The CMVP: Past, Present, and Future

Miles Smid

Orion Security Solutions

September 14, 2004

The Past

1965 - May 24, 2001

The beginnings

- Brooks act (PL89-306) required new standards for improving the utilization of computers by the Federal Government (1965)
- NBS assess the need for Computer Security within the Federal Government (1968)
- NBS ICST saw need for Data Encryption Standard (DES) for protection of computer data (1972)
- DES standard published (January 1977)

DES Validations

- Required by NIST Director
- Performed by NIST
- Certificates of conformance
- Trust but verify
- DES: 269 FIPS 140-3 Certificates (since October 25, 1999)
- TDES: 273 Certificates

FS 1027

General Security Requirements for Equipment using the Data Encryption Standard

- Issued by GSA
- Endorsements by NSA
- Limited Flexibility
  - DES only
  - Hardware only
  - Manual or KOI-18 key entry
- Limited number of products endorsed
- FS 1027 transferred to NIST where it became FIPS 140

Rethinking the process

- Raise the security bar without excessive costs
  - Design costs
  - Evaluation costs
  - Engineering costs
  - Documentation costs
  - Validation costs
  - Time to market costs

- Government and Industry working together
- Specific requirements
- Validation cost under $50K
- Validation time under 6 months
- Privatization

The Making of FIPS 140-1

- Multiple encryption algorithms
- Wireless radio modules
- Smart Cards for key loading, etc.
- Twelve Security Areas
- Security levels and physical embodiments to cover span on applications
- Software cryptography allowed but required to meet requirements equivalent to hardware
- Allows cryptographically authenticated loading of approved software

The CMVP

- Needed program to manage testing laboratories
- National Voluntary Laboratory Accreditation Program (NVLAP)
- NIST and CSE Cooperation and mutual recognition
- Started with three laboratories and few participating vendors

Success of FIPS 140-1

- Slowly recognized as the standard for cryptographic modules
- Excellent cooperation between NIST and CSE
- Implemented by major vendors
- First DOD uses
- 300+ certificates of validation

The Present

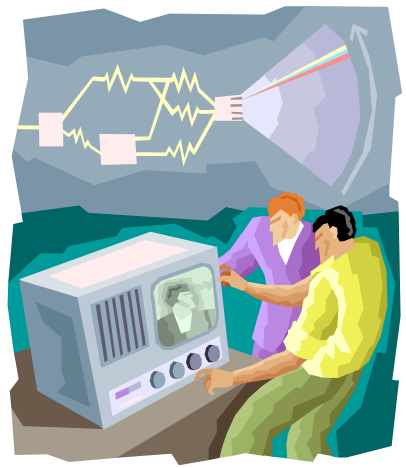
May 25, 2001- September 14, 2004

FIPS 140-2

- Revised and improved FIPS 140-1
- Generally kept the essence of FIPS 140-1
- Some additions (See NIST paper)
  - Strength of authentication
  - Configuration Management
  - Delivery and operation
- Physical Security not required for software

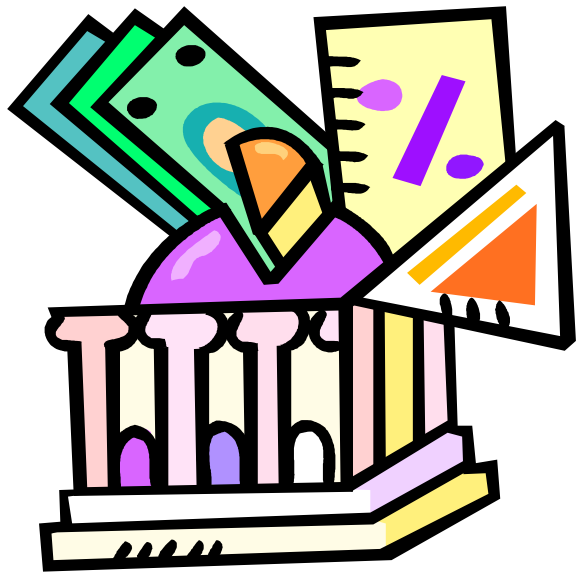
CMVP Today

- FIPS 140-2 recognized throughout the U.S. Federal Government, Canada, and UK
- Nine laboratories in three countries
- Software, hardware, firmware
- 457 validation certificates
- 120 vendors
- Increasing to perhaps 100 certificates this year!



