Corsec) FIPS 140-2

The **Federal Information Processing Standard (FIPS) 140-2 is a U.S. and Canadian co-sponsored security standard** that a hardware or software product using cryptography must meet if it is intended for use in a security system that processes sensitive but unclassified information.

Why Pursue FIPS 140-2 Validation?

Achieving third-party certifications and security validations enables product vendors to:

- Access previously untapped markets, such as the Intelligence Community, Financial Services, Health Care, Critical Infrastructure, and US and Foreign governments

- Demonstrate their corporate commitment to product security

- Elevate their company's brand to potential customers that their products have been independently evaluated against transparent and auditable standards for security

- Gain competitive edge in the marketplace

The Big Questions

How much does a FIPS 140-2 validation cost?

Validation costs vary greatly, depending upon the complexity of the product, the level of validation being sought, and the amount of planning done prior to starting the process. Costs for FIPS 140-2 validations typically fall into six major areas: product design consulting, product design changes and implementation, algorithm testing, documentation production, laboratory testing, and government fees.

How long does a FIP 140-2 validation take?

There are three major phases to a FIPS 140-2 validation: Design and Documentation, Laboratory Testing, and Government Review. A typical validation effort will take anywhere from eight to twelve months from start to finish.

### Who are the key players in the FIPS 140-2 validation process?

There are three key players in FIPS 140-2 validation process: **1.** The National Institute of Standards and Technology's (NIST) Cryptographic Module Validation Program (CMVP) sets information security mandates for products containing cryptography, and is ultimately responsible for issuing certificates; **2.** Third-party laboratories, which are accredited by NVLAP, test products to ensure they adhere to FIPS 140-2 standards; and, **3.** IT product vendors must ensure their products conform to the Standard, and submit documentation to a third-party lab for testing.

To what types of products does FIPS 140-2 apply?

If a product uses cryptography for secure remote management, data encryption, digital signatures, or information protection, it is likely that FIPS 140-2 validation would be required.
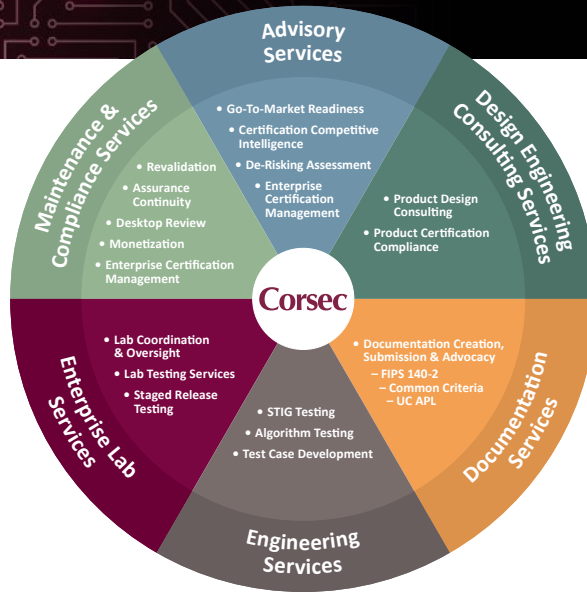
Do all product vendors have to comply with FIPS 140-2?

In the United States, a FIPS 140-2 validation is legally required before products that implement cryptography can be sold to the U.S. Federal Government.
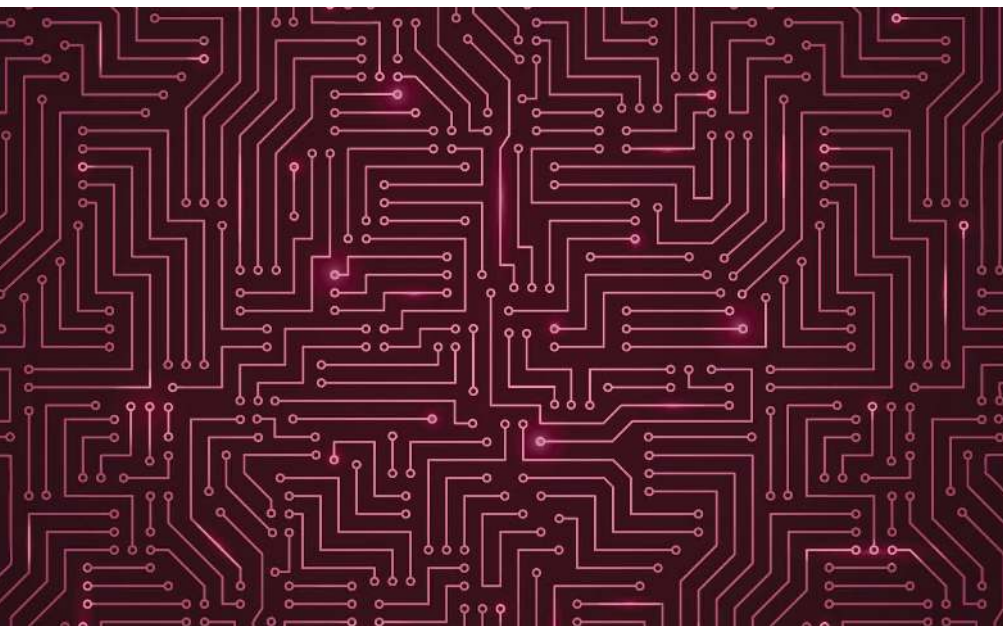
Corsec's Solutions

