	FIPS 140-3 Security Level			
Requirement Area	**1**	**2**	**3**	**4**
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module including all hardware, software and firmware components. All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function, or process in an approved manner.			
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths		Trusted channel	
Roles, Services, and Authentication	Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	Multi-factor authentication
Software / Firmware Security	Approved integrity technique. Defined SFMI, HFMI and HSMI. Executable code	Approved digital signature or keyed message authentication code-based integrity test	Approved digital signature based integrity test	
Operational Environment	Non-modifiable. Limited or Modifiable Control of SSPs	Modifiable. Role-based or discretionary access control. Audit mechanism		
Physical Security	Production-grade components	Tamper evidence. Opaque covering or enclosure	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing EFP or EFT	Tamper detection and response envelope. EFP. Fault injection mitigation
Non-Invasive Security	Module is designed to mitigate against non-invasive attacks specified in Annex “F”.			
	Documentation and effectiveness of mitigation techniques specified in Annex “F”		Mitigation testing	Mitigation testing
Security Parameter Management	Random bit generators, SSP generation, establishment, entry & output, storage & zeroization			
	Automated SSP transport or SSP agreement using approved methods			
	Manually established SSPs may be entered or output in plaintext form		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures	
Self-Tests	Pre-operational: software/firmware integrity, bypass, and critical functions test			
	Conditional: cryptographic algorithm, pair-wise consistency, SW/FW loading, manual entry, conditional bypass & critical functions test			
Life-Cycle Assurance				
Configuration Management	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle		Automated configuration management system	
Design	Module designed to allow testing of all provided security related services			
FSM	Finite State Model			
Development	Annotated source code, schematics or HDL	Software high-level language. Hardware high-level descriptive language		Documentation annotated with pre-conditions upon entry into module components and postconditions expected to be true when components is completed
Testing	Functional testing		Low-level testing	
Delivery & Operation	Initialisation procedures	Delivery procedures		Operator authentication using vendor provided authentication information
Guidance	Administrator and non-administrator guidance			
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available			Specification of mitigation of attacks with testable requirements

THE ANNEXES OF ISO/IEC 19790:2012 & FIPS 140-3

The Annexes of the ISO/IEC standard allow for each approval authority (i.e. the CMVP) to tailor the standard for their own requirements. Drafts of the NIST Annexes are due in September 2019.

Annex	NIST SP	Description
A	SP 800-140A	Documentation requirements for each of the eleven requirement areas
B	SP 800-140B	Details of the requirements for the contents of the non-proprietary security policy and the order of the contents. This aims to make the security policy document more consistent between vendors.
C	SP 800-140C	A default set of Approved security functions, referring to various ISO standards for block ciphers, stream ciphers, asymmetric algorithms and techniques, message authentication codes, hash functions, entity authentication, key management and random bit generation
D	SP 800-140D	A list of the approved sensitive security parameter generation and establishment methods
E	SP 800-140E	Approved authentication mechanisms
F	SP 800-140F	Approved non-invasive attack mitigation test metrics

Associated Documents

ISO/IEC 19790	**Security Requirements for Cryptographic Modules** Provides the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems.
ISO/IEC 24759	**Test Requirements for Cryptographic Modules** Specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012.
ISO/IEC 30104	**Physical Security Attacks, Mitigation Techniques & Security Requirements** Addresses how security assurance can be stated for products where the risk of the security environment requires the support of such mechanisms.
ISO/IEC 17825	**Testing Methods for the Mitigation of Non-invasive Attack Classes against Cryptographic Modules** Specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790 for Security Levels 3 and 4.
ISO/IEC 18367	**Cryptographic Algorithms and Security Mechanisms Conformance Testing** Provides guidelines for cryptographic algorithms and security mechanisms conformance testing methods. Based on the conformance testing methods employed in JCMVP and in CAVP
ISO/IEC 29128	**Verification of Cryptographic Protocols** Specifies design evaluation criteria as well as methods to be applied in a verification process for such protocols. It also provides definitions of different protocol assurance levels consistent with evaluation assurance components in ISO/IEC 15408.
ISO/IEC 19249	**Catalogue of Architectural & Design Principles for Secure Products, Systems and Applications** Provides a catalogue of architectural and design principles that can be used in the development of secure products, systems and applications together with guidance on how to use those principles effectively.
ISO/IEC 20543	**Test and Analysis Methods for Random Bit Generators within ISO/IEC 19790 and ISO/IEC 15408** Specifies a methodology for the evaluation of non-deterministic or deterministic random bit generators intended to be used for cryptographic applications.
ISO/IEC 19896	**Competence Requirements for Information Security Testers and Evaluators** Provides a framework and minimum requirements for the knowledge, skills and effectiveness of individuals performing testing activities for a conformance scheme.