator (RNG) tests to include ISO standards
    - Applicable to deterministic and non-deterministic RNGs

ISO 19790: Security Requirements for Cryptographic Modules

- ISO 19790 – content and format same as FIPS 140-2
  - No major technical changes
- Document schedule
  - Working draft (WD): November 2002
  - Committee Draft (CD): May 2004
  - Final Draft International Standard (FDIS): November 2004
  - International Standard (IS): May 2005

ISO 19790: Security Requirements for Cryptographic Modules

- Editor:
  - Randall Easter (US)
- Co-editors:
  - Mike Chawrun (Canada)
  - Jean-Pierre Quemard (France)

CMVP: New Areas and Possibilities
(unfunded)

- Training for laboratories
- New proficiency testing artifacts
- New test methods
- Test suites for non-FIPS algorithms

Building More Secure Systems for the New Millennium
(sm)

Terminology Note

- *Common Criteria* – ISO 15408 – Dictionary
- *Protection Profiles / Security Targets* – specific functional and assurance requirements
- *NIAP / National Information Assurance Partnership* – US scheme for CC-based testing
- *Key Government Policies*
  - National Security Systems (NSTISSP #11 aka CNSS #11)
  - Unclassified systems – NIST 800-23

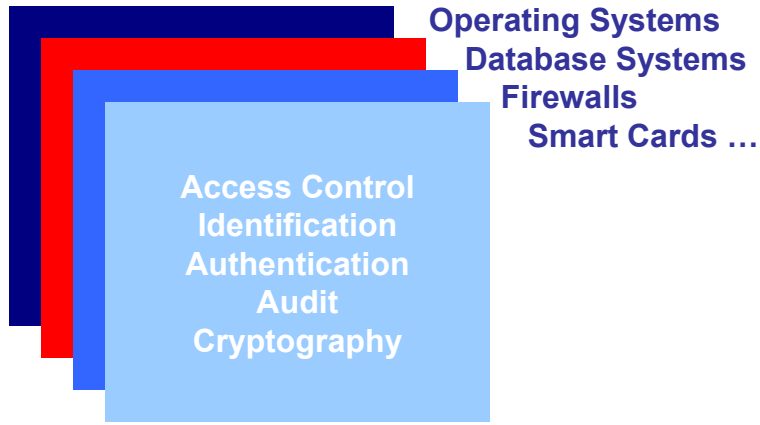
The term "CC" is sometimes used loosely for all of the above. We need to be precise.

Use of CC to Define Requirements

ISO Standard 15408

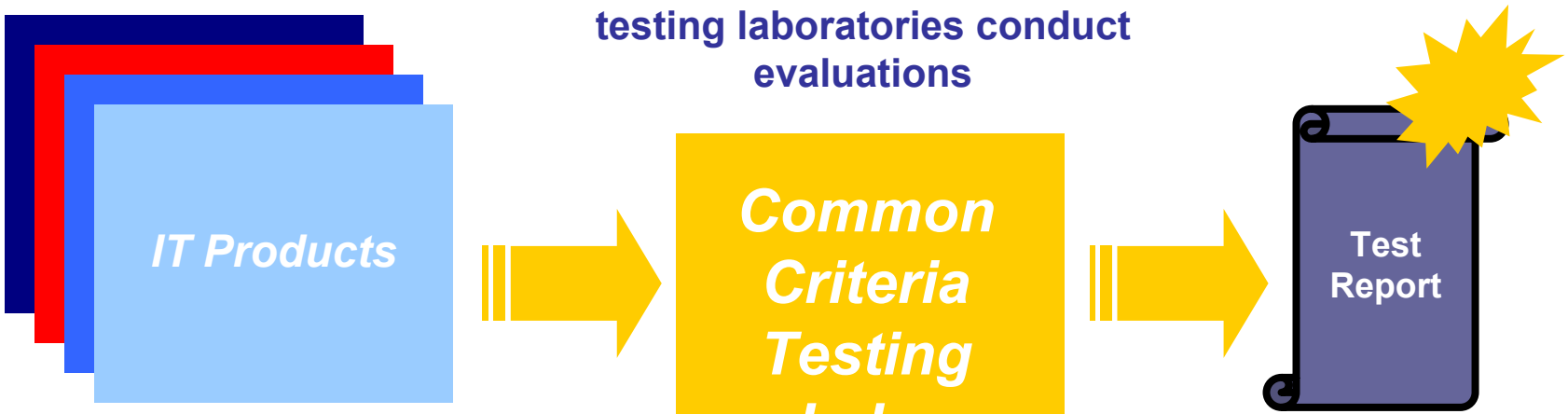
A flexible, robust catalogue of IT security requirements (features and assurances)

