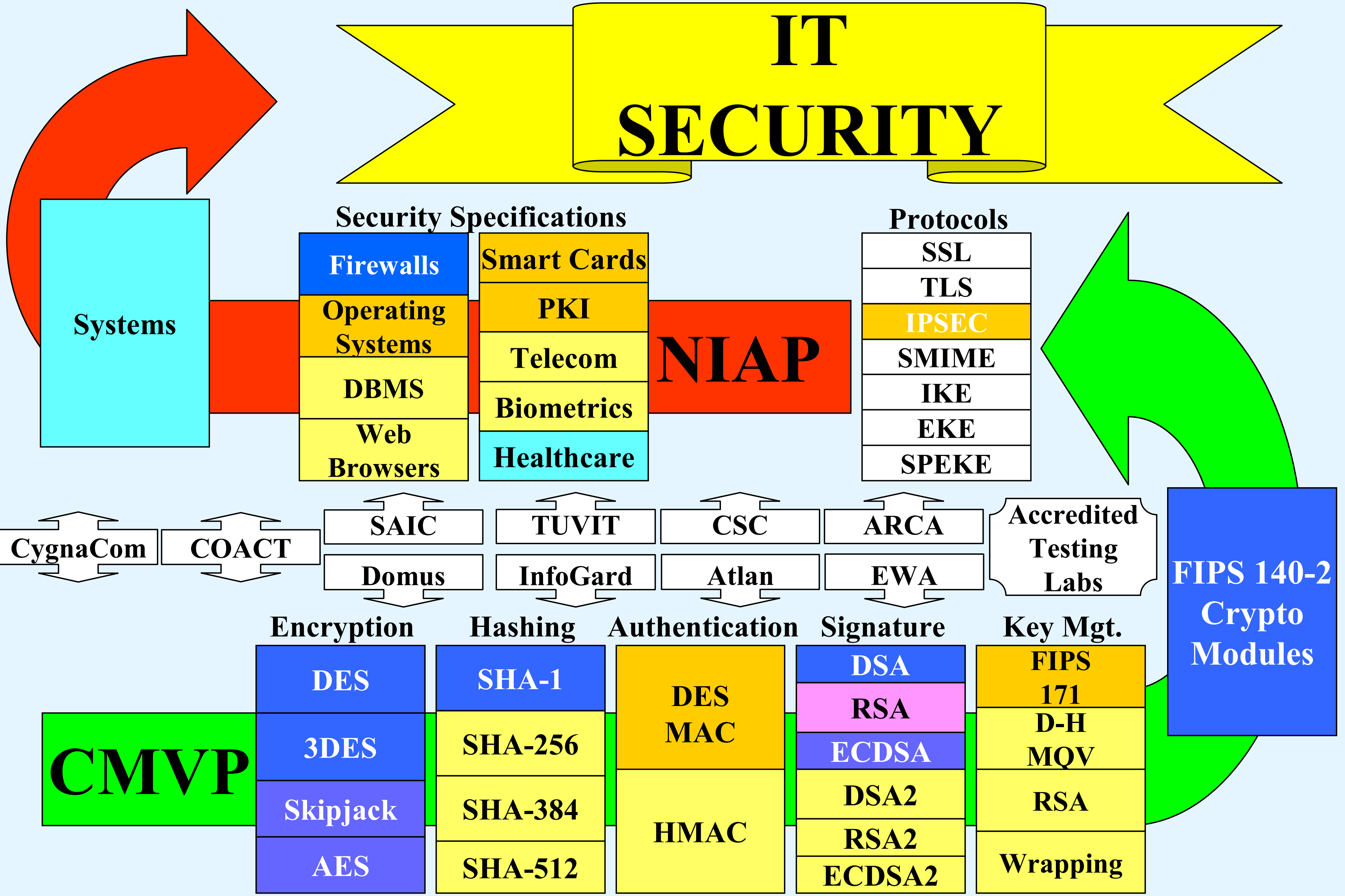
CMVP Status and FIPS 140-1&2

Annabelle Lee

Director, CMVP

March 26, 2002

IT SECURITY



Systems

NIAP

Security Specifications

Firewalls

Operating Systems

DBMS

Web Browsers

Smart Cards

PKI

Telecom

Biometrics

Healthcare

Protocols

SSL

TLS

IPSEC

SMIME

IKE

EKE

SPEKE

CygnaCom

COACT

SAIC

Domus

TUVIT

InfoGard

CSC

Atlan

ARCA

EWA

Accredited Testing Labs

FIPS 140-2 Crypto Modules

CMVP

Encryption

DES

3DES

Skipjack

AES

Hashing

SHA-1

SHA-256

SHA-384

SHA-512

Authentication

DES MAC

HMAC

Signature

DSA

RSA

ECDSA

DSA2

RSA2

ECDSA2

Key Mgt.

