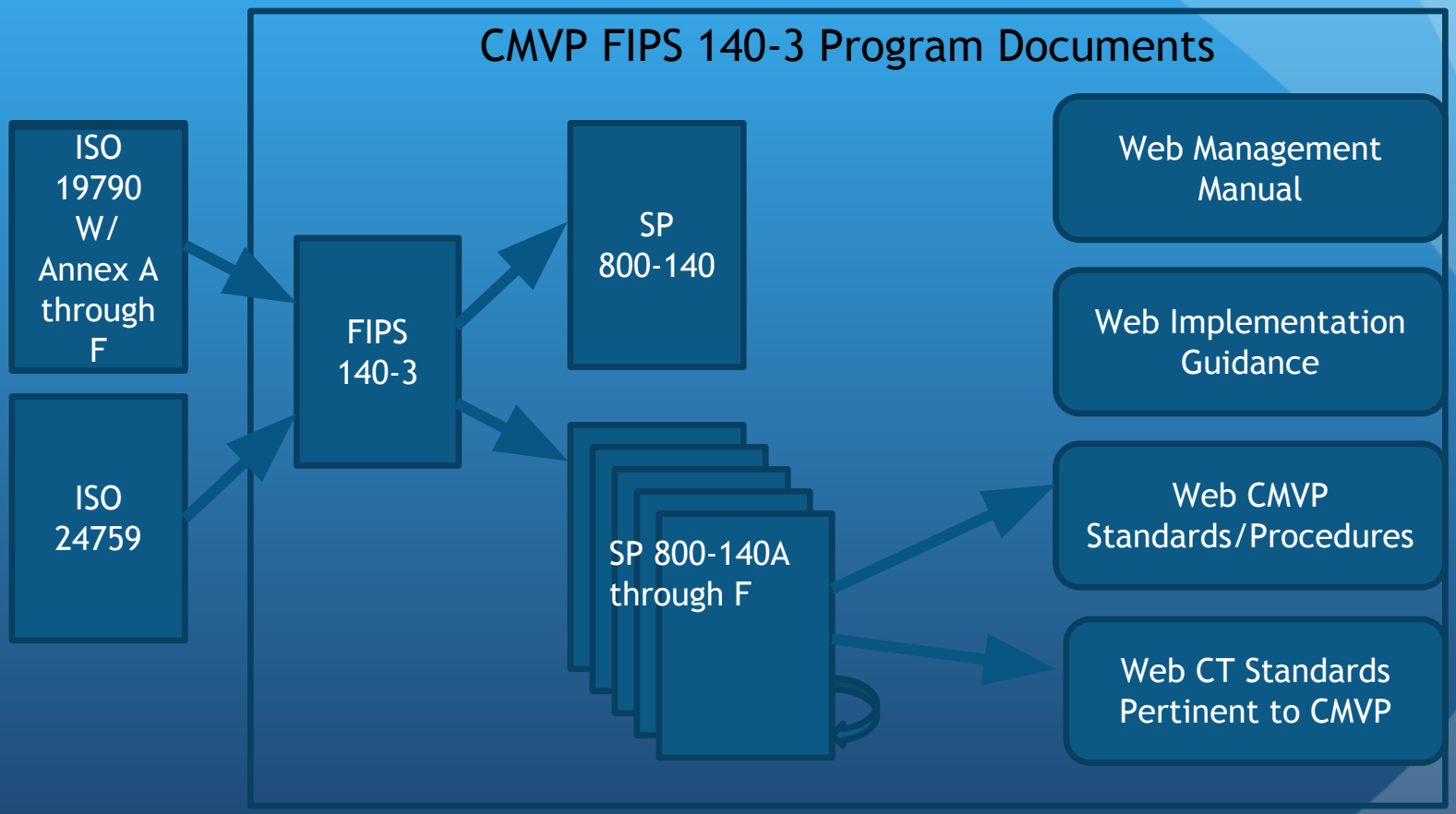
NIST FIPS 140-3 Update

Michael Cooper

ICMC May 9, 2018

Overview

- Quick status
  - Draft documents completed NIST reviews
  - Needs Signature by the Secretary of Commerce
- Necessary Standards
  - ISO 19790 and ISO 24759
  - FIPS 140-3
  - SP 800-140 and SP 800-140A through F
  - Management Manual
  - Implementation Guidance
- Questions


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

Benefits and Value

- **Collaboration on Cryptographic Requirements**
- **Collaboratively developed Protection Profiles**
  - **Standards-based**
  - **Define baseline security functionality and test activities for COTS IT products**
  - **Mandated for National Security Systems (NSS)**
- **NIST recognition and use of ISO/IEC 19790**
  - FIPS 140-3 will map to ISO/IEC 19790 *Security Requirements for Cryptographic Modules*
  - SP800-140 will map to ISO/IEC 24759 *Test Requirements for Cryptographic Modules*
- US Standards necessary to support the ISO
  - FIPS 140-3 wrapper document that will point to the ISO standard
  - FIPS 140-3 appendices A-F will point to the ISO appendices and SP800-140 A-F
  - SP800-140 (test requirements) will point to ISO 24759

Automation

- Automated Cryptographic Validation Testing (ACVT)
- Algorithms
  - ACVT Pilot is complete
  - Development near complete – Fall 2018
  - Hybrid program until all algorithm testing uses ACVT
  - Future transition to only automated testing using the NIST ACVT service (first-party and third-party testing)
- Modules
  - Proof of concept is in progress

Questions/Suggestions