Protection Profiles



Security requirements in specific information technology areas

Security Evaluation



Examples of Uses

- User communities

  US Government – NSA the most active – medium robustness focus

  - Smartcard community
  - Financial Services Roundtable/BITS
  - Healthcare community
  - Process control community
  - IEEE
- New uses of the CC: research & application
  - Composite evaluations
  - Composite PPs
  - System evaluations
  - Technology-specific applications of the CC

NIAP Testing Advantages

- Specification of security features and assurances based on an international standard
- Evaluation methodology based on an international standard---leading to comparability of test results
- Government technical oversight
- Testing results recognized by many nations

Mutual Recognition of Evaluations

NIAP, in conjunction with the U.S. State Department, negotiated a CC Recognition Arrangement that:

- Provides recognition of U.S. issued certificates by 18 nations
- Eliminates need for repeating security evaluations
- Supports global market opportunities
- Applies for EAL 1-4 only

Meaning of the Certificate

- **Does** mean that the government CCMRA members believe the evaluation has been conducted properly and the conclusions of the private sector testing laboratories are consistent with the evidence produced.
- **Does** imply that a good faith effort has been made to ensure that the product conforms to the security claims stated by the vendor in the security specification.
- **Does not** imply **with absolute certainty** that the product conforms to the security claims stated by the vendor in the security specification.
- **Does not** imply that the product conforms to security claims in documents other than the security specification (i.e., security claims in promotional literature, vendor documentation, and other documents **are not** covered by the validation certificate).
- **Is not** an endorsement or warranty of the product by NSA, NIST, NIAP or equivalent foreign government organizations.
- **Does not** imply or guarantee that the product is free from malicious or erroneous code.
- **Does not** imply that security functional specifications and achieved level of assurance of the product provide adequate protection for data contained in the product's intended operational environment.
- **Does not** presume that subsequent versions or releases of the product should not be or do not have to be evaluated.

Status

- As of October 2003
  - 59 products "in process" (58 STs, 1PP)
  - 48 certificates issued to date (32 STs, 16 PPs)
  - 14 cancelled / withdrew
- Historical
  - 2001 – 11 certs
  - 2002 – 22 certs
  - 2003 – 16 certs

Lack of significant improvements in testing & test methods

- Still done much as before
- Not high research priority
- Little automation
- At higher assurance levels (> EAL 4) still:
  - More art than science
  - More subjective than objective
  - Very labor intensive
  - Very costly
  - Can not really measure "security improvement"

Improving…

Here are some examples of what *could* be done(*):

- Develop PPs for basic robustness for use by a wide community in key technology areas by involving vendors, users, and government → goal of single-voice consensus

- Develop corresponding technology area-specific tests and test methods (e.g., smart cards, biometrics) that will provide more uniformity and comparability of evaluation results and result in more rapid evaluations for products.

(*) with resources

Improving…

Here are some examples of what *could* be done(*):

- Develop NIAP guidance advising product developers how to reuse evaluation results from prior evaluations of the product.

- Develop NIAP guidance to maintain Common Criteria certificates for product maintenance changes (i.e., new versions) without the need to undergo a complete new evaluation.

