Cryptographic Module Validation Program

FCSM

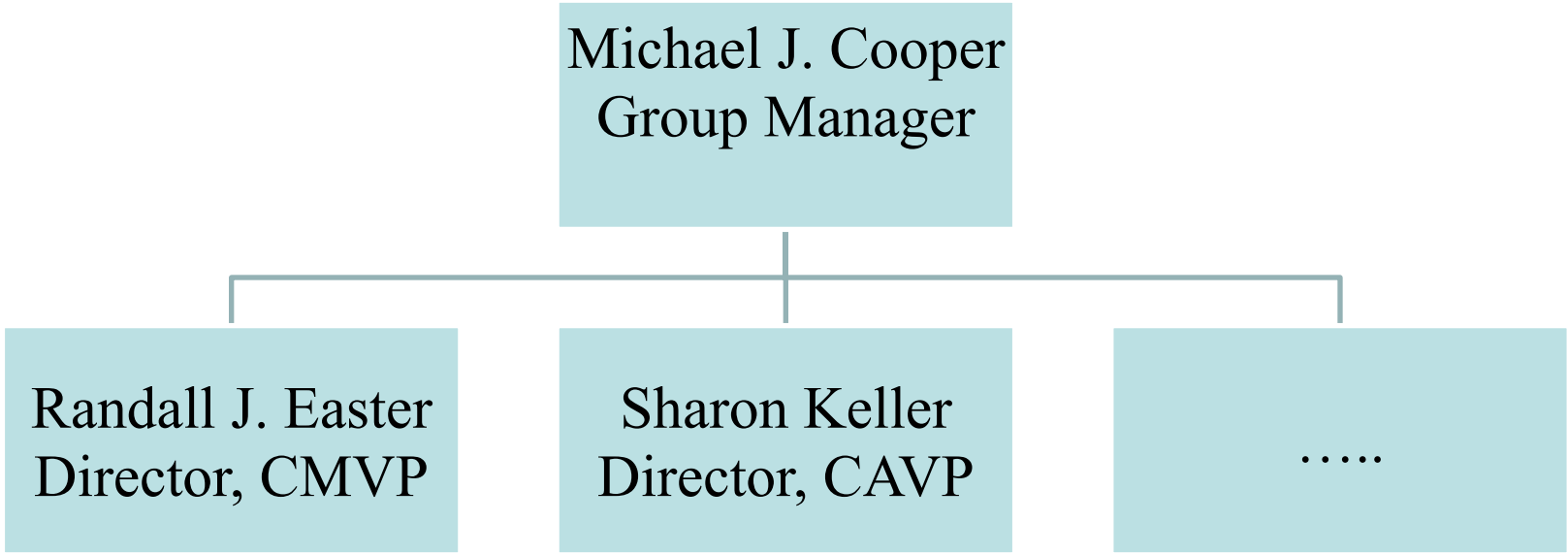
Kim B. Schaffer
NIST CMVP

June 13, 2012

NIST Information Technology Laboratory

Computer Security Division

Security Testing Validation and Metrics Group



Cryptographic Algorithm Validation Program (CAVP)

- Purpose: Provide assurance that cryptographic algorithm implementations conform to the specifications detailed in the associated cryptographic algorithm standards.
  - Approved Security Functions including Random Bit Generators and Key Establishment Methods found in FIPS 140-2 Annexes A, C and D
- Created as a separate program from CMVP in 2003
- The validation of cryptographic algorithm implementations is a prerequisite to the validation of cryptographic module

Cryptographic Module Validation Program (CMVP)

- Established by NIST and the Communications Security Establishment Canada (CSEC) in 1995
  - **FIPS 140-1** published Jan 1994
  - **FIPS 140-1 DTR** published Mar1995
  - **FIPS 140-2** published May 2001
  - **FIPS 140-2 DTR** published Nov 2001
- Original FIPS 140-1 requirements and updated FIPS 140-2 requirements developed with industry input
- Independent 3rd party conformance testing

International

- **International Standards Organization**
  - ISO/IEC 19790 *Security Requirements for Cryptographic Modules*
    - *Published March 2006*
  - ISO/IEC 24759 *Test requirements for cryptographic modules*
    - *Published July 2008*
  - ISO/IEC rev19790 *Security Requirements for Cryptographic Modules*
    - *Expected Publish 2012*

FIPS 140-2 and Applicability

- FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information.
- U.S. Federal organizations shall 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.