FIPS 171

D-H MQV

RSA

Wrapping

Industry Standard, Specification or Recommendation	Future Standard, Specification or Recommendation	Standard in Progress	Existing Standard no Testing	Existing Standard Test Development in Progress	Standard and Testing Available

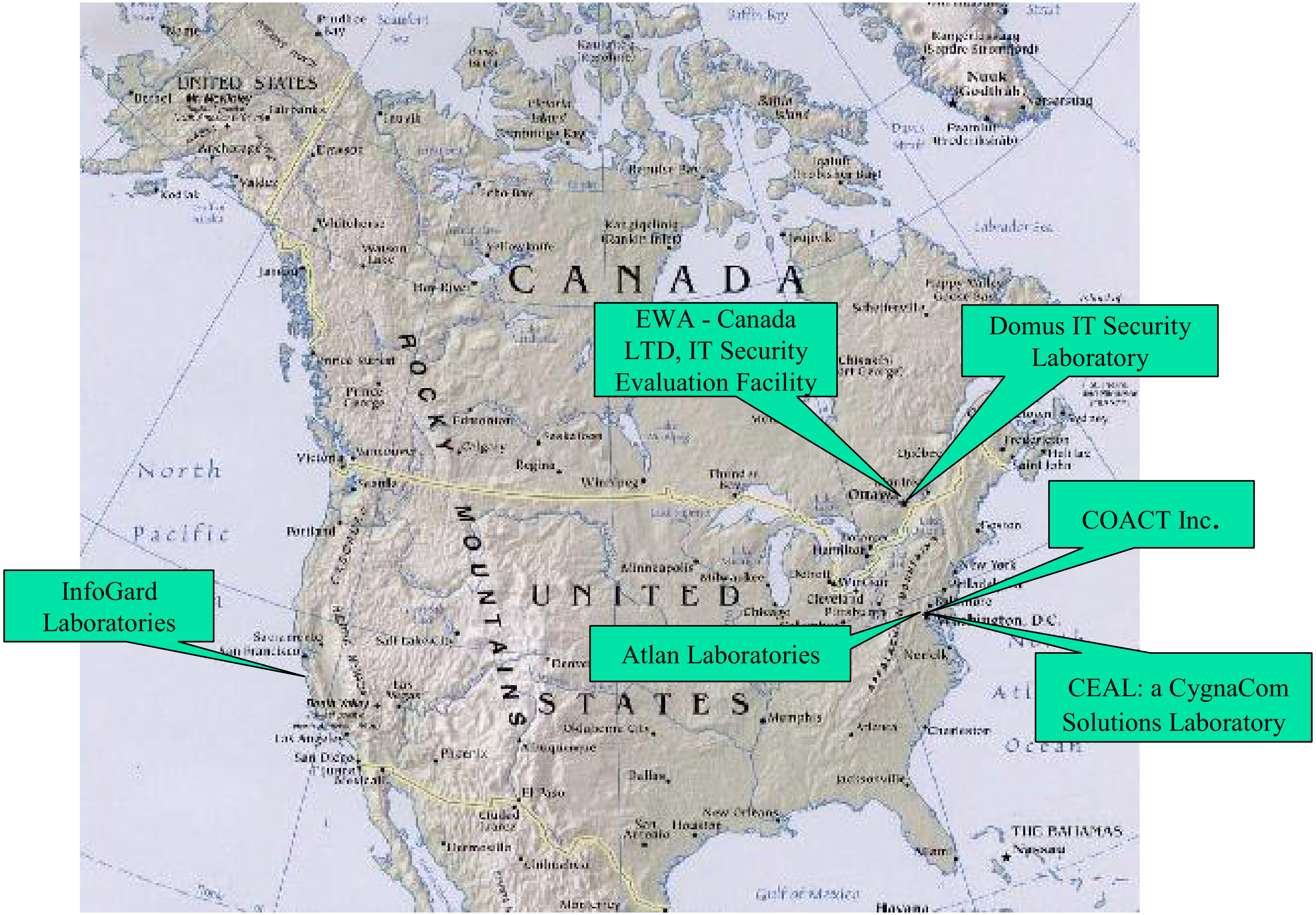
FIPS
VALIDATED
140-1
TM

FIPS
VALIDATED
140-2
TM

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
- Six NVLAP-accredited testing laboratories
  - True independent 3rd party accredited testing laboratories
  - Cannot test and provide design assistance

CMVP Accredited Laboratories


EWA - Canada LTD, IT Security Evaluation Facility

Domus IT Security Laboratory

COACT Inc.