(*) with resources

Improving…

Here are some examples of what *could* be done(*):

- Develop an Assurance Maintenance module for the standard so only the changes to a previously evaluated product need be evaluated.
- Develop CC interpretations that clarify and simplify how parts of the CC are to be evaluated.
- Using technology area-specific tests and test methods, establish accreditation criteria for labs that wish to specialize in evaluating products in a specific technology area (e.g., smart cards). Extend NIAP accreditation, on a voluntary basis, to those labs that wish to specialize in the technology area. This will result in cheaper, more rapid and more consistent evaluations for products in those technology areas

(*) with resources

Improving…

Here are some examples of what *could* be done(*):

- Provide better training to lab evaluators and NIAP validators, with emphasis on which actions need to be performed and which do not.
- Provide an extensive/complete set of guidance documents for all stakeholders in the evaluation process (e.g., developers, evaluators, validators, commercial and government users).
- Provide clear guidance to stakeholders to choose only those assurance requirements that are meaningful for their intended use/environments.

(*) with resources

Improving…

Here are some examples of what *could* be done(*):

Perform a critical assessment of the current evaluation process to ensure that:

- NIAP activities and levels of effort are consistent with those of other CC Recognition Arrangement partners
- Evaluation activities are being performed efficiently
- There are no unnecessary activities being performed
- All activities that can be performed in parallel are in fact done that way.

(*) with resources

Looking beyond CC and NIAP

- Conduct more **research** with the objective of developing new means to conduct security testing. The current techniques we have are either too expensive, involve too much human subjectivity, or both.

- While it is important to understand and test security at the *product* level (the principal focus of NIAP), we need also to **look outwards at the *system* and *enterprise architecture* level**. For example, we need a means to rigorously understand the security implications that result when NIAP evaluated products are integrated together into a system. We also need to look inwards at IT building blocks such as protocols. Again, research will be a key to advancing our ability to make significant strides.

- We also need to **look beyond the (admittedly important) question of whether a product meets a security specification** at other important security issues. How do we gain assurance that the product does not do what is unintended? How can we gain assurance that no malicious code is buried deep inside software or hardware? How can we do such analysis as more and more development is taking place off-shore? Again, research is needed.

Questions / Discussion

Additional Slides

Examples of CC use

- The major bankcard issuers (e.g., American Express, Mastercard, Visa) formed a working group that used the CC to develop a profile for the smartcards they issue to their customer banks. A significant effort (the first of this type) was the group's development of their profile for smartcards.

- The Financial Services Roundtable/BITS, whose members consist of major banks and insurance companies, has used the CC to specify the security functionality its members would like to see in various IT products. When a product that meets BITS security functionality receives a CC certificate, BITS will issue its mark on that product based on the CC evaluation that was performed.

- Process Control Security Requirements Forum (PCSRF), led by NIST, is composed of government and private sector representatives who are defining security requirements for products used in real-time processing and SCADA systems. The goal of this effort is to influence the key vendors that supply products and systems globally for real-time and SCADA systems to meet process control security requirements. If vendors respond to these market signals, the improved security would be reflected in major critical infrastructure systems such as nuclear power plant control; electric power generation and distribution; control of water distribution; building environmental, security, and safety controls; and manufacturing plant controls.

- The healthcare community, with NIST's assistance, has used the CC for defining security requirements. Examples include: functional security requirements for Health Care Financing Administration's Proposed Internet Security Policy; functional security requirements for the Department of Health and Human Services which maps the Health Insurance Portability and Accountability Act of 1996 Proposed Rule on "Digital Signature and Security Standards" into CC constructs; and a complete profile for patient "Point-of-Care Admission, Discharge and Transfer" in collaboration with Share Medical Systems (SMS).

Some International Uses of CC

- France: Regulation recommending the use of CC evaluations for public administration
- European Union:
  - Resolution on information and network security
  - Electronic signature
  - European central bank.
- NATO: CC is the standard
- Germany: CC evaluations required in digital signature legislation

How Component Evaluations Contribute to IS Assurance