FIPS 140-2: Security Areas

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. EMI/EMC requirements
9. Self Tests
10. Design Assurance
11. Mitigation of Other Attacks

Appendix C – Security Policy

Annex A – Approved Security Functions

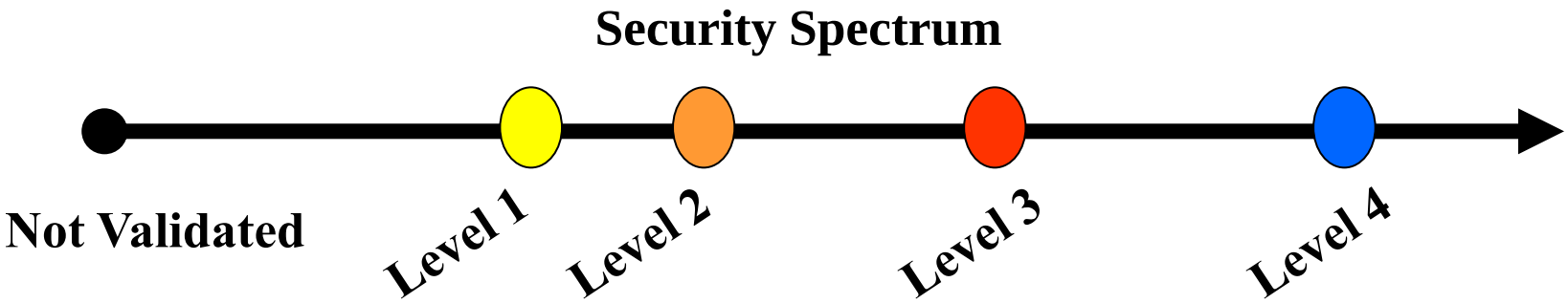
Annex B – Approved Protection Profiles

Annex C – Approved RNGs

Annex D – Approved Key Establishment

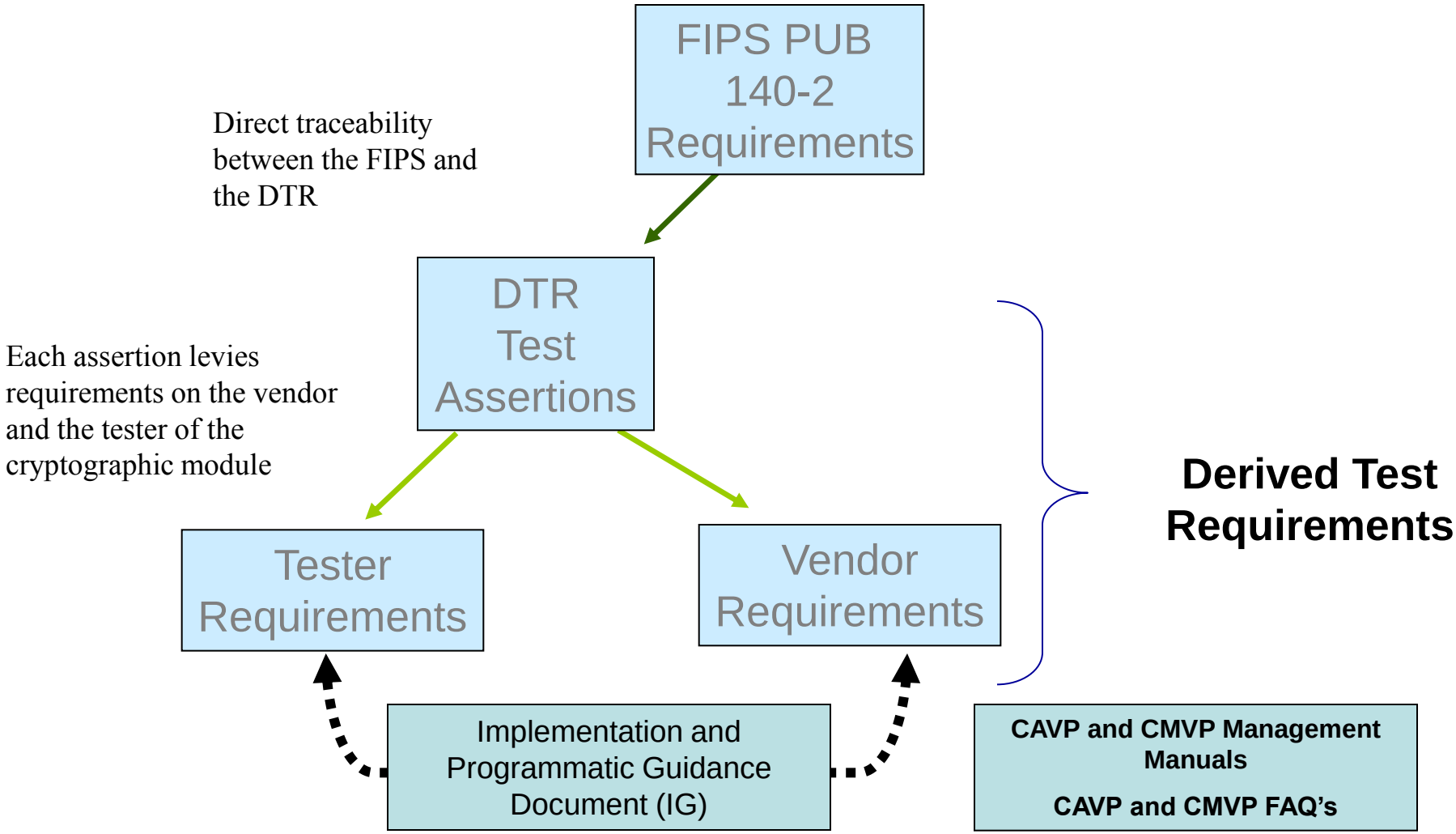
FIPS 140-2: Security Levels

How does the module protect Critical Security Parameters?



- Level 1 is the lowest, Level 4 most stringent
- Requirements are primarily cumulative by level
- Overall rating is lowest rating in all sections
- Validation is applicable when a module is configured and operated in accordance with the level to which it was tested and validated

The cryptography is not dependant on the security level


FIPS PUB 140-2 Requirements
Direct traceability between the FIPS and the DTR
DTR Test Assertions
Each assertion levies requirements on the vendor and the tester of the cryptographic module
Tester Requirements
Vendor Requirements
Derived Test Requirements
Implementation and Programmatic Guidance Document (IG)
CAVP and CMVP Management Manuals
CAVP and CMVP FAQ's

CMVP Testing: Process

- CMVP
  - Conformance testing of cryptographic modules using the Derived Test Requirements (DTR) and Implementation Guidance (IG)
  - Not evaluation of cryptographic modules. Not required are:
    - Vulnerability assessment
    - Design analysis, etc.
- Laboratories
  - Test submitted cryptographic modules
- NIST/CSEC
  - Validate test results and post module validation information

NVLAP Accredited FIPS 140-2 CST Lab

Vendor selects a lab;
Submits module for testing;
Module IUT

Cryptographic Module Vendor

Lab submits questions for guidance and clarification

Test for conformance to FIPS 140-2

Module Certificate (Web Entry)

