National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Looking over the horizon: FIPS 140-3

Jean Campbell

Communications Security Establishment

CMVP Symposium 2004

15 September 2004

Presentation Outline

- History of FIPS 140
- Motivation for change
- Areas of change
- Milestones
- Previous validations

History of FIPS 140

- Federal Standard 1027
  - General Security Requirements for Equipment using DES
- FIPS 140
- FIPS 140-1 (11 January 1994)
  - Security Requirements for Cryptographic Modules
- FIPS 140-2 (25 May 2001)
  - Security Requirements for Cryptographic Modules

History of FIPS 140

- Federal Standard 1027
- FIPS 140
- FIPS 140-1
- FIPS 140-2

General Security Requirements for Equipment using DES

- Very hardware oriented
- Restrictive

History of FIPS 140

Federal Standard 1027

FIPS 140

FIPS 140-1

FIPS 140-2

Security Requirements for Cryptographic Modules

- Cover change for the FED STD 1027

History of FIPS 140

Federal Standard 1027

FIPS 140

FIPS 140-1

FIPS 140-2

Security Requirements for Cryptographic Modules

- Starts at giving flexibility to the vendors
- Still hardware oriented
- Start at recognizing software modules
- "Creativity" was used for software modules

History of FIPS 140

Federal Standard 1027

FIPS 140

FIPS 140-1

FIPS 140-2

Security Requirements for Cryptographic Modules

- Re-organized FIPS 140-1
- Clarified some requirements
- Incorporation of refinements contained in Implementation Guidance
- Introduction of Design Assurance

Motivation for Change

- U.S. Federal Requirement
  - Must be reviewed every 5 years
- Tremendous technology advances
  - Standard is becoming out of date
  - Difficult to generically apply to new technologies
- Protection for more sensitive information
- Requirement improvements and strengthening
- Refinements and corrections

Possible Areas of Change

(Subject to change)

- FIPS mode of operation
- Software cryptographic modules
  - cryptographic boundary; environment interactions
- Roles and services, authentication
- Cryptographic key life cycle
  - key establishment; input/output; distribution
  - random number generator requirements

Possible Areas of Change

(Subject to change)

- Physical security
- Self-tests
  - Power-up, module integrity checks
  - Conditional tests
  - Error handling
- Security policy
  - Realign with what users need

Milestones

	Start Date	Length
• Public Comment on FIPS 140-2 – Federal Registry Notice	Jan 05	3 months
• CMVP Prepares Draft #1 FIPS 140-3 – Use received comments – Incorporate new requirements	Apr 05	4 months
• Public Comment on Draft #1 FIPS 140-3 – Preparation of DTR FIPS 140-3	Oct 05	3 months

WWW.NIST.GOV/CMVP

Milestones

	Start Date	Length
• CMVP Prepares FIPS PUB 140-3	Jan 06	1 month
– Use received comments		
• FIPS 140-3 Approval process	Feb 06	3 months
• FIPS 140-3 Approved !	**May 06**	
• FIPS 140-3 in effect (+ 6 mo)	**Nov 06**	
• FIPS 140-2 retires	**May 07**	
• validations still effective		

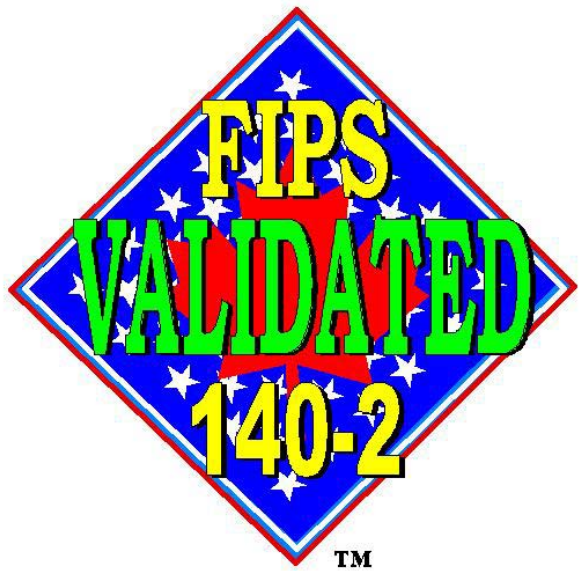
Concurrent Activities

- Implementation Guidance for FIPS 140-3 and Derived Test Requirements for FIPS 140-3 should be issued in parallel with for FIPS PUB 140-3

- New logo for for FIPS 140-3 !

