Corsec®

# Understanding FIPS 140-2 Validation

John Morris

jmorris@corsec.com

23rd NISS Conference

October, 2000

# Outline

- What is FIPS 140-2
- FIPS 140-2 Applicability
- Process, Players, Testing
- What's in FIPS 140-2
- How do I use it/Choose it

# Who made this “FIPS”?

- U.S. Department of Commerce
  - Responsibility for improving utilization & management of computer systems in the Federal government
  - National Institute of Standards and Technology
  - NIST Information Technology Laboratory
  - Development of standards and guidelines
  - Publishes FIPS.

Corsec®

# FIPS PUBs

- Federal Information Processing Standard Publication
  - Apply to all sensitive, but unclassified (SBU) U.S. Federal Government computer systems.
  - Requests for Proposals (RFPs) often explicitly refer to FIPS.
  - Vendor challenges may add FIPS to RFPS
- FIPS PUB ###-#
  - Major number - version

# FIPS PUB 140-2

- Security Requirements for Cryptographic Modules
- Supersedes FIPS PUB 140-1
- Expected signature in September 2000
  - One year transition period
- Read as “Phips one forty dash two”
  - Differentiate from FIPS 140-1 and FIPS 140

# History of FIPS 140-2

- 1982 -- FIPS PUB 140 (FS 1027)
  - Hardware
- 1994  -- Federal Information Processing Standards Publication 140-1
  - (FIPS PUB 140-1), (FIPS 140-1)
  - Security requirements for cryptographic modules
- 2000 -- FIPS 140-2 (1-year rollover)

# FIPS 140-2 Applicability

- Applies to all Hardware *and* Software that contains cryptography
- Applies to every SBU purchase by the U.S. Federal Government
- Joint standard with Canadian Government
  - Communications Security Establishment (CSE)
  - Both U.S. and Canada accept FIPS 140-2 validated modules

# FIPS 140-2 Applicability (Contd)

- Financial Services Community
  - American National Standards Institute (ANSI)
  - ANSI adoption in several standards
  - Draft ANSI X9.66 in X9F3
- USPS use of FIPS 140-1 for IBIP
- Identrust use of FIPS 140-1
- ABA, Columbian Banks, etc.
- Commercial & International interest