InfoGard Laboratories

Atlan Laboratories

CEAL: a CygnaCom Solutions Laboratory

Sixth CMT laboratory added in 2001

Applicability of FIPS 140-2

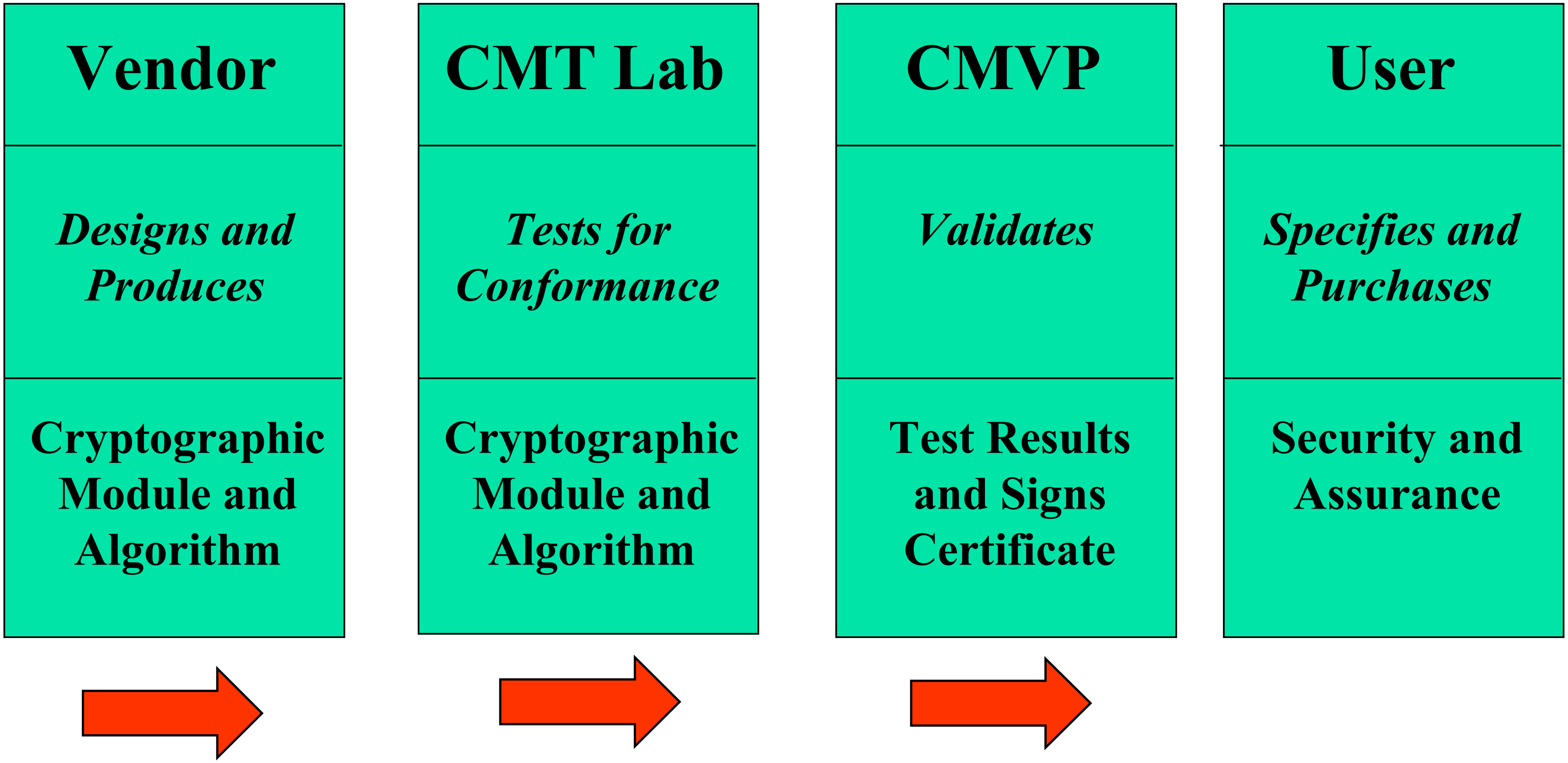
- U.S. Federal organizations must use validated cryptographic modules
- GoC departments are recommended by CSE to use validated cryptographic modules
- International recognition

