NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
INFORMATION TECHNOLOGY LABORATORY
COMPUTER SECURITY DIVISION
SECURITY TESTING, VALIDATION, AND MEASUREMENT

MICHAEL COOPER – MANAGER STVM

May 8, 2019

TESTING GROUP MISSION

Advance information security testing, measurement science, and conformance.

STVM's testing-focused activities include validating cryptographic algorithm implementations, cryptographic modules, and Security Content Automation Protocol (SCAP)-compliant products; developing test suites and test methods; providing implementation guidance and technical support to industry forums; and conducting education, training, and outreach programs.

PROGRAMS IN STVM

- CAVP – Cryptographic Algorithm Validation Program
- CMVP – Cryptographic Module Validation Program
- SCAP – Security Content Automation Protocol Validation Program
- PIV – Personal Identity Verification Validation Program

- NVD – National Vulnerability Database
- NCP – National Checklist Program
- USGCB – US Government Configuration Baseline
- Metrics Research – shared with the math division

TESTING PROGRAMS: CAVP

- Tests each individual algorithm implementation against the associated standard.
- Test tool – Crypto Algorithm Validation System (CAVS)
  - ACVP – New Protocol developed to automate algorithm Testing

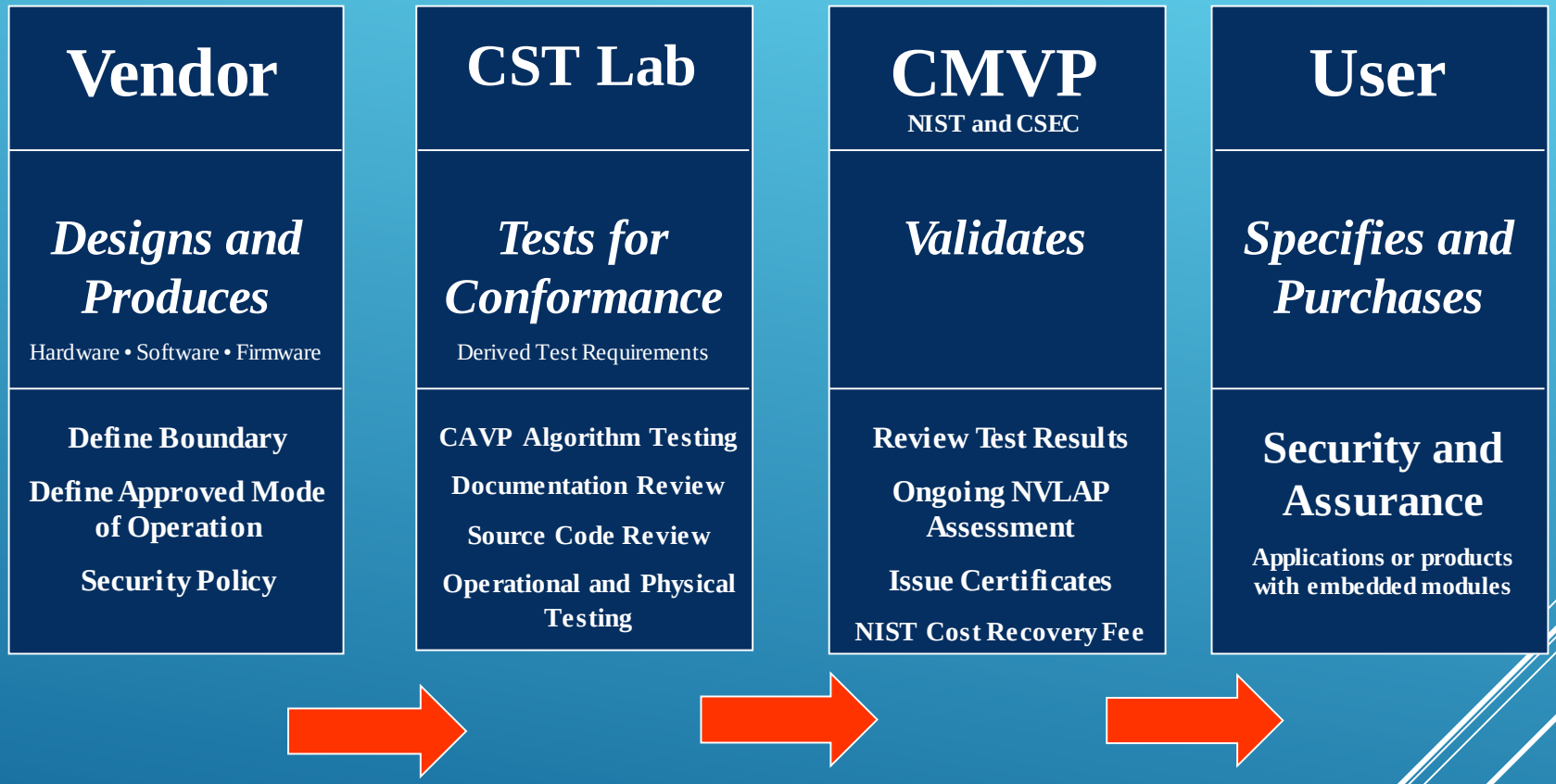