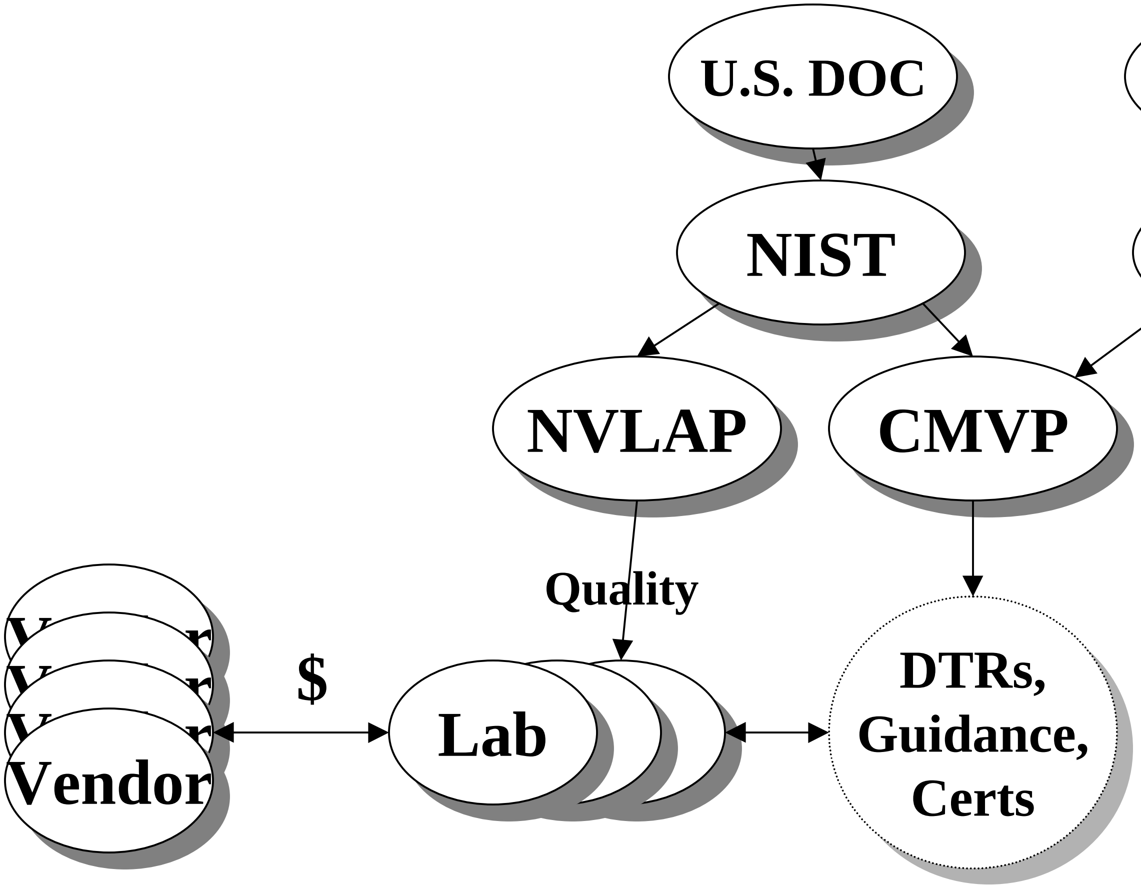
# More than just a standard

- Cryptographic Modules Validation Program (CMVP)
- Validated Modules List
  - http://csrc.nist.gov/cryptval/140-1/1401val.htm
- Derived Test Requirements
- Implementation Guidance
- Testing Laboratories
- Expert Consulting & Outsourcing