CESG
protecting the information age

Communications-Electronics Security Group (CESG) - UK

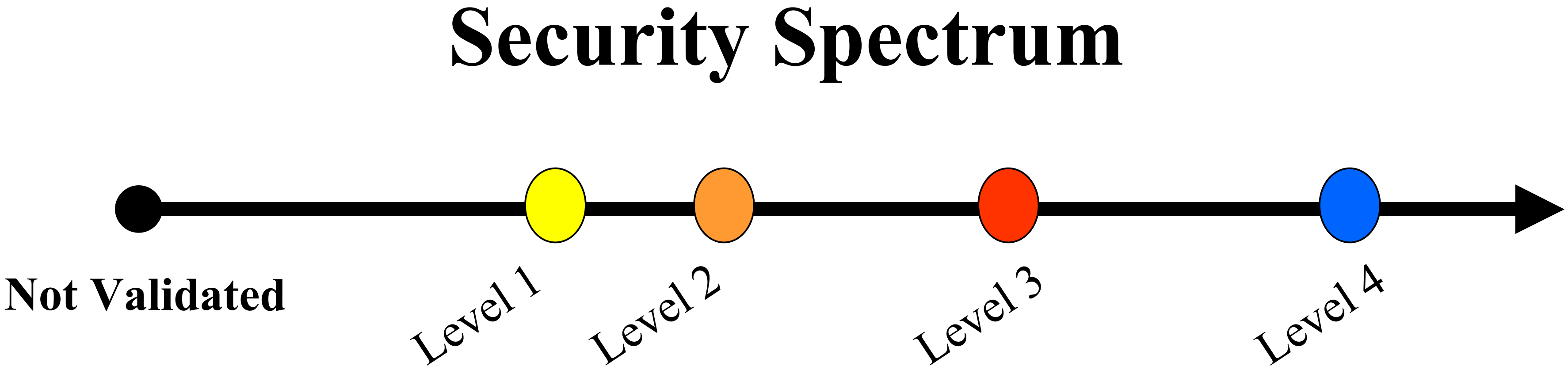
- December 28, 2001
  - – CESG proposes the use of FIPS 140 as the basis for the evaluation of cryptographic products used in a number of UK government applications and encourages the setting up of accredited laboratories in the UK to perform these evaluations.

Flow of a FIPS 140-2 Validation



Vendor	CMT Lab	CMVP	User
Designs and Produces	*Tests for Conformance*	*Validates*	*Specifies and Purchases*
Cryptographic Module and Algorithm	Cryptographic Module and Algorithm	Test Results and Signs Certificate	Security and Assurance

FIPS 140-2 Security Levels



- **Level 1 is the lowest, Level 4 most stringent**
- **Requirements are primarily cumulative by level**
- **Overall rating is lowest rating in all sections**

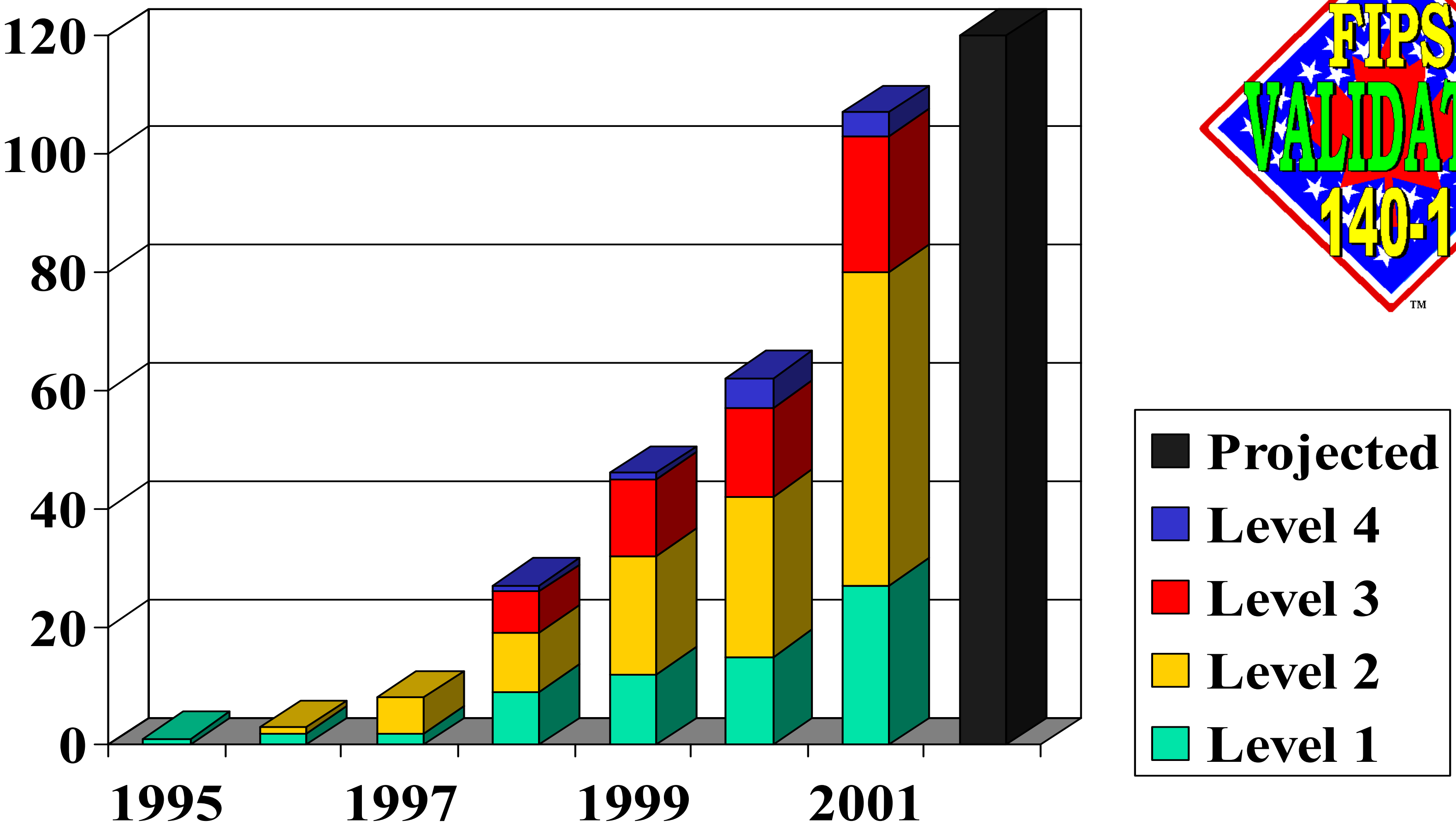
CMVP Status
(March 2002)

