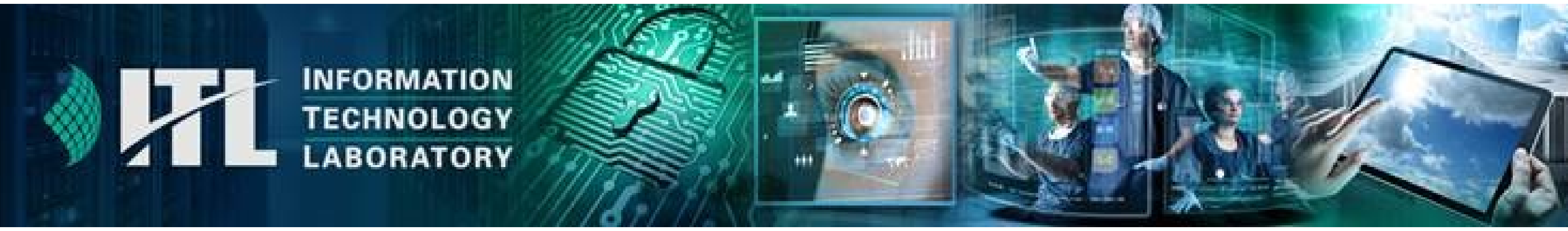


ITL BULLETIN MAY 2019

FIPS 140-3 Adopts ISO/IEC Standards

Kim Schaffer
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) to specify requirements for computer systems used by non-military government agencies and government contractors. The latest FIPS publication, FIPS PUB 140-3 *Security Requirements for Cryptographic Modules*, supersedes FIPS 140-2. The updated standard specifies requirements for cryptographic modules within cyber systems protecting sensitive information. The standard covers areas related to the secure design, implementation, and operation of a cryptographic module, including module specification; module interfaces; roles, services, and authentication; software/firmware security; operating environment; physical security; non-invasive security; sensitive parameter management; self-tests; and life-cycle assurance.

Utilizing International Standards

The most notable change in this version of the standard is the use of International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards, ISO/IEC 19790:2012 and associated testing standard ISO/IEC 24759:2017. The U.S. was very active in the earlier ISO/IEC 19790:2006, which was based on the FIPS 140-2. U.S. and Canadian support of the ISO efforts helped ISO gain worldwide participation and review, offering an updated standard in 2012. The ISO/IEC 24759 has a similar history with the latest version being ISO/IEC 24759:2017.

NIST and the Canadian Centre for Cyber Security participate in a joint effort, the Cryptographic Module Validation Program (CMVP). The CMVP will be a validation authority under the ISO/IEC scheme. CMVP modules validated as conforming to FIPS 140 standards are accepted by the federal agencies of both countries for the protection of sensitive information (United States) or Protected Information (Canada). The goal of the CMVP is to promote the use of validated cryptographic modules and provide federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.

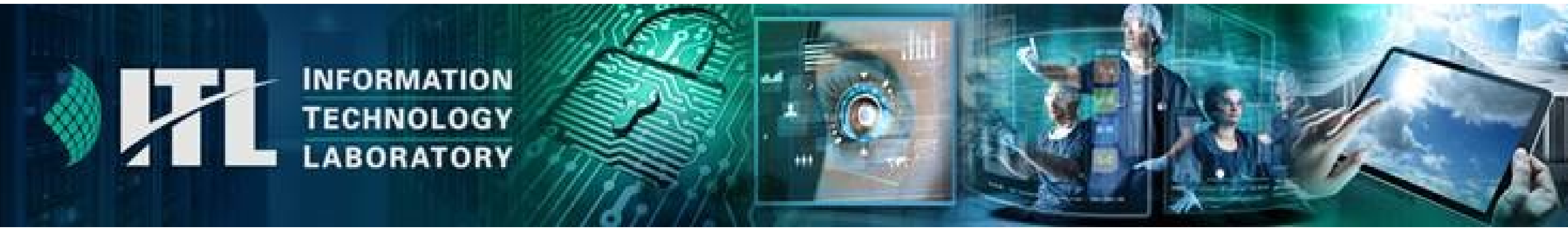
Third Party Testing with NIST Oversight
Vendors of cryptographic modules wishing to sell to these governments validate modules through the independent, accredited Cryptographic and Security Testing (CST) laboratories. National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories perform cryptographic module compliance/conformance testing, protecting the vendor's Intellectual Property (IP) while assuring high quality assessment. Currently using FIPS 140-2 and the associated derived test requirements, the labs will be transitioned to using the ISO/IEC 19790 and derived test requirements specified in ISO/IEC 24759, as modified by the validation authority.

The FIPS 140 standards have been the vessel for enforcing the use of federally approved cryptographic standards into the module requirements. ISO/IEC 19790 also permits this format by specifying ISO/IEC standards where appropriate while allowing the validation authority to supplement or replace cryptographic, non-invasive security and authentication needs specific to CMVP. A set of special publications, SP 800-140, FIPS 140-3 Derived Test Requirements (DTR) and SP 800-140A-F (see Additional Resources) detail the CMVP requirements specific to the validation authority.

Use of Validated Modules
U.S. federal agencies, at their discretion, may continue to purchase any of the products on the FIPS 140-2 CMVP validated modules list. FIPS 140-2 products are expected to dominate the validation list for at least five years after FIPS 140-3 testing has begun. To meet future Federal Information Security Modernization Act (FISMA) requirements, agencies should develop plans for the acquisition of FIPS 140-3 validated products. **Note**: the CMVP Historical list is provided for reference purposes only and should not be used for procurement decisions.

Additional Resources:

- FIPS 140-3: https://csrc.nist.gov/publications/detail/fips/140/3/final
- CMVP URL https://www.nist.gov/cmvp
- Canadian Centre for Cyber Security, P.O. Box 9703, Terminal, Ottawa, Ontario K1G 3Z4
- Special Publication 800-140x Development
  https://csrc.nist.gov/projects/fips-140-3-development#sp800-140
- SP 800-140, FIPS 140-3 *Derived Test Requirements (DTR)*
- SP 800-140A, *CMVP Documentation Requirements*
- SP 800-140B, *CMVP Security Policy Requirements*
- SP 800-140C, *CMVP Approved Security Functions*
- SP 800-140D, *CMVP Approved Sensitive Security Parameter Generation and Establishment Methods*
- SP 800-140E, *CMVP Approved Authentication Mechanisms*
- SP 800-140F*, CMVP Approved Non-Invasive Attack Mitigation Test Metrics*



ITL Bulletin Publisher: Katherine Green
Information Technology Laboratory
National Institute of Standards and Technology
katherine.green@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.