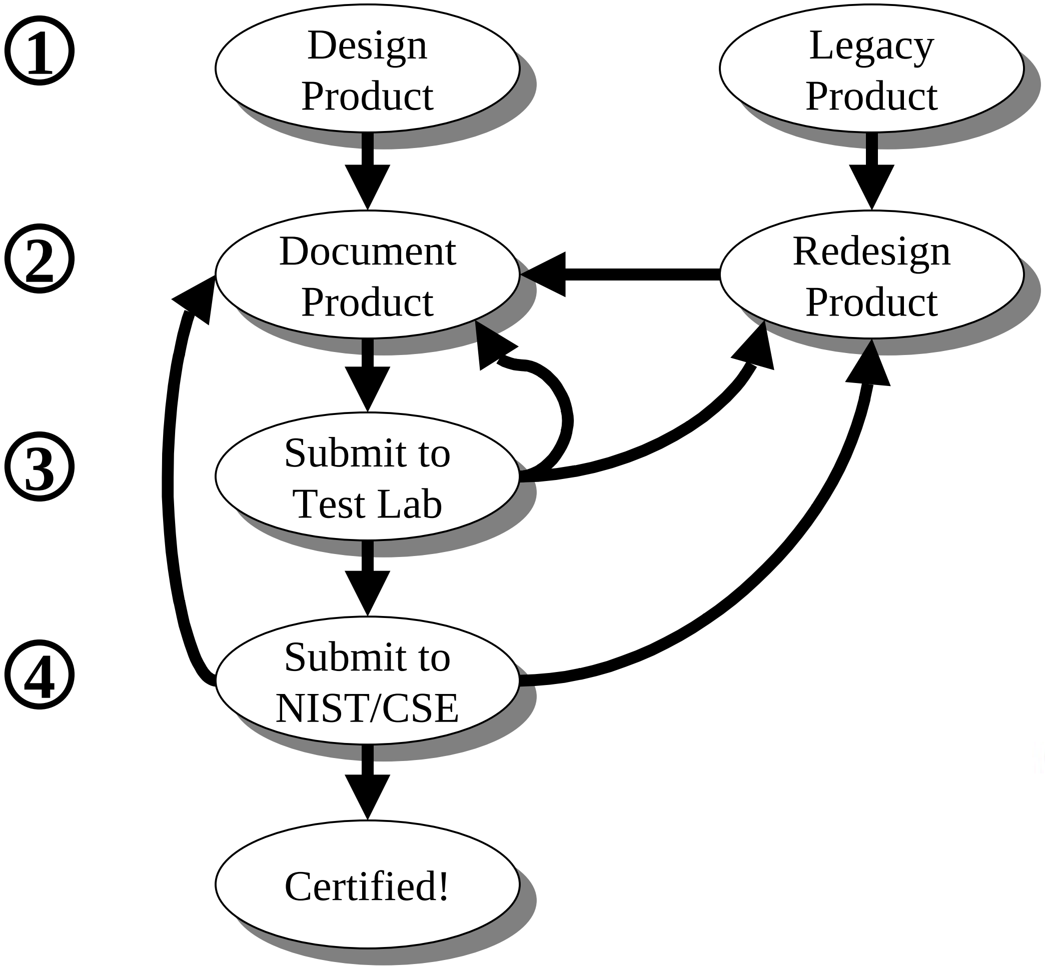
# FIPS 140-2 Testing

- NVLAP National Voluntary Laboratory Accreditation Program
- Four Accredited Laboratories
- Independent contracting with vendors
- NIST and CSE review of laboratory reports
- NIST and CSE issue validations

# FIPS 140-2 Players



# FIPS 140-2 Process



①

②

③

④

Design Product

Legacy Product

Document Product

Redesign Product

Submit to Test Lab

Submit to NIST/CSE

Certified!

Corsec®

# FIPS 140-2

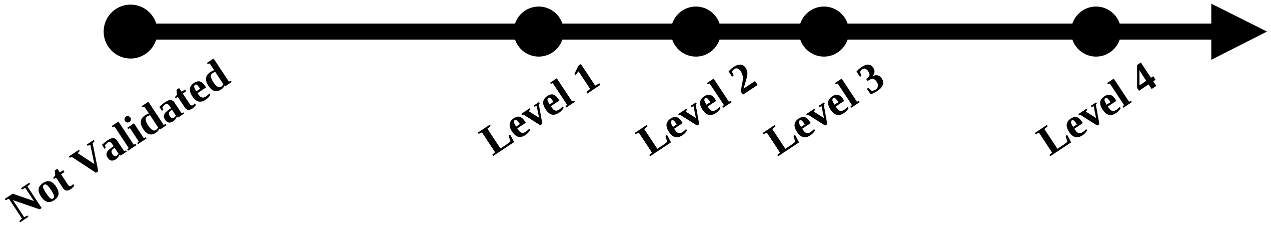
- Four levels of validation (1-4)
- Eleven categories of requirements
- Three physical module embodiments

**Cryptographic Modules**
**Module Interfaces**
**Roles and Services**
**FSM Model**
**Physical Security**
**Design Assurance**

**Operating System Security**
**Cryptographic Key Management**
**EMI/EMC**
**Self-Tests**
**Mitigation of**
**Other Attacks**

# Level What?

**FIPS 140-2 security spectrum**



- Level 1 through Level 4
  - Level 1 is the lowest, Level 4 most stringent
  - Requirements are mostly cumulative by level
  - Overall rating is lowest rating in each of eleven sections

# Level by Level

- Level 1
  - Philosophy:  Any production module can be successfully validated against these (reasonably difficult) security engineering requirements, including software on common platforms.
  - Cryptographic Module Specification
  - Finite State Machine Model
  - FIPS 140-2 Security Policy
  - Separation of Roles and Services

# Level by Level (Continued)

- Level 1 (Continued)
  - Production Grade Equipment
  - Interface Specification
  - Tested Algorithms
  - FCC tested business use
  - Configuration Management
  - Mitigation of other attacks

# Level by Level (Continued)

- Level 2
  - Philosophy: Modules generally in the control of the user. Role-based I&A and tamper evidence protect when not under user control
  - All level 1 requirements
  - Role-based authentication
  - Tamper evident cover or pick-resistant locks
  - EAL2 Trusted Operating System