- Continued record growth in the number of cryptographic modules validated
  - Over 200 Validations representing nearly 250 modules
- All four security levels of FIPS 140-1 represented on the Validated Modules List
- Over forty participating vendors

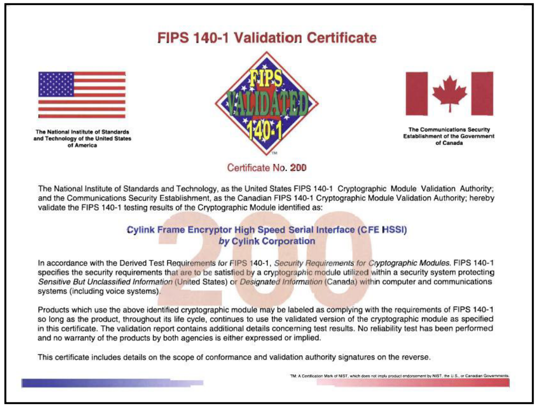
FIPS 140-1 and FIPS 140-2 Validations by Year and Level

(January 15, 2002)

FIPS VALIDATED 140-1 ™



2001 Validation Milestones



FIPS 140-1 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 200

The National Institute of Standards and Technology, as the United States FIPS 140-1 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-1 Cryptographic Module Validation Authority; hereby validate the FIPS 140-1 testing results of the Cryptographic Module identified as:

Cylink Frame Encryptor High Speed Serial Interface (CFE HSSI)
***by* Cylink Corporation**

In accordance with the Derived Test Requirements for FIPS 140-1, *Security Requirements for Cryptographic Modules.* FIPS 140-1 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive But Unclassified Information* (United States) or *Designated Information* (Canada) within computer and communications systems (including voice systems).

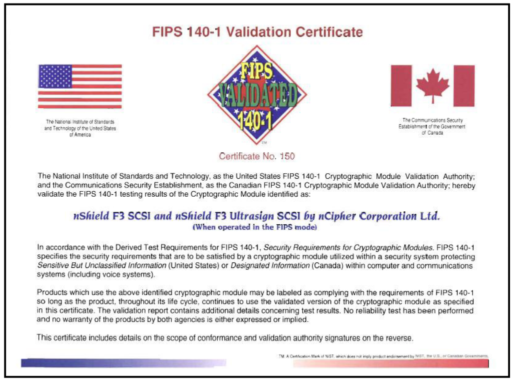
Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-1 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.

Certificate 200

December 18, 2001



FIPS 140-1 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 150

The National Institute of Standards and Technology, as the United States FIPS 140-1 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-1 Cryptographic Module Validation Authority; hereby validate the FIPS 140-1 testing results of the Cryptographic Module identified as:

nShield F3 SCSI and nShield F3 Ultrasign SCSI by nCipher Corporation Ltd.
(When operated in the FIPS mode)

In accordance with the Derived Test Requirements for FIPS 140-1, *Security Requirements for Cryptographic Modules.* FIPS 140-1 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive But Unclassified Information* (United States) or *Designated Information* (Canada) within computer and communications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-1 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