Testing and Implementation Guidance

Testing and Report Generation

CMVP performs Continuous Quality and Competency Review

Module Test Report to CMVP for review

CMVP

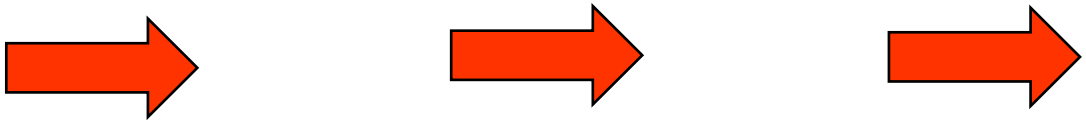
Module Validation

List of Validated FIPS 140-2 Modules

Module validation entries at www.nist.gov/cmvp

CMVP Testing and Validation Flow

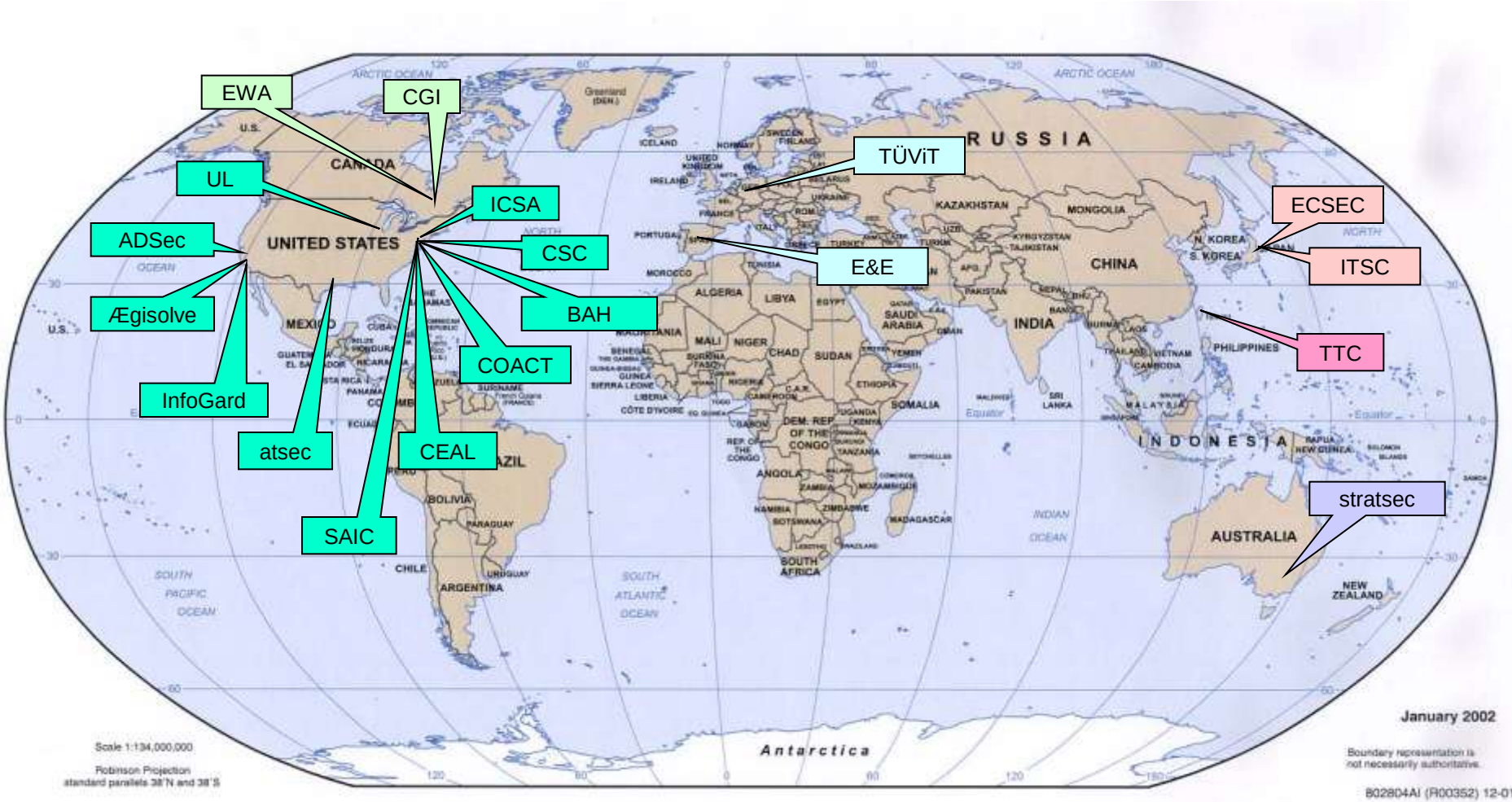
Vendor	CST Lab	CMVP NIST and CSEC	User
Designs and Produces Hardware • Software • Firmware	***Tests for Conformance*** Derived Test Requirements	***Validates***	***Specifies and Purchases***
Define Boundary **Define Approved Mode of Operation** **Security Policy**	**Algorithm Testing** **Documentation Review** **Source Code Review** **Operational and Physical Testing**	**Review Test Results** **Ongoing NVLAP Assessment** **Issue Certificates** **NIST Cost Recovery Fee**	**Security and Assurance** **Applications or products with embedded modules**



Cryptographic and Security Testing (CST) Laboratories

- Eighteen NVLAP-accredited testing laboratories
  - True independent 3rd party accredited testing laboratories
  - Cannot test and also provide design assistance for the same module
  - US, Canada, Germany, Spain, Japan, Taiwan and Australia
    - Additional domestic and international labs in FY11