FIPS 140-2 Recognized for financial Applications

- On ACS X9 Registry of approved standards and techniques
  - Registry item 00001, Security Requirements for Cryptographic Modules, 2004/05/03

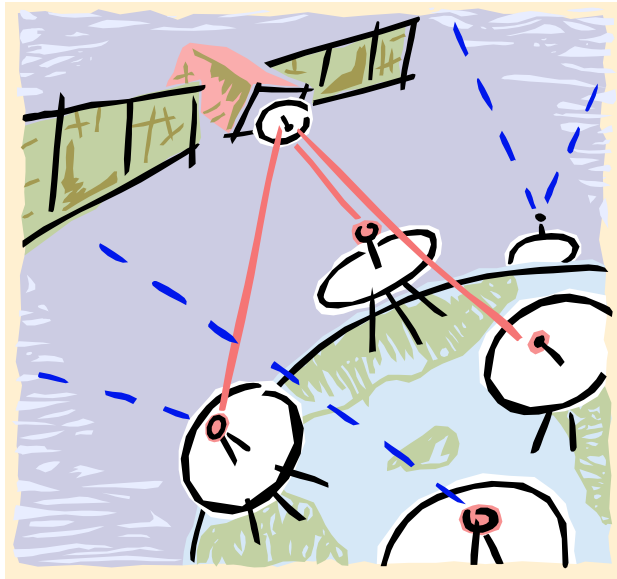


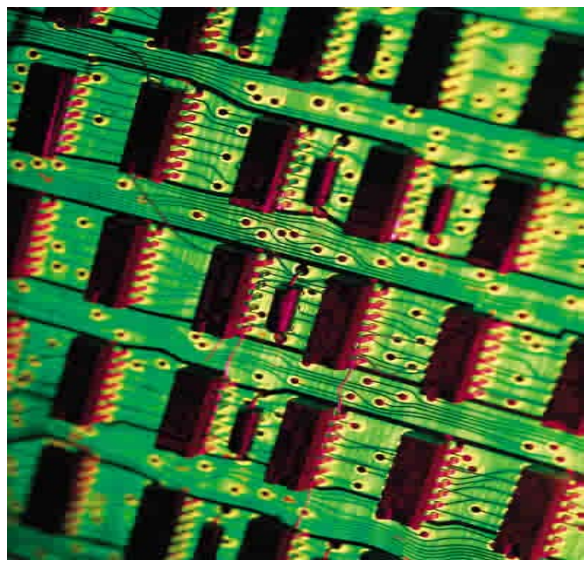
The Future

September 15, 2004 - ???

FIPS 140-3

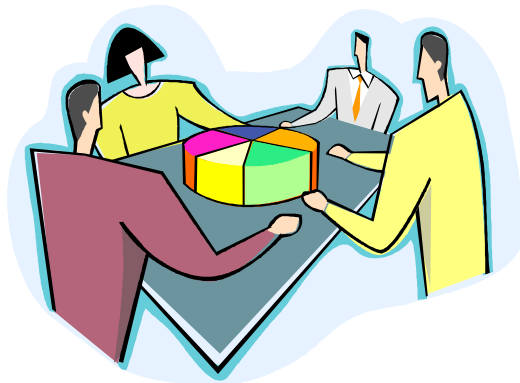
- Beginning to approach 5-year review
- Remote Operations
- Conformance to Random Bit Generation (DANS X9.82)
  - Deterministic & Non-Deterministic methods
  - Seed generation
  - Entropy Source
  - RNG self-tests