Corsec's guidance through the maze of certification processes can be the difference between generating revenue when it was budgeted, and having to delay and reforecast, perhaps for months or even years. **Our capabilities enable product vendors in the following areas:**

Advisory Services
- Go-To-Market Readiness
- Certification Competitive Intelligence
- De-Risking Assessment
- Enterprise Certification Management

Design Engineering Consulting Services
- Product Design Consulting
- Product Certification Compliance

Documentation Services
- Documentation Creation, Submission & Advocacy
  – FIPS 140-2
  – Common Criteria
  – UC APL

Engineering Services
- STIG Testing
- Algorithm Testing
- Test Case Development

Enterprise Lab Services
- Lab Coordination & Oversight
- Lab Testing Services
- Staged Release Testing

Maintenance & Compliance Services
- Revalidation
- Assurance Continuity
- Desktop Review
- Monetization
- Enterprise Certification Management

Corsec

"**Corsec did a great job in the planning, guidance, and execution throughout the entire FIPS 140-2 process**. Their expertise and prompt response played a tremendous role in the successful completion of our FIPS 140-2 validation."

— **Eric Jen,**
Director of Engineering,
Openpeak, Inc.

Companies have different needs, different capabilities and different timelines.
To support their unique needs, **Corsec has created several solutions bundles including:**

Core Solution

For those companies who are seeking guidance with a limited scope of services, our **Core Solution** pulls from our Advisory, Design Engineering Consulting and Documentation Service areas, and covers certification fundamentals, including a De-Risking Assessment, Product Design Consulting and Documentation Creation.
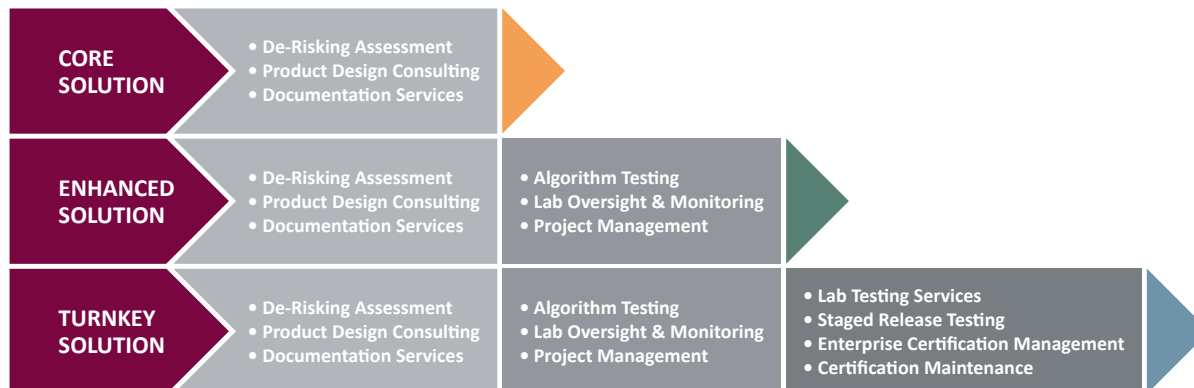
Enhanced Solution

In addition to the documentation set, all key certifications require additional engineering efforts. With FIPS 140-2, the requirement is Algorithm Testing. Corsec's **Enhanced Solution** augments vendors' engineering capabilities by completing this requirement.

Turnkey Solution

For companies seeking the least risky path to certificate issuance, or companies with critical go-to-market timelines, the **Turnkey Solution** is designed to cover every possible need. It includes the Enhanced Solution, plus all phases of lab testing, all government fees, and program management and oversight. It is a solution for companies requiring end-to-end management of the certification process.

Why Corsec?

Corsec is the global leader in providing access to new markets via IT security validations. With the largest staff of experts in the industry and a comprehensive solution that spans consulting, documentation, testing, enterprise lab services, and strategic product roadmap planning, Corsec has secured more than 350 FIPS 140-2, Common Criteria and UC APL certifications for hundreds of organizations on five continents over the last 15 years.

For more information,
visit **corsec.com**.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
Phone: 703.267.6050
info@corsec.com

© Corsec Security, Inc.

FIPS 140-2 — *Satisfies Cryptographic Requirements for U.S. / International Government and Commercial Markets*

CORE SOLUTION
- De-Risking Assessment
- Product Design Consulting
- Documentation Services

ENHANCED SOLUTION
- De-Risking Assessment
- Product Design Consulting
- Documentation Services
- Algorithm Testing
- Lab Oversight & Monitoring
- Project Management

TURNKEY SOLUTION
- De-Risking Assessment
- Product Design Consulting
- Documentation Services
- Algorithm Testing
- Lab Oversight & Monitoring
- Project Management
- Lab Testing Services
- Staged Release Testing
- Enterprise Certification Management
- Certification Maintenance