# Level by Level (Continued)

- Level 3
  - Philosophy: Modules subject to hostile attack, and protect contents with hardened cover, I&A, and interfaces.
  - All Level 1 & Level 2 requirements
  - Hardened cover or tamper response
  - Critical information on separate physical ports
  - EAL3 Trusted Operating System & Trusted Path

# Level by Level (Continued)

- Level 4
  - Philosophy:   Highest level of validation, design rigor, and physical and logical protections
  - All Level 1, Level 2, Level 3 requirements
  - Tamper Protection Envelope and Tamper Response
  - Environmental Failure Protection/Testing

# Level by Level (Concluded)

- Level 4 (Contd.)
  - EAL4 Trusted Operating System
  - TOE Security Policy Modeling
  - Cover Channel Analysis
  - Modularity
  - Formal Methods and Proofs.

# How do I use it/Choose it

- FIPS 140-2 validation can be a yes/no requirement
  - The law requires it for Federal purchases
  - It’s nice to explain it in an RFP up-front
- Look at the validated module list
  - If it’s not on the list, it’s not validated
  - Some options are still limited
  - Don’t rule out desired solutions

Corsec®

# Using FIPS 140-2

- Choose a level to impose
  - Level 1+ or higher for general things & software clients
  - Level 2+ personal tokens, small value monetary
  - Level 3+ Certificate Authority, centralized infrastructure, larger value monetary
  - Level 4+ Specialized purposes
  - Lower level = lower cost, more choice but less validation and more risk

# FIPS 140-2 Changes

- Changes are evolutionary, not revolutionary
  - Mitigation of Other Attacks
    - Power Analysis (SPA, DPA)
    - Timing Analysis
    - Fault Induction
    - TEMPEST
  - Approved Algorithms
  - EAL2, 3, 4 Operating Systems
    - CC, CAPP, or equivalent

# FIPS 140-2 Changes (Continued)

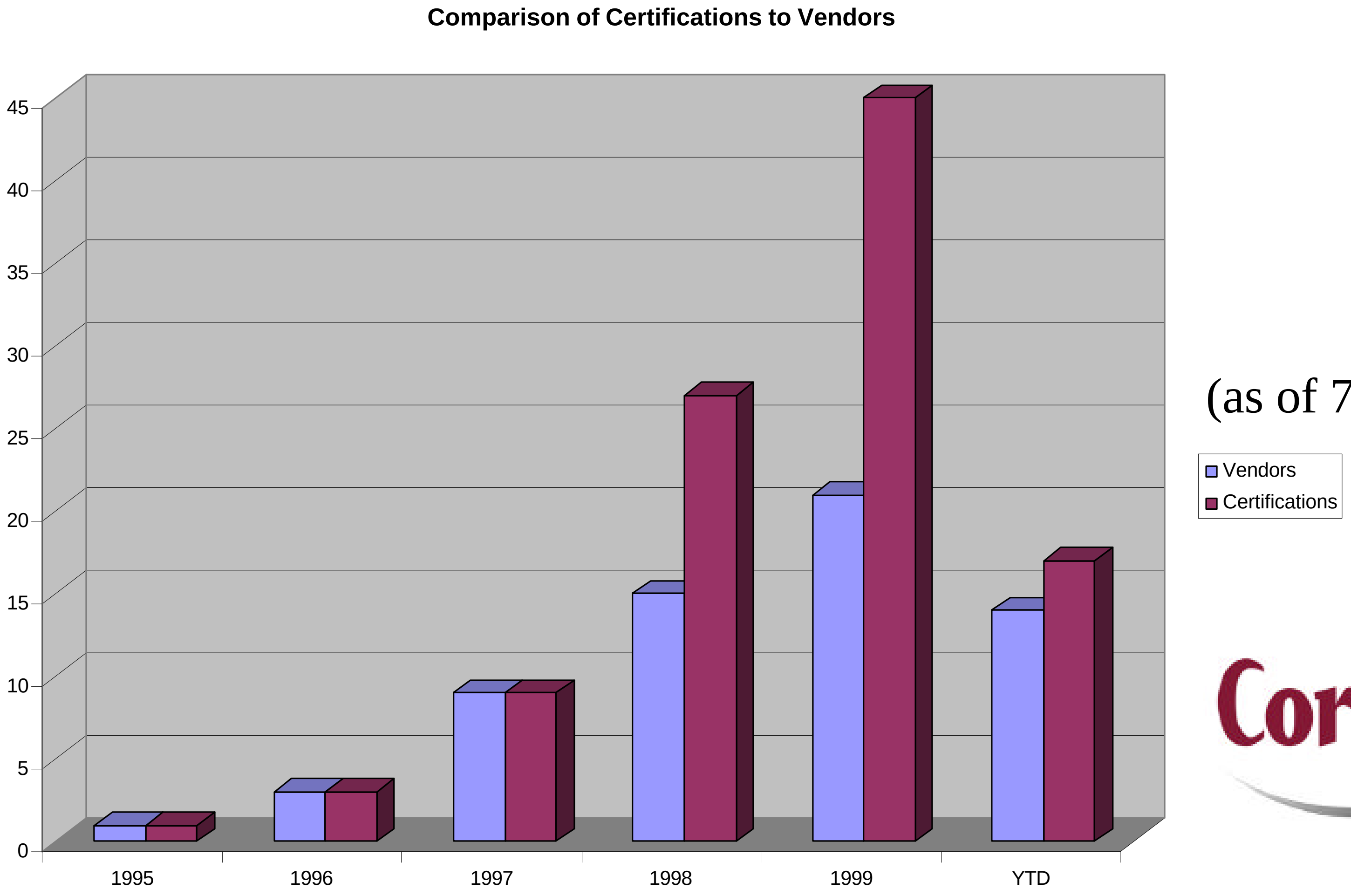
– Design Assurance (Software Security
  - Configuration Management
  - Secure Installation & Generation (level 1), Distribution (level 2)
  - Design & Policy Correspondence
  - Guidance Documents

