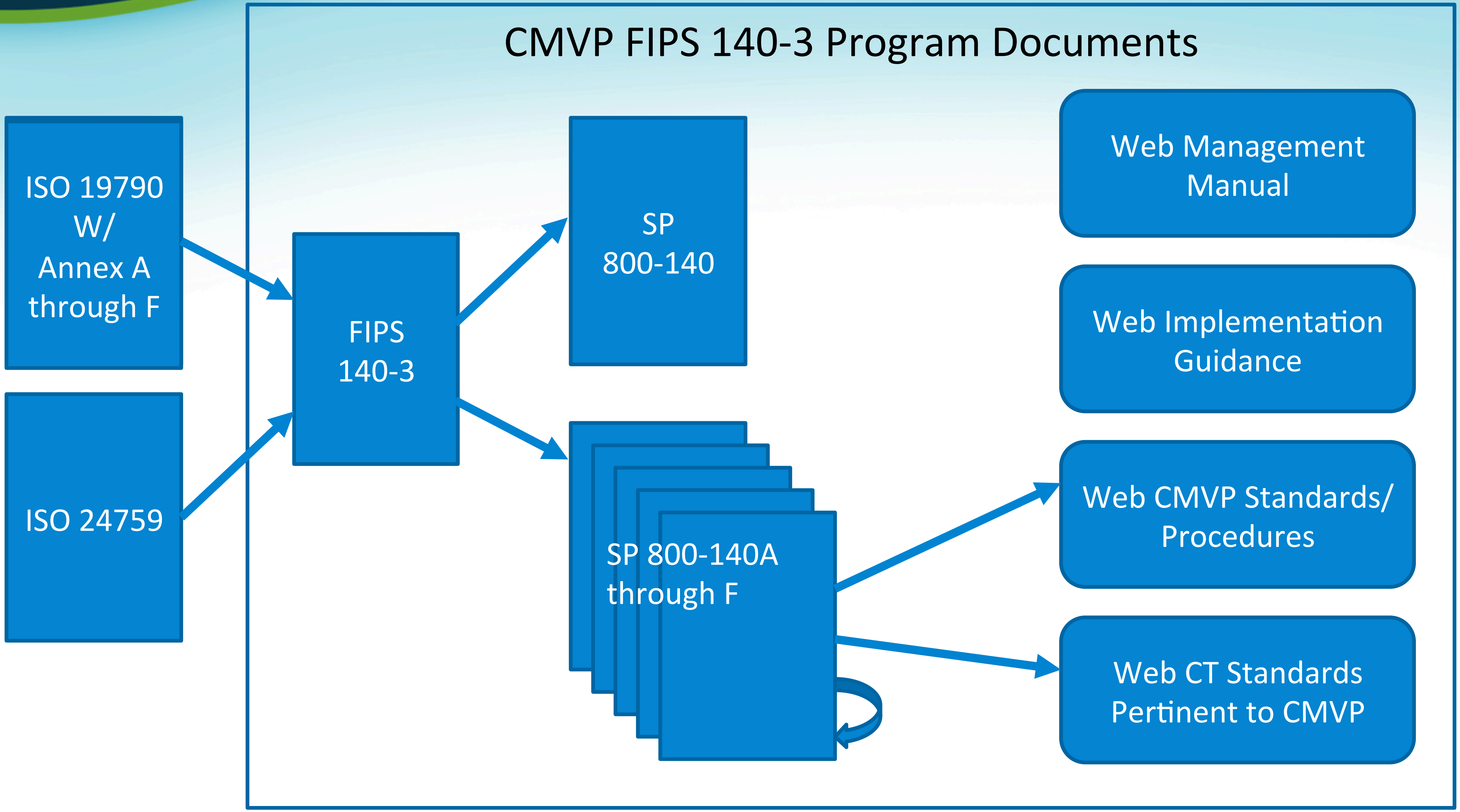
Draft FIPS 140-3 Implementation using ISO Standards

Presented by Kim Schaffer, DSc
At ICMC 2017

- Quick status
  - Draft documents awaiting public comment period
- Overview of documentation
  - 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

ISO/IEC 19790:2012(E)

- Purpose is:
  - Security requirements for cryptographic modules
  - Annexes define requirements 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 24759:2014(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 24759:2014(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 24759:2014(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 800-140A Documentation Requirements

- Dictates the presentation of ISO/IEC 19790:2012(E) Annex A requirements
- Can change any additional requirements in ISO/IEC 24759:2014(E) 6.13
- Could call for the use of the Security Policy Template

SP 800-140B Crypto Module Security Policy

- Dictates the presentation of ISO/IEC 19790:2012(E) Annex B requirements
- Can change any additional requirements in ISO/IEC 24759:2014(E) 6.14
- Could call for the use of the Security Policy Template

SP 800-140C Approved Security Functions

- Replaces ISO/IEC 19790:2012(E) Annex C requirements
- Can change any additional requirements in ISO/IEC 24759:2014(E) 6.15
- Draft should point to CT administered website for requirements

SP 800-140D Approved Sensitive Security Parameter Generation and Establishment Methods

- Replaces ISO/IEC 19790:2012(E) Annex D requirements
- Can change any additional requirements in ISO/IEC 24759:2014(E) 6.16
- Draft should point to CT administered website for requirements

SP 800-140E Approved Authentication Mechanisms

- Replaces ISO/IEC 19790:2012(E) Annex E requirements
- Can change any additional requirements in ISO/IEC 24759:2014(E) 6.17
- Draft should ?
  - Point to CT administered website for requirements
  - Point to new standard
  - Incorporate draft annex from old Draft 140-3

SP 800-140F Non-Invasive Attack Mitigation Test Metrics

- Replaces ISO/IEC 19790:2012(E) Annex F requirements
- Can change any additional requirements in ISO/IEC 24759:2014(E) 6.18
- Draft should ?
  - Point to CT administered website for requirements
  - Point to new standard

Implementation Guidance

- Updated from 140-2 to address 140-3 issues
- Transition to web-based document
- Under control of CMVP at www.nist.gov/cmvp

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