TESTING PROGRAMS: CMVP

- Vendors of cryptographic modules use independent, accredited Cryptographic and Security Testing (CST) laboratories to test their modules.
- CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against FIPS 140-2.
- NIST's Computer Security Division (CSD) and CSEC jointly serve as the Validation Authorities for the program, validating the test results and issuing certificates.

Some facts about FIPS-140

- FIPS 140-1 was issued on January 11, 1994
  - developed by a government and industry working group
  - NIST established the Cryptographic Module Validation Program
- FIPS 140-2 was issued on May 25, 2001
  - only very modest changes compared to predecessor
  - same year when AES became a standard
  - FISMA-2002 removed the statutory provision that allowed agencies to waive mandatory FIPS

CMVP Testing and Validation Flow



TESTING PROGRAMS: CMVP

TESTING PROGRAMS: CMVP

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

Section 4.5: Physical Security

Level 1: Production Grade Components

Level 2: Provide Evidence of an Attack
- Tamper evident seals
- Opacity

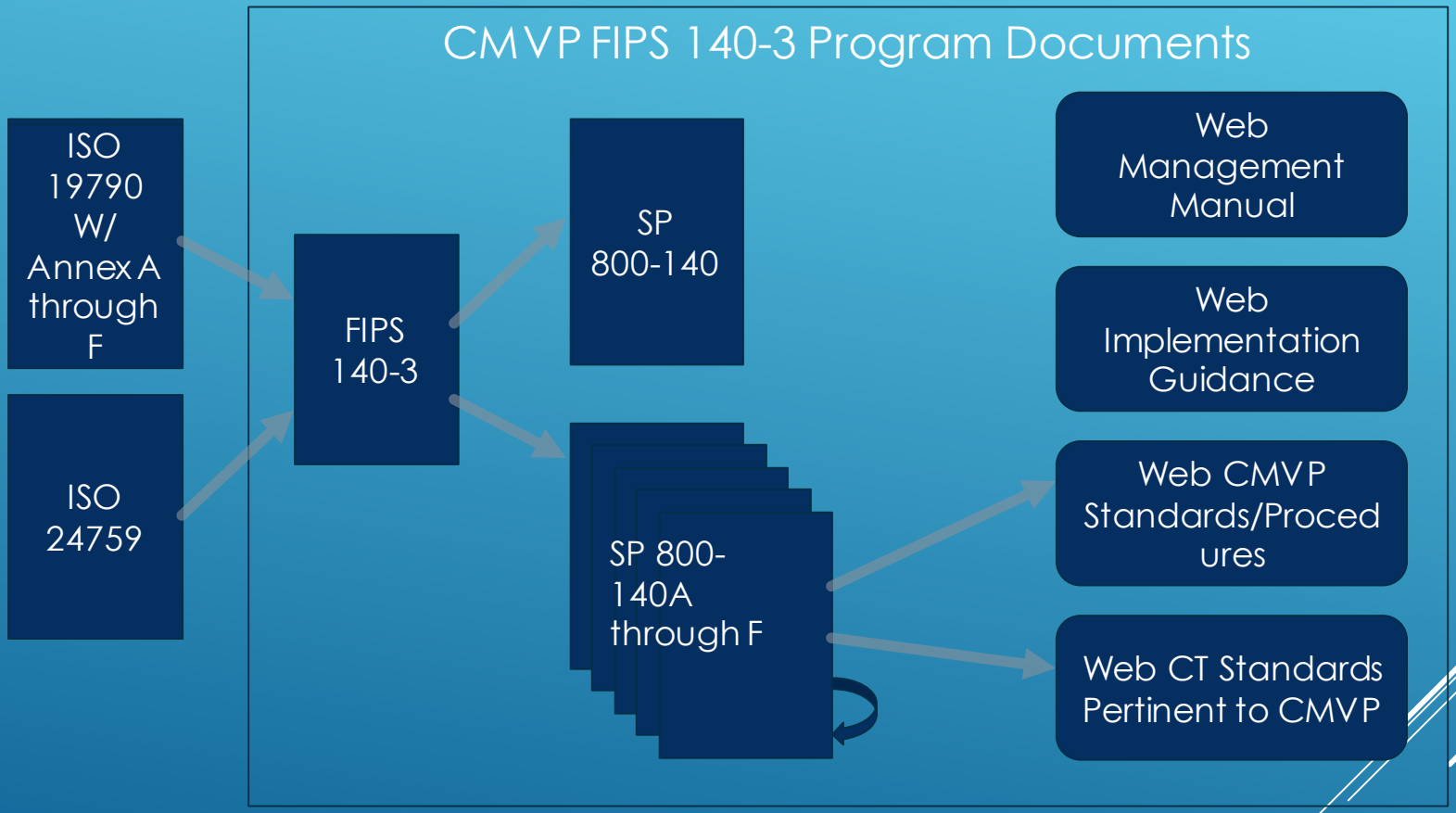
Level 3: Deterrence of Moderately Aggressive Attacks
- Strong enclosure or covered with hard coating or potting material
- Tamper response and zeroization for any doors or removable covers