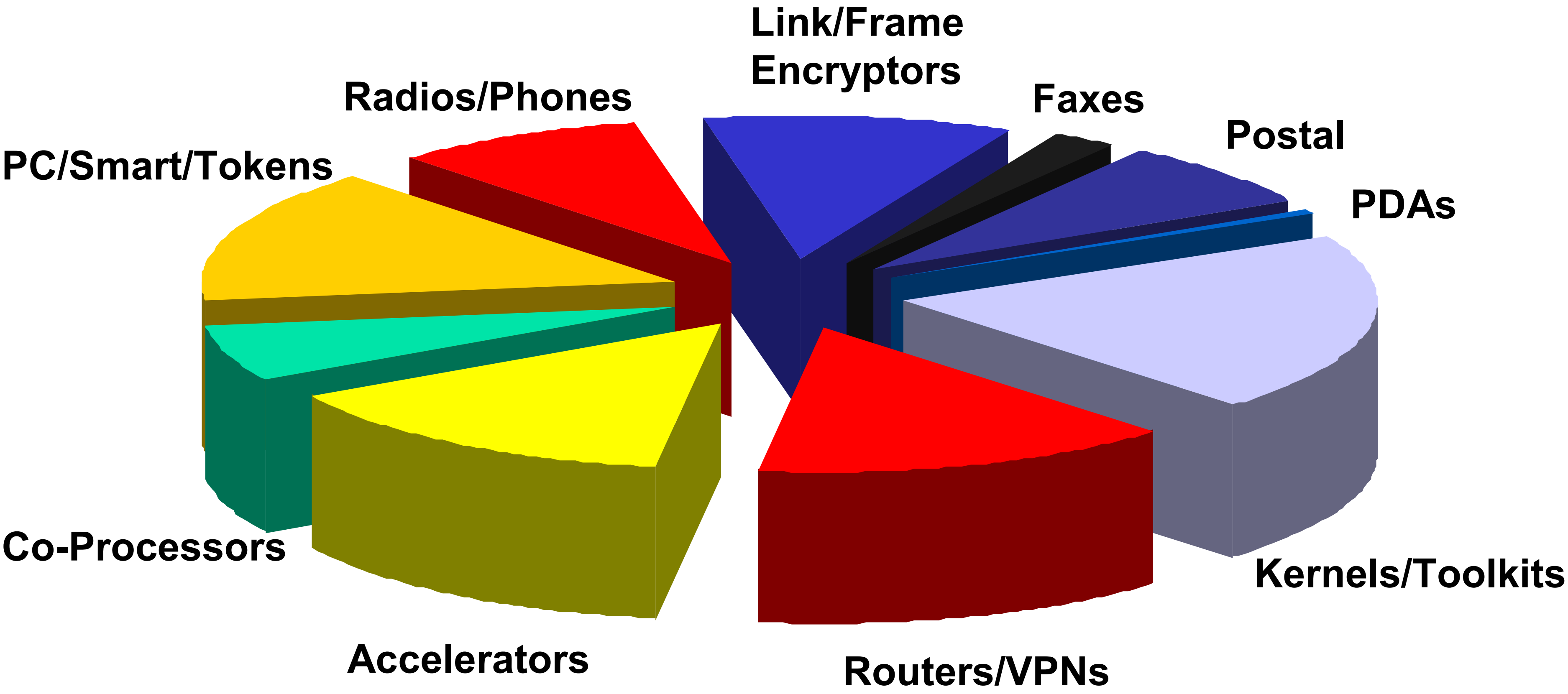
TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.

Certificate 150

May 23, 2001

- **FIPS 140-2 Signed 05/25/01**
- **FIPS 140-2 DTR Available 11/15/01**
- **FIPS 140-2 Validations Accepted**

Validated Modules By Type



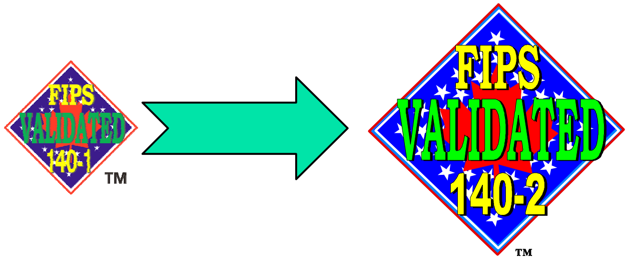
Pre-validation Status List

- Pre-validation phases
  - Implementation Under Test (IUT)
    - The crypto module and documentation are resident at the CMT lab
    - The vendor has a viable contract with the CMT lab
  - Validation Review Pending
    - Testing documentation submitted to NIST and CSE
  - Validation Review
    - Comments developed by NIST and CSE
    - Combined comments sent to CMT lab

Pre-validation Status List
(concluded)

