One Lab, One Process

Our Accredited Testing and Evaluation (AT&E) Lab is accredited by the National Voluntary Laboratory Accreditation Program (NVLAP Lab Code 200427-0) to provide Common Criteria (CC), Federal Information Processing Standards (FIPS) 140, FIPS 201, Security Content Automation Protocol (SCAP), Personal Identity Verification (PIV), and a host of other ad-hoc evaluation and consulting services. As the industry volume leader, our labs have certified more than 1,000 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 combines 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 validations and Common Criteria evaluations; internationally recognized for:

- Performing the most National Information Assurance Partnership Common Criteria certifications
- Performing the 2nd most FIPS 140 certifications
- Industry 1st NIAP 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, General Purpose OS, and Server Virtualization
- Industry 1st Personal Identity Verification Middleware validation
- Industry 1st Secure Content Automation Protocol v1.1 and v1.2 validations
- Industry 1st Transportation Worker Identification Credential validation

Common Criteria

The Committee on National Security Systems Policy (CNSSP) Number 11 requires that all commercial off-the-shelf information assurance-enabled IT products used in national security systems to be certified by the National Information Assurance Partnership (NIAP) program according to National Security Agency approved processes. NIAP operates the Common Criteria Evaluation and Validation Scheme (CCEVS) to oversee evaluation of commercial information technology products for conformance to the Common Criteria.

In addition to NIAP/CCEVS in the U.S., Common Criteria is an international standard (ISO/IEC 15408) operated by 17 certificate authorizing nations and accepted by 31 nations for its respective government acquisition requirements similar to CNSSP-11.

COMMON CRITERIA SERVICES

The Leidos Common Criteria Lab provides turnkey certification services, including:

Vendor Organizational Readiness and Product Gap Analysis

Initial CC readiness assessment with product engineers and management.

Security Target Development and Consulting

Primary CC artifact required for NIAP PP and International CC certification.

Product Certificate Maintenance

Organizations have the option to refresh certification via an abbreviated process.

Ad-Hoc Consulting Services

In cases where an organization's technical resources may not be available, we can provide the needed resources to help augment your staff.

Protection Profile (PP) Evaluation and Consulting

- PP Evaluation – CC certification conducted to industry-defined baseline technology type functionality.
- PP Conformance Pre-testing –Augment the academic Gap Analysis effort with targeted testing to ensure the product's proper application of PP requirements.
- Guidance Development and Maintenance – CC requires the customization of your organization's product documentation to specify how to configure and operate the product in its static CC mode.
- Entropy / Key Management Development and Maintenance – NIAP may require entropy if the targeted Protection Profile requires the declaration of how the product's SP 800-90B Random Bit Generator (RBG) implementation and/or the Management Document (Isolation Document) detailing the isolation implementation of connected computers.

International Evaluation Assurance Level (EAL) Evaluation and Consulting

- International EAL Evaluation – CC certification conducted against the product functionality as-is defined by the product vendor.
- Design and Architecture Development and Maintenance – Design/develop the product's internal interfaces, external interfaces, and architectural design.
- Vendor Functional Testing – Complete test reports confirming the Security Target claimed functionality.
- Vendor Lifecycle Consulting – Lifecycle support of the product vendor's delivery mechanisms, product configuration management system, product configuration management controls and at higher levels the development facility security controls, vendor life-cycle definition and product tools and techniques.

FIPS 140

NIST established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) 140. The CMVP is a joint effort between NIST and the Canadian Centre for Cyber Security (CCCS), a branch of the Communications Security Establishment (CSE). Modules validated as conforming to FIPS 140 are accepted by the Federal Agencies of both countries for the protection of sensitive information. FIPS 140-2 superseded FIPS 140-1 and FIPS 140-3 is set to supersede FIPS 140-2 in late 2020. The applicability statement from FIPS 140 (page iv):

FIPS 140 acquisition and deployment requirements are currently being expanded to the U.S. Federal Contractor space. DFAR 252.204-7012 states that defense contractors must comply with the security controls outlined in NIST SP 800-171 r1 for non-federal networks that may store or process Controlled Unclassified Information (CUI). NIST SP 800-171 r1 states the following in regards to FIPS 140 validated crypto:

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

In layman's terms, commercial vendors are required to achieve FIPS 140 validation of their crypto modules in support of their commercial federal contractors DFARs requirements, in addition to achieving FIPS 140 for current Department of Defense acquisition.

Applicability. This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract. Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against this standard. The adoption and use of this standard is available to private and commercial organizations.

ate@leidos.com | leidos.com/CC-FIPS140

FIPS 140 SERVICES

The Leidos FIPS 140 Lab provides a full range of turnkey certification services, including:

Vendor Organizational Readiness and Product Gap Analysis

Initial FIPS 140 readiness assessment to identify gaps in the cryptographic module and meet the FIPS 140 standard. Upon completion, Leidos provides a formal report.

FIPS 140 Documentation Consolidation

Turnkey consulting service to help consolidate all FIPS 140 specific documentation needed for a successful FIPS 140 Validation.

FIPS 140 Validation

Testing and evaluation of your cryptographic module against the latest FIPS 140 publication.

Cryptographic Algorithm Testin

Conduct algorithm testing for submission to the Cryptographic Algorithm Validation Program (CAVP) and upon approval published to a public listing. CAVP is sometimes a prerequisite for FIPS 140 validations and CC PP Evaluations.

CAVP Test Harness Development

Develop test harness to test your cryptographic module against the CAVP and/or Automated Cryptographic Validation Protocol (ACVP) test frameworks.