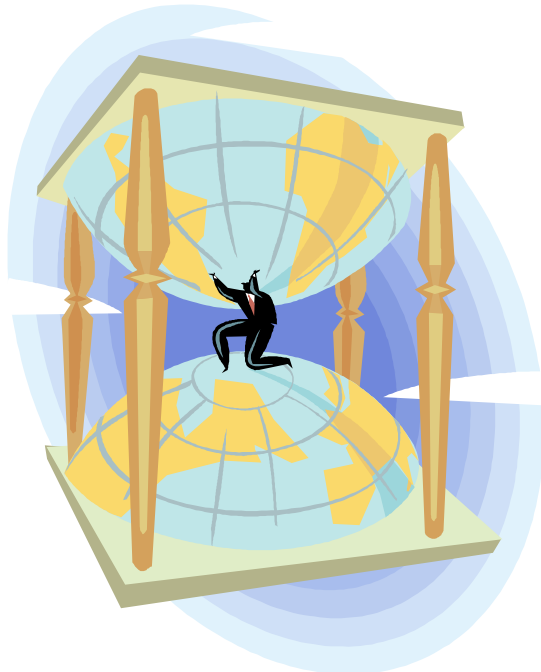
FIPS 140-3 continued

- Key Establishment Schemes (DSP 800-56)
  - Multiple schemes
  - Assurance of key and domain parameter validity
  - Assurance of possession
  - Key derivation
- Key Management Guidance (DSP 800-57)
  - New restrictions
  - New techniques
- Protocols?
- Continue to consider vendor, laboratory, and public input

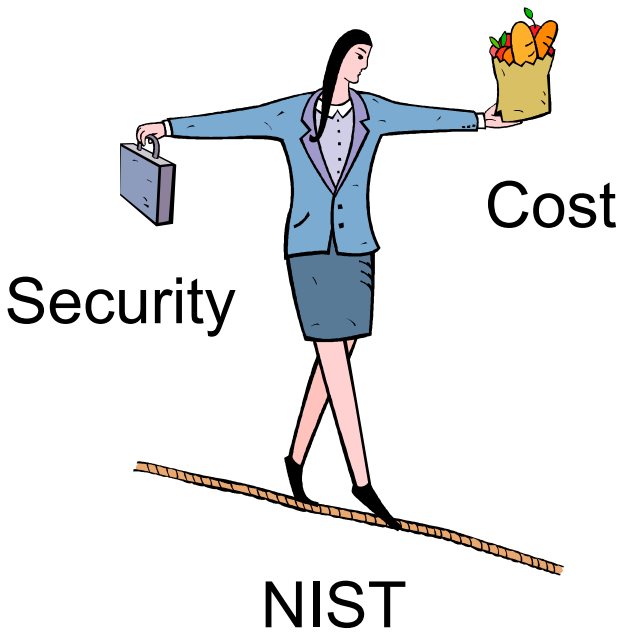


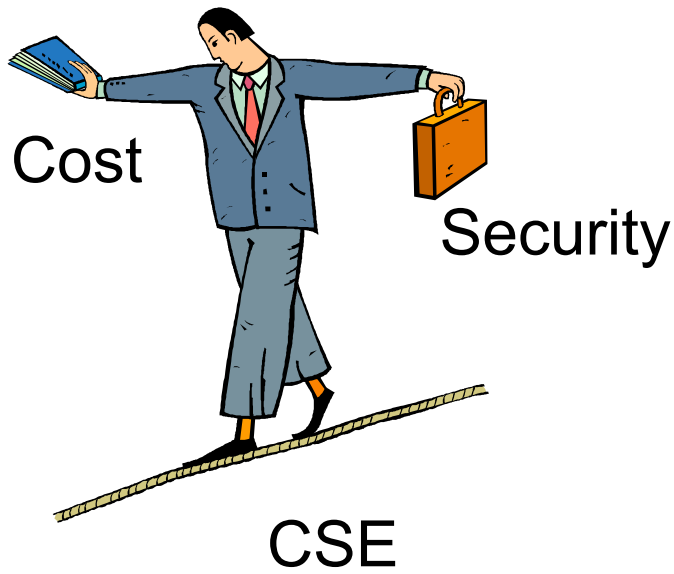
Related International Standard

- ISO CD19790: IT Security Techniques – Security Requirements for Cryptographic Modules
- Multi-national recognition of principles
- Mutual recognition?



Keep the proper balance





We've come a long way, but there is still further to go!

Raise the security bar without excessive costs

Questions?