Level 4: Deterrence of Aggressive Attacks
- Attacker assumed to have prior knowledge, specialized tools, unfettered access and no time restriction.
- Tamper Response and Zeroization Envelope
- Mitigation of Temperature and Voltage Attacks

TESTING PROGRAMS: CMVP

FIPS 140-3 SCHEDULE

- Signed Document FIPS 140-3 — March 22 2019
  - 800-140 A-F Publication
- FIPS 140-3 Effective Date — September 22 2019
- FIPS 140-3 Milestone — March 22 2020
  - Documents complete:
    - IG, Management, Validation Certs, Cryptic
    - Pearson Roadmap
    - Resolve Roadmap
  - Test Labs begin preparations
- FIPS 140-3 Testing Starts — September 22, 2020
- FIPS 140-2 Validation Submission Ends — September 22, 2021
- FIPS 140-2 Certifications End? — September 22, 2026


CMVP FIPS 140-3 Program Documents
ISO 19790 W/ Annex A through F
ISO 24759
FIPS 140-3
SP 800-140
SP 800-140A through F
Web Management Manual
Web Implementation Guidance
Web CMVP Standards/Procedures
Web CT Standards Pertinent to CMVP

ISO/IEC 19790:2012(E)

- Purpose is:
  - Security requirements for cryptographic modules
  - Annexes define requirements and modifiable by validation authority
- Current ISO version is ISO/IEC 19790:2012/Cor.1:2015(E)
  - Is referred to as ISO/IEC 19790:2012(E) so that changes will not have to be made when ISO is updated unless specifically needed.

ISO/IEC ISO/IEC 24759:2017(E)

- Purpose is:
  - Test requirements for cryptographic modules
  - Specifies testing (TE) and vendor evidence (VE)
- Current ISO version is ISO/IEC 24759:2014/Cor.1.2015(E)
  - Is referred to as ISO/IEC 24759:2017(E) so that changes will not have to be made when ISO is updated unless specifically needed.

FIPS 140-3

- Purpose is:
  - Confirms US decision to use ISO/IEC 19790:2012(E) to replace FIPS 140-2
  - Defines basis for CMVP validation program
- Declares SP 800-140 series as requirements for validation program
  - Clarify/Replace ISO/IEC 19790:2012(E) Annexes with SP 800-140A through F
  - Identify SP 800-140 as the validation authority requirements, supplementing ISO/IEC 24759:2017(E)

SP 800-140

- Identify validation authority changes (addition/modification/deletion) to the vendor evidence (VE) and testing (TE) necessary to meet the requirements in ISO/IEC 19790:2012(E)
- Introduce additional language necessary to support program specific implementation

SP 800-140C APPROVED SECURITY FUNCTIONS

- Replaces ISO/IEC 19790:2012(E) Annex C requirements
- Can change any additional requirements in ISO/IEC 24759:2017(E) 6.15
- Draft should point to CT administered website for requirements

IMPLEMENTATION GUIDANCE

- Updated and possibly split from 140-2 to address 140-3 issues
- Transition to web-based document
- Under control of CMVP at www.nist.gov/cmvp
- Quick review is that many IGs will be removed from the 140-3 guidance
  - Quick review is 2 years ago.
  - Some to Management manual
  - Some overtaken by changes in 140-3

MANAGEMENT MANUAL

- Addresses how to do business with CMVP
- Moving to web-based
- Will be updated to address FIPS 140-3 relevant issues
- Under control of CMVP at www.nist.gov/cmvp

OTHER EFFORTS

- Lab Preparation
  - Cryptic replacement
  - Training
  - Testing
- Resolve
  - Continue 140-2 for 6+ years
  - Introduce 140-3 in 1 year
- User Awareness Briefing