



Communication Devices Inc.  
85 Fulton Street  
Boonton, NJ 07005  
PH: 973.334.1980  
FX: 973.334.0545  
<http://www.commdevices.com>



## Dancing with the FIPS (140-2)

Vendors from near and far are lining up in droves to compete in the latest incarnation of this popular show to see who can best dance around the National Institute of Standards FIPS 140-2 CERTIFICATION process.

Key to this competition is meeting strict NIST Standards. Only a product that has been submitted to a 3<sup>rd</sup> party NVLAP accredited lab which tests and evaluates the entire product, source code, security policy, and state machine, can be deemed CERTIFIED. This Certification is done through NIST with the results of the NVLAP testing. A Certificate is then issued by NIST for the entire product.

Today's contestants will dazzle you with their boldness and fancy dance moves, claiming to have NIST approval status (compliant, validated, or certified).

One contestant claims to be FIPS 140-2 COMPLIANT (GASP!)



Being compliant is a statement that you believe that you have built the device according to the FIPS 140-2 standard. In reality the only way for them to be sure of compliance is to have their product CERTIFIED. Sorry! (AWWW!)

Another contestant claims to be FIPS 140-2 VALIDATED (SIGH!)



Cryptographic MODULES can be VALIDATED. This means that a NVLAP has seen and tested the module on its own. Quite often these MODULES are available for sale to vendors that want to sell to the government but do not have the resources to go through the FIPS process. The vendor acquires the module and then has to implement that module exactly how it is required by the lab. There is no checking at this point, so, the vendor must be taken at their word. The vendor can only claim to be using a FIPS VALIDATED MODULE and specify what module is being used and what it does. The product IS NOT CERTIFIED.

An example would be a vendor using a VALIDATED SSL module. This is fine for SSL but – their SSH implementation is not validated or certified. The SSH protocol may be what the customer is really using. A customer sees FIPS 140-2 VALIDATED and assumes that the SSH validation is included. Not cool!



Our Third contestant claims to be FIPS 140-2 tested–without showing a certificate. How did they even get on the show?



Our fourth contestant and winner has been FIPS 140-2 certified and has a certificate claiming that their product has been submitted to NIST and has passed! (Wild applause!).



Thank you for watching and join us next time for Dancing with the FIPS!