Product Validation Maintenance (Revalidation)

A vendor can avoid repeating the cumbersome full validation process by updating their current certificate to include newer product versions (software, firmware, hardware). Leidos can process the changes as a revalidation including but not limited to: bug fixes, new product features, operating system/processor porting, new hardware, etc.

FIPS 140-2 and FIPS 140-3 Differences Analysis Consulting

Be at the forefront of the FIPS 140 evolution with this in-depth overview of the key differences between FIPS 140-2 and FIPS 140-3.

Embedded "FIPS Inside" Module Compliance Review

A product often embeds a FIPS 140 Validated Cryptographic Module within (i.e., "FIPS Inside"), but fails to use the module in a correct and secure fashion. Leidos can review the module integration and advise issues and/or non-compliance.

Ad-Hoc Consulting Services

We can provide the needed resources to help augment your staff when technical resources may not be available.

Other AT&E Services

The Leidos AT&E Lab provides a full range of other security and consulting services, including:

Turnkey Programmatic Support
Our Program Management team can fulfill all duties expected of a "Vendor Certification Manager," such as:

- Layered multi-product organizational certification schedules detailing inner-dependencies across product suites with associated cost metrics (e.g., monthly burn, milestone payments, etc.).
- Requirements definition and coordination with internal and external stakeholders (e.g., 3rd party consultant, government, etc.).
- Program execution serving as a single point for scheduling and financial data needs.

FIPS 201 – NIST PIV
Leidos is accredited to perform NIST PIV FIPS 201 testing in compliance with NIST SP 800-73. The program scope includes testing of two PIV components; PIV middleware and PIV card application.

FIPS 201 – GSA PIV
Similar to NIST PIV, we are accredited to perform testing against the GSA iteration of FIPS 201, which expands the scope of work beyond NIST SP 800-73.

SCAP Compliance Testing
We are accredited to perform SCAP Compliance Testing against the most recent version of the standard(v1.3). SCAP tests the ability of authenticated configuration scanners designed to detect vulnerabilities and misconfigurations with patches or policy settings.

The Committee on Foreign Investment in the United States
Leidos successfully serves as the 3rd party auditor for corporations that have technical entanglements of concern to the U.S. State Deparment.

FedRamp
Our suppliers provide turnkey advisory and assessment services for cloud service providers (IaaS / PaaS / SaaS).

U.S. Department of Defense Information Network Approved Products List Approval
Leidos provides turnkey DoDIN APL acceptance services by coupling our industry leading Information Assurance CC and FIPS 140 validations with our suppliers conducting the latter interoperability (IO) testing to achieve DoDIN APL posting.

FIPS 140 SP 800-90B
We help vendors provide and/or develop the generation of random bit raw data in accordance to SP800-90B 3.1.1, create documentation (source information of entropy, IID claims, conditioning, and health tests), and provide supporting documentation (e.g., IG 7.15) with justification sufficient for acceptance by CMVP.

3rd Party Customized Consulting
Leidos AT&E lab is not restricted to the activities detailed above. The lab has successfully leveraged the disciplines of the accreditations; from CC based life cycle audits, CC based vulnerability and penetration testing activities, to FIPS 140 based Suite-B algorithm testing we create customized deliverables to meet our client's unique business needs.

The Leidos AT&E Lab Management team consists of security certification experts that are on the forefront of Common Criteria and Crypto Security (notably FIPS 140-2) industry updates.

KEY BENEFITS

Turnkey Certification

Leidos leverages its variety of subject matter experts and strong Program Management team to lead the certification efforts with minimal vendor involvement. We set up an overall program plan, working backward from GA code release dates to ensure all elements of the certification efforts stay on track. This approach can cut vendor engineering involvement in half allowing your team's engineers to stay on track with the product development/ maintenance.

Intellectual Property (IP) Protection

As the pre-imminent IT Security federal contractor, we understand how to protect sensitive data; proven by the many successful audits affirming our IP protection mechanisms. The Leidos AT&E lab's NVLAP (Lab code 200427-0) accreditation affords vendors an additional level of IP protection by replicating Leidos' corporate processes on a smaller scale. By treating all materials as "sensitive IP," all vendor products (hardware, software) have similar controls — product testing must be executed in either an accredited AT&E Lab or controlled vendor environment.

Commercial Solutions for Classified (CSfC) Trusted Integrator

The Leidos AT&E lab is tightly synced with the Leidos CSfC Trusted Integration Team to provide one trusted voice for eventual CSfC compliance. Leidos will happily process the CSfC application on the vendor's behalf.

WHY PARTNER WITH LEIDOS?

Our technical and programmatic teams are ready to listen to your business needs and will apply our extensive certification and validation expertise in devising a customized and achievable cost competitive strategy to meet your federal sale prerequisites.

ABOUT LEIDOS

Leidos is a Fortune 500® information technology, engineering, and science solutions and services leader working to solve the world's toughest challenges in the defense, intelligence, homeland security, civil, and health markets. The company's 37,000 employees support vital missions for government and commercial customers. Headquartered in Reston, Virginia, Leidos reported annual revenues of approximately $11.09 billion for the fiscal year ended January 3, 2020. For more information, visit www.Leidos.com.

LinkedIn: Leidos
Facebook: Leidosinc
YouTube: Leidosinc
Twitter: @Leidosinc

FOR MORE INFORMATION

ate@leidos.com | leidos.com/CC-FIPS140

Export control #20-Leidos-0110-21333 | Leidos Creative 20-98393