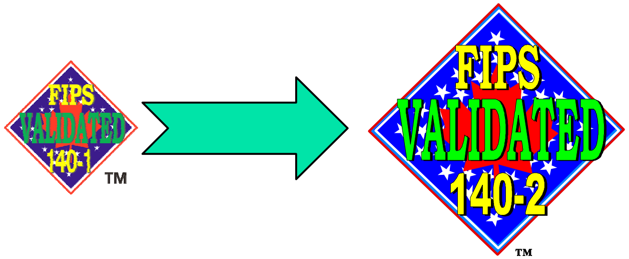
- Pre-validation phases
  - Validation Coordination (process may be iterative)
    - Testing documents revised
    - Additional documentation (if required)
    - Additional testing performed (if required)
    - Resubmission to NIST and CSE
  - Validation Finalization
    - Final resolution of validation review comments
    - Certificate number assigned
    - Certificate printing and signature process initiated

FIPS 140-2 - Testing Begins



- FIPS 140-2 Testing officially began November 15, 2001
- FIPS 140-1 Testing ends May 25, 2002
- Testing laboratories may submit FIPS 140-1 validation test reports until May 25, 2002
- After May 25, 2002 all validations and revalidations must be done against FIPS 140-2

FIPS 140-2 - Testing Begins …



- Agencies may continue to purchase, retain and use FIPS 140-1 validated products after May 25, 2002

- NIST has provided common algorithmic testing tool to Accredited Laboratories:
  - Includes DES, Triple-DES and AES
  - DSA and SHA-1 - to be integrated
  - ECDSA available as separate tool – to be integrated
  - RSA, SHA-{256,384,512}, DH, MQV - future

CMVP Status
(continued)

- End of FIPS 140-1 testing and beginning of FIPS 140-2 testing and validations with new implementations of FIPS 197 (AES) expected to cause unparalleled growth
- Increasing international recognition of the CMVP and FIPS 140-2

CMVP Status
(concluded)

- CMVP web-site
  - January 2002 through March 2002
    - Approximately 80,000 hits per month
  - November 2001
    - Over 125,000 hits

… Making a Difference

- **164 Cryptographic Modules Surveyed (during testing)**
  - 80 (48.8%) Security Flaws discovered
  - 158 (96.3%) FIPS Interpretation and Documentation Errors
- **332 Algorithm Validations (during testing) (DES, Triple-DES, DSA and SHA-1)**
  - 88 (26.5%) Security Flaws
  - 216 (65.1%) FIPS Interpretation and Documentation Errors
- **Areas of Greatest Difficulty**
  - Physical Security
  - Self Tests
  - Random Number Generation
  - Key Management

CMVP

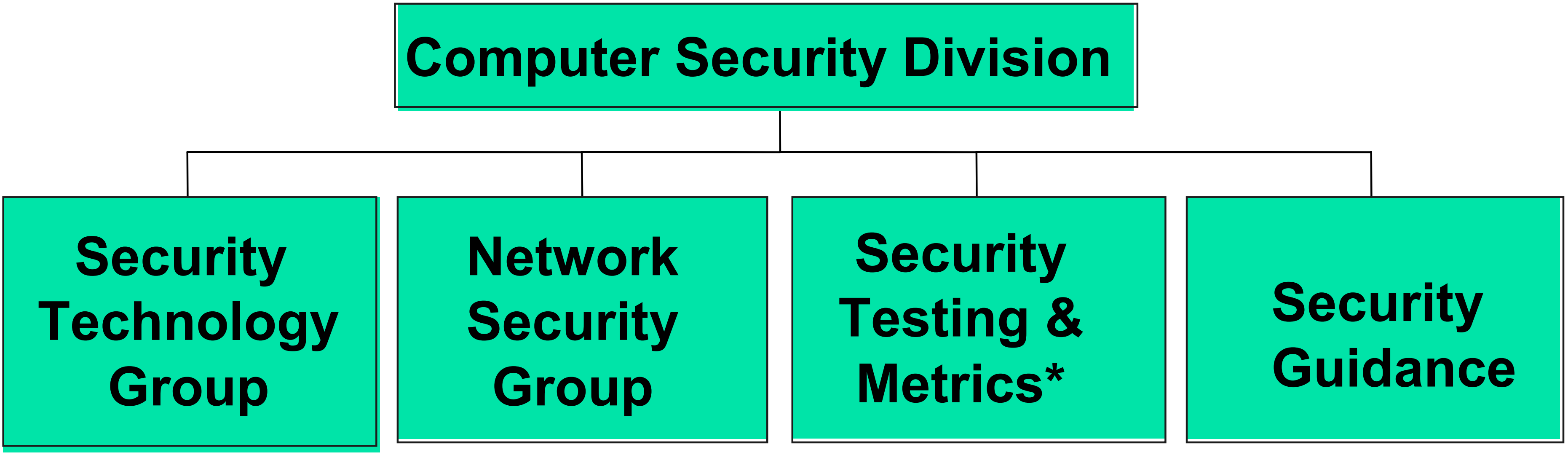
Conformance through Testing

FIPS VALIDATED 140-2

… Making a Difference

- **Program Efficiency:**
  - 107 Modules Validated in calendar year 2001 by 2.5 FTE
  - 42.8 modules per FTE

