FIPS 140-2 Validation and Consulting

The Committee on National Security Systems Policy Number 11 (CNSSP) requires that all commercial off-the-shelf information assurance-enabled IT products used in national security systems be evaluated and validated as specified by the Cryptographic Module Validation Program (CMVP) and/or the Cryptographic Algorithm Validation Program (CAVP). The CMVP is a joint effort between the United States based National Institute of Standards and Technology (NIST) and Canadian based Communications Security Establishment (CSE). Modules validated as conforming to FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

FIPS 140-2 applies to any system that stores, transmits or receives sensitive government data; not just classified systems. FIPS 140-2 tests Cryptographic Module security requirements related to design and implementation.

ONE LAB, ONE PROCESS

Our Accredited Testing and Evaluation (AT&E) Lab is accredited by the National Institute of Standards and Technology (NIST) to provide Common Criteria, Federal Information Processing Standards (FIPS) 140-2, FIPS 201, Security Content Automation Protocol (SCAP), Transportation Working Identification Credential (TWIC), and Personal Identity Verification (PIV) evaluation and testing services. As the industry volume leader, our labs have certified more than 1000 IT security products across these certification standards.

Working as one lab, our subject matter experts intimately understand which standards apply to your product, how to meet the required criteria, and how those requirements fit together. Our lab personnel combine evaluation expertise with programmatic experience allowing Leidos to provide a single source for all of your testing and certification needs which decreases overall cost and timelines.

Since 2000, Leidos is the industry leader in FIPS 140-2 validations and Common Criteria evaluations; internationally recognized for:

> Performing the most NIAP CC Certifications

> Performing the 2nd most FIPS 140-2 Certifications

> 1st NIAPP PP certifications—Wireless LAN Access Systems, Network Device, Network Device+VPNGW, Network Device + VPN Gateway + Stateful Traffic Filter Firewall, Full Disk Encryption, IPSec VPN Client, and General Purpose OS.

> 1st PIV Middleware validation

> 1st Secure Content Automation Protocol (SCAP) v1.1 and v1.2 validations

> 1st Transportation Worker Identification Credential (TWIC) validation

leidos

WHY PARTNER WITH LEIDOS?

Partner with Leidos to protect your proprietary information (product, source code) while conducting relatively low effort and cost competitive FIPS 140-2 validation. As the industry technical and volume leaders, we can provide scalability to concurrently support multiple certification efforts that meet your aggressive sales timelines. With our experience, we've become trusted advisors and thought leaders helping set the certification standard.

Through our many industry firsts, we continue our pioneering pedigree to influence future directions of the CMVP Program when it comes to providing input to the creation and/ or maintenance of FIPS 140-2 Implementation Guidance, CMVP policy changes, thought leadership via industry conference presentations and shepherding our clients through the validation standard.

Our technical and programmatic teams are ready to listen to your business needs and will happily apply our extensive certification and validation expertise in devising a customized and achievable cost competitive strategy to meet federal sale prerequisites. Talk to a FIPS 140-2 Subject Matter Expert today.

FOR MORE INFORMATION

L_AT&E_ate_lab@leidos.com

leidos.com/CC-FIPS140

Lcol-240 R0

FIPS 140-2 SERVICES

The Leidos FIPS 140-2 Lab provides a full range of services, including:

> **Vendor Organizational Readiness and Product Gap Analysis** – Initial product FIPS 140-2 readiness assessment is conducted in workshop fashion with your product engineers and management.

> **FIPS 140-2 Evidence Consolidation** – Turnkey consulting service to help you consolidate all FIPS 140 specific documentation needed for a successful FIPS 140 validation (Testing and Evaluation).

> **FIPS 140-2 Validation (Testing and Evaluation)** – Testing and evaluation of your cryptographic module against the FIPS 140-2 Publication.

> **Cryptographic Algorithm Testing** – Conduct algorithm testing that will be submitted to the Cryptographic Algorithm Validation Program (CAVP) and upon approval published to a public listing. CAVP is sometimes a prerequisite for FIPS 140-2 Validations and Common Criteria PP Evaluations.

> **Product Validation Maintenance (Revalidation)** – Once FIPS 140 validated, a vendor can avoid having to repeat the cumbersome full validation process by updating their current certificate to include newer product versions (software, firmware, hardware). The changes Leidos can process as a Revalidation include but are not limited to: bug fixes, new product features, operating system/ processor porting, etc.

> **FIPS 140-2 and ISO/IEC 19790 Differences Analysis Consulting** – Be on the forefront of the FIPS 140 evolution with this in depth overview of the key differences in the proposed international iteration of FIPS 140.

> **Ad-Hoc Consulting Services** – We can provide the needed resources to help augment your staff when an organization's technical resources may not be available.

> **Embedded "FIPS Inside" Module Compliance Review** – Oftentimes, a product embeds a FIPS 140 Validated Cryptographic Module within i.e. "FIPS Inside", but fails to utilize the Module in a correct and secure fashion. Leidos can review the Module integration within your product and advise on any flaws and non-compliances.

leidos