– I&A Strength
  - One in a million chance
  - One in ten thousand per minute

# FIPS 140-2 Changes (Continued)

- Approved RNG/PRNG
  - tightened the range of Type I errors
- Functional Testing (level 2 and up)
  - (this has been removed from current draft)

# FIPS 140-1 Certifications



(as of 7/1/00)

Corsec®

# Responding to Vendor Concerns

## (Common objections to FIPS 140-2)

- It’s not a requirement.
  - Sorry, read the standard.  It’s required
- This is not a cryptographic module.
  - If it uses encryption, signing, or hashing, it is.
- It costs too much and it’s too slow.
  - For a robust product, it can be fast and cheap
  - Expert help is available -- use it to speed things up and reduce costs

# Responding to Vendor Concerns

(Common objections to FIPS 140-2)

- No one uses this standard.
  - The US, Canada, ABA, USPS, and major financial institutions of the world consider it critical
- Our product can’t pass this.
  - Perhaps you competitor can or already has
  - A well-designed product can pass, and even existing products can pass with small modifications

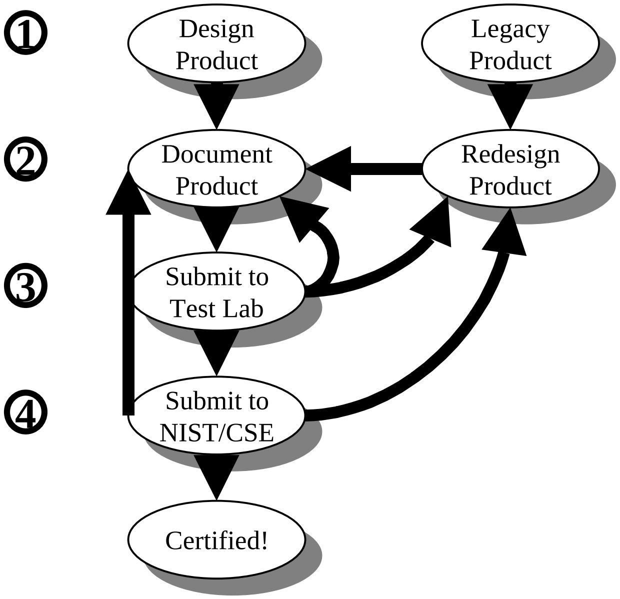
# Responding to Vendor Concerns

(Common objections to FIPS 140-2)