Status of Previous Validations

- Validations to FIPS 140-1 and FIPS 140-2 will still be recognized
- Migration path from previous validation to FIPS 140-3 will be defined
  - similar to FIPS 140-1 to FIPS 140-2



Conclusion

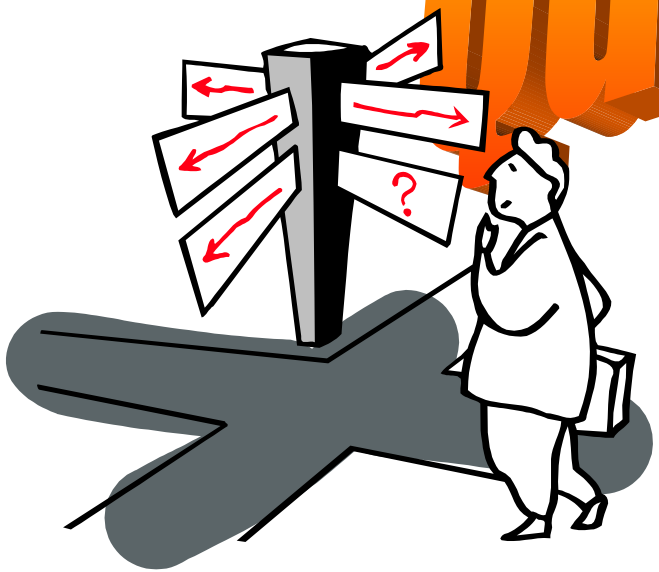
- FIPS 140-3 development has begun
- Public participation solicited
- Watch the CMVP website
  - WWW.NIST.GOV/CMVP

CMVP
Conformance through Testing

FIPS VALIDATED 140-2

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

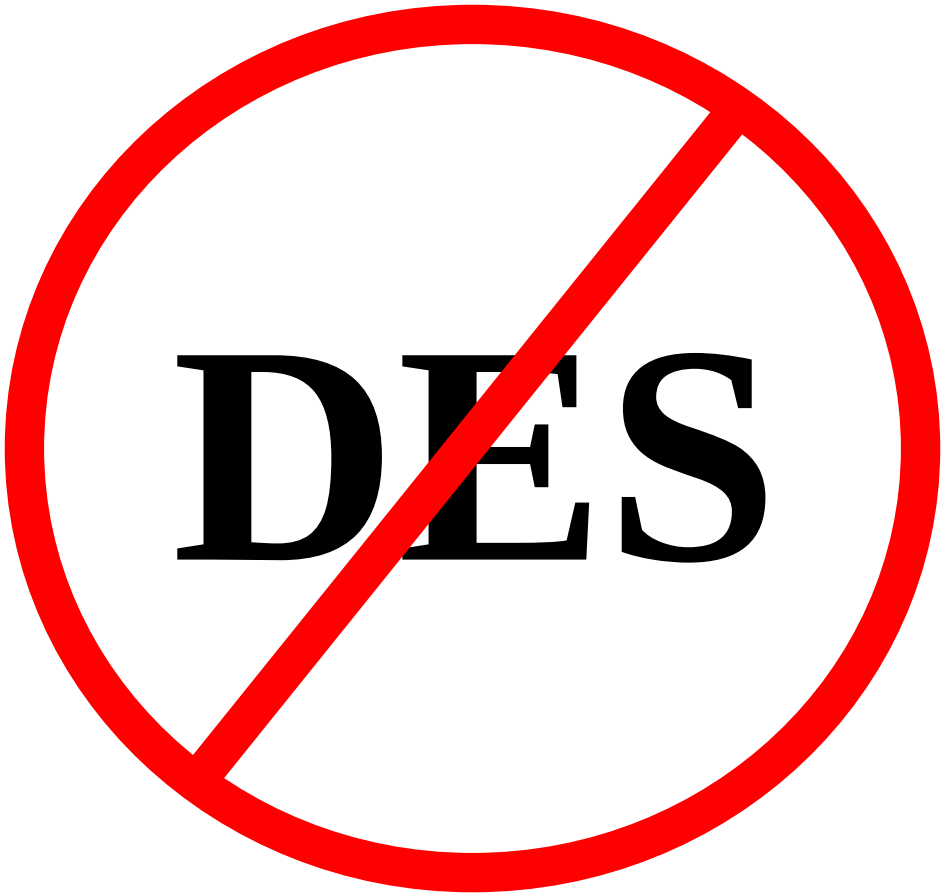
Questions



Jean Campbell
Communications Security Establishment
☎: (613) 991-8121
🖱: Jean.Campbell @cse-cst.gc.ca

Randall J. Easter
National Institute of Standards and Technology
☎: (301) 975-4641
🖱: Randall.Easter@nist.gov

WWW.NIST.GOV/CMVP


DES