Computer Security Division Restructuring for Testing



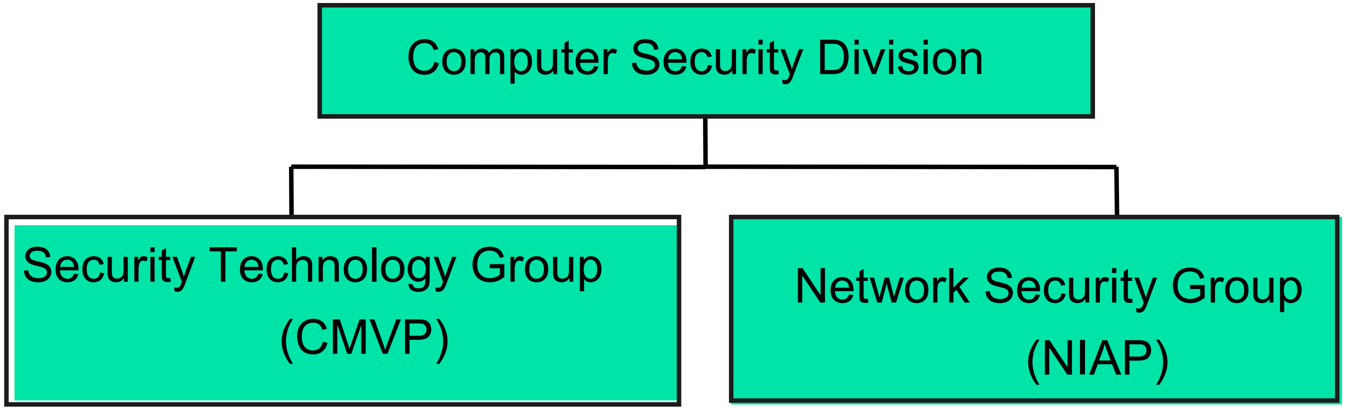
Computer Security Division

Security Technology Group

Network Security Group

Security Testing & Metrics*

Security Guidance



Computer Security Division

Security Technology Group (CMVP)

Network Security Group (NIAP)

Crypto Modules to Products

- Very difficult for User's to correlate list of crypto modules to vendor products
- Ideas?
  - Vendor Web Link
  - Product List by type
  - Different Vendor contact?

Participating Vendors

(March 2002)

Alcatel
Algorithmic Research, Ltd.
Ascom Hasler Mailing Systems
Attachmate Corp.
Avaya, Inc.
Baltimore Technologies (UK) Ltd.
Blue Ridge Networks
Certicom Corp.
Chrysalis-ITS Inc.
Cisco Systems, Inc.
Cryptek Security Communications, LLC
CTAM, Inc.
Cylink Corporation
Dallas Semiconductor, Inc.
Datakey, Inc.
Ensuredmail, Inc.
Entrust Technologies Limited
Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd.
F-Secure Corporation
Fortress Technologies
Francotyp-Postalia
GTE Internetworking
IBM
Intel Network Systems, Inc.
IRE, Inc.
Kasten Chase Applied Research
L-3 Communication Systems
Litronic, Inc.
M/A Com Wireless Systems
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.
Network Associates, Inc.
Nortel Networks
Novell, Inc.
Oracle Corporation
Pitney Bowes, Inc.
PrivyLink Pte Ltd
PSI Systems, Inc.
Rainbow Technologies
RedCreek Communications
Research In Motion
RSA Data Security, Inc.
SchlumbergerSema
Spyrus, Inc.
Stamps.com
Technical Communications Corp.
Thales e-Security
TimeStep Corporation
Transcrypt International
Tumbleweed Communications Corp.
V-ONE Corporation, Inc.

FIPS VALIDATED 140-1 ™

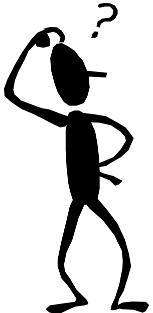
FIPS 140-1 Product Display

- Annabelle Lee - annabelle.lee@nist.gov
- Randy Easter - randall.easter@nist.gov
- Nelson Hastings - nelson.hastings@nist.gov
- Ray Snouffer - ray.snouffer@nist.gov

CMVP

Conformance through Testing

FIPS VALIDATED 140-2



NIST

National Institute of Standards and Technology

Technology Administration
U.S. Department of Commerce

http://www.nist.gov/cmvp

- FIPS 140-1 and FIPS 140-2
- Derived Test Requirements (DTR)
- Annexes to FIPS 140-2
- Implementation Guidance
- Points of Contact
- Laboratory Information
- Validated Modules List
- Special Publication 800-23