CST Accredited Laboratories



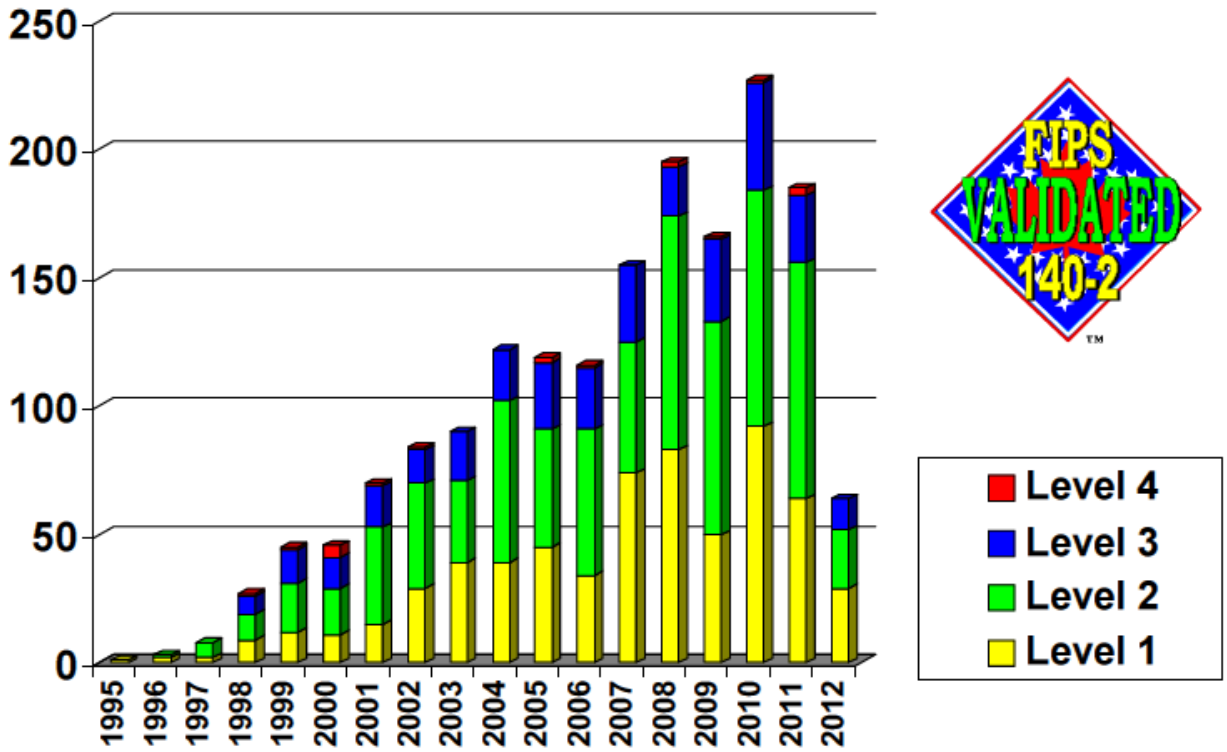
Status

June 4, 2012

- Continued growth in the number of cryptographic modules validated for conformance to FIPS 140-1 or FIPS 140-2
  - 1724 Validations representing over 3844 modules
- All four security levels represented on the Validated Modules List
- 427 validated modules vendors

FIPS 140-1 and FIPS 140-2 Validation Certificates by Year and Level

(May 31 2012)



1724	Hughes Network Systems, LLC. 11717 Exploration Lane Germantown, MD 20876 USA -Tim Young TEL: 301-428-1632 CST Lab: NVLAP 200492-0	Hughes SPACEWAY Crypto Kernel (Firmware Version: 1.0) Validated to FIPS 140-2 Security Policy Consolidated Validation Certificate	Firmware	05/23/2012	*Overall Level:* 1 -Tested: ST HN9500 with VxWorks 5.4; AGW2 with VxWorks 5.4; AGW5 with VxWorks 5.4 *-FIPS-approved algorithms:* AES (Cert. #1788); DRBG (Cert. #126); HMAC (Cert. #1053); SHS (Cert. #1570) *-Other algorithms:* Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength); MD5 Multi-chip standalone "The HSCK v1.0 is a firmware library that provides cryptographic functionality for securing communications over the Hughes SPACEWAY Satellite communication systems. SPACEWAY enables a full-mesh digital network that interconnects with a wide range of end-user equipment and systems."

Security Policy

- Description of Module
- Instructions for Setup
- Listing of Services for Each Role
- Listing of Cryptographic Algorithms and CSPs
- Zeroization Process
- Versioning
- Updated as needed by Vendor

Assurance … Making a Difference

- **Cryptographic Modules Surveyed (during testing)**
  - **Contained at least one non-conformance**
    - 59% Level 1 and Level 2 Modules
    - 65% Level 3 and Level 4 Modules
  - 96.3% FIPS Interpretation and Documentation Errors
  - ~10% Algorithm Implementation Errors
- **Areas of Greatest Difficulty**
  - Key Management
  - Physical Security
  - Self Tests
  - Random Number Generation

Points of Contact

NIST

- **Randall J. Easter** – Director, CMVP, NIST
  reaster@nist.gov

- **Sharon Keller** – Director, CAVP, NIST
  skeller@nist.gov

CSEC

- **Carolyn French** – Technical Authority, CMVP, CSEC
  carolyn.french@CSE-CST.GC.CA