
Corsec
Shattering FIPS 140-2
Myths & Misconceptions
FIPS

A benchmark for product security in the U.S. and Canada is the FIPS (Federal Information Processing Standard Publication) 140-2 validation process. It is required for products which utilize cryptography/encryption and are used in security systems that process Sensitive But Unclassified (SBU) information. The certification applies to hardware, software, and firmware solutions.

With the interest around product security hardening and data protection increasing, it is not uncommon to discover conflicting information on how to protect your product, including, but not limited to the requirements, processes, terminology, and timeframe to complete the process. It is a complicated endeavor, and a long-term investment that includes: strenuous documentation, product engineering to meet Derived Test Requirements (DTRs), algorithm testing, and program management.

After two decades of performing FIPS validations, Corsec has amassed and clarified several misconceptions that prevent companies from completing the process:

Myth 1: FIPS-Inside is the same as being FIPS 140-2 validated.
The short answer is no. Completing your own FIPS 140-2 validation provides tangible evidence that your product was tested and validated by an accredited lab and scheme. This allows you to assure customers that your solution has been vetted and meets the required security standards issued by the U.S. and Canada. This also allows you to work on your own timelines when updating or changing your product.

The term "FIPS-Inside" or "Compliant" indicates that you've embedded a 3rd party's validated solution into your product. This is a self-designation and has no backing by a Government or accredited testing lab. You are relying on 3rd party certified solutions, their certification team, and their maintenance team. This means that if issues arise with their solution (expiring/getting revoked), you now must deal with those issues. You are also sending a message to customers that, "We didn't test their solution ourselves, but I'm sure they did it right", your company lacks accountability. If you are asked for your certification number, you will not be able to provide one.

Myth 2: I designed my product to follow FIPS 140-2 guidelines, I can claim compliance.
Similar to Myth 1 - The claim of "compliance" becomes irrelevant without the issuance of a certification. Although you may have used FIPS approved algorithms, or featured 256-bit AES encryption, the actual product hasn't undergone the rigorous and extensive testing process to ensure that the crypto functionality is up to standards.

Myth 3: I don't need a FIPS 140-2 validation, I already sell into the FED and/or I know the "right people".
While having connections can sometimes have its perks, the U.S. and Canada have mandated products to complete the validation process prior to procurement. At any point your current customer could discontinue use and halt procurement without a validation number, often seen when other companies complete validation and attempt to lock out competition.

Myth 4: My product was developed outside of the U.S./Canada, so FIPS 140-2 doesn't apply.
The location of your company or origin of product development isn't relevant to achieving a FIPS 140-2 Validation. Products developed outside the U.S./Canada are 100% eligible to sell into the FED and can complete FIPS 140-2 validation like products developed in North America.

There are Independent validation labs in six other countries working with both the U.S. and Canadian Governments to achieve accreditation.

Myth 5: My product used to be on the FIPS 140-2 validated list, I can still use that to leverage sales within the U.S. FED/Canadian Governments.
If your product's validation has been revoked, then unfortunately no. There is a CMVP Historical Validation List that includes modules that Federal Agencies are not to use for procurement. There are several different reasons you may have been placed on the Historical list, but only modules on the active list are approved for purchase.

Myth 6: Getting FIPS 140-2 validated takes too long, we'll never see a ROI.
A typical FIPS 140-2 Validation effort will take roughly 8-12 months from start to completion.

However, it is important to keep in mind that the "time to completion" differs from the "time to revenue". After submitting to the lab, your product will be added to a Government run website and designated as "In-Process" or "Implementation Under Test" (IUT). This status allows you to begin offering your solution to potential customers with government backing.

Myth 7: Getting a FIPS 140-2 validation doesn't provide any real competitive advantage.
Only FIPS validation products can sell into the U.S. FED and Canadian governments. With roughly $90 Billion (USD) allocated in federal spending in 2017, securing your place at the table to gain a portion of this market space is vital and can set you apart from competition.

Myth 8: I already have a FIPS 140-2 validation, I don't need other security certifications.
Maybe. The level of sophistication of your competitors and your customer requirements may also present you with requirements for Common Criteria. If you plan on selling into the U.S. Department of Defense, you will need the **DoDIN APL**, the military's approved product list.

Putting your product through the FIPS validation process can be a game changer for your company and its revenue goals. Being able to separate fact from fiction can help eliminate some of the mystery that might be holding you back from pursuing your validation. Over the past 19 years, Corsec Security, Inc. has helped hundreds of companies complete 450+ security certifications globally. If you have questions on how to get started or have run into roadblocks while attempting to complete the process then get in touch with one of our experts and uncover a successful path to certification.

www.corsec.com