- It's too new
  - FIPS 140-1 was published in 1994
  - Last year over 50 products were certified
- FIPS 140-2 adds too many changes
  - Most changes are minor technically
  - Documentation changes are burdensome, but necessary

# Getting FIPS 140-2 Validation

- Step 0: Plan the Effort
- Step 1: Design or Re-design
- Step 2: Document
- Step 3: Testing
- Step 4: Government Review
- Proceed through the steps. Avoid jumping back in steps.



# Design for FIPS 140-2

- Meet lowest requirement for target level in all eleven areas
- Include FIPS 140-2 design requirements from earliest stage
- Have independent review against requirements
- Plan for updates and upgrades

# FIPS 140-2 Required Documentation

- Design Specification of hardware, software, and firmware
- Functional Specification
- Crypto Officer & User Guidance Documentation
- Finite State Machine (FSM)

# FIPS 140-2 Required Documentation

- Non-Proprietary FIPS 140-1 Security Policy
- Algorithm Certificates
- Vendor Evidence Document

# Contrast with Common Criteria

- NIAP (National Information Assurance Partnership)
- Mutual Recognition
  - Australia, Canada, France, Germany, New Zealand, UK, US
  - Replaces TCSEC, CTCPEC, ITSEC etc.
- Functional & Assurance Requirements
- ISO Standard 15408 v2

# Testing Laboratories

- NIAP:  NIST-NSA joint partnership
- NVLAP and NIAP Accredited laboratories
  - use strengths of FIPS 140-2 structure
- Evaluations Tailored
  - One set of Common Criteria
  - Industry/Class defined Protection Profiles
  - Individual Security Targets
  - Very Individual Target of Evaluation

# Evaluation Assurance Levels

- EAL 1 through EAL 7

**EAL1: Functionally tested**
**EAL2: Structurally tested**
**EAL3: Methodically tested, and checked**
**EAL4: Methodically designed, tested, and reviewed**
**EAL5: Semi-formally designed, and tested**
**EAL6: Semi-formally verified design, and tested**
**EAL7: Formally verified design, and tested**

# Functionality Classes

- Audit, Cryptographic Support
- Communications User Data Protection
- Identification and Authentication, Security Management, Privacy
- Protection of the TOE Security Functions, Resource Utilization TOE Access
- Trusted Path/Channels

# Assurance Classes

- Protection Profile & Security Target Eval.
- Configuration Management
- Delivery and Operation, Development
- Guidance Documents, Life Cycle Support
- Tests, Vulnerability Assessment
- Maintenance of Assurance

# CC Documentation (e.g)

– TOE, configuration management

– delivery documentation

– administrator guidance

– secure installation

– generation, and start-up procedures

– functional specification

– user guidance

– high level design

# CC Documentation (e.g)

– correspondence analysis between the TOE summary specification and the functional specification

– correspondence analysis between the functional specification and the high-level design

– vulnerability analysis

– development security documentation

– test documentation

– test coverage analysis

# CC Documentation (e.g)

- depth of testing analysis
- strength of function claims analysis
- current information regarding obvious vulnerabilities
- etc.

# FIPS and Common Criteria

- Different testing laboratories
- Different accrediting bodies
- Different foci for validation
- Different time and cost
- A lot of work to consolidate the two

# FIPS and Common Criteria

- Effort to define a Protection Profile that includes FIPS 140-2
- Possibility of labs internationally joining NVLAP program
- Evaluation to include FIPS requirements
- Certification for FIPS 140-2 included as a subset of an CC evaluation
  - (algorithms and FCC certification is now a subset of FIPS 140-2 validation)

# Questions?

- For More Information
- FIPS 140-2 FAQ (http://www.fips140-2.com/Body/resourceSET.html)
- NIST/CSE (http://csrc.nist.gov/cryptval/)
- Corsec Security:
  - www.corsec.com

Corsec®