	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Machine Model	Specification of finite state machine model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production-grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP and EFT.
Operating System Security	Executable code. Authenticated software. Single operator.	CAPP evaluated at EAL2.	CAPP plus trusted path evaluated at EAL3 plus security policy modeling.	CAPP plus trusted path evaluated at EAL4 plus security policy modeling, covert channel analysis, and modularity.
Cryptographic Key Management	Approved key generation/distribution techniques.		Entry/output of keys in encrypted form or direct entry/exit with split knowledge procedures.	
EMI/EMC	FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for voice).		FCC Part 15. Subpart B, Class B (Home use).	

Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.		Statistical RNG/PRNG tests – callable on demand.	Statistical RNG/PRNG tests–performed at power-up.
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification. Functional testing.	High-level language implementation. Test Coverage analysis.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements			