From: [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comment on Control 3.13.11
Date: Wednesday, September 14, 2022 4:47:57 PM

NIST,

I am providing commentary on SP 800-171 control 3.13.11

*3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. DISCUSSION Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Cryptographic standards include FIPS**[1]**validated cryptography and/or NSA-approved cryptography. See [NIST CRYPTO]; [NIST CAVP]; and [NIST CMVP].*

Problem:
Analysis by DIBCAC that over 50% of the DIB partners that have been assessed for compliance with DFARS 252.204-7012 and thus SP 800-171 are not satisfying this control points to a significant issue. With the coming CMMC also referencing this same control from 800-171, a failure to meet the control will become make or break in terms of even being able to accept a DoD contract. The underlying goal of this control is to ensure that when CUI is being protected via encryption, that the encryption itself is tested and trusted – you wouldn't want a home grown algorithm or a flawed implementation to result in the release of CUI. This is a laudable and appropriate goal, but as written can and does introduce further risk by tipping the scales against closing security vulnerabilities.

Where this falls apart is really on the FIPS validation side as opposed to the 800-171 side. While this is a separate NIST process and not this subject of this comment, it still boils back to the same organization and how could 3.13.11 be adjusted to accommodate the FIPS process. As you know when a vendor chooses to pursue FIPS validation, they must build their system a specific way, produce documentation, etc. Once it is built they must submit the product to a lab for testing. When the lab signs off then it heads over to the Government for review and certification. I know I am simplifying the process, but the two points are: the submission is static point in time and the process takes months/years to complete. FIPS 140-3 was supposed to address the timeliness, but evidence to the contrary, everything FIPS wise has stalled industry-wide.

Here is a real world example that depicts what is being experienced across the board.

1. Vendor submits a product for validation
2. 18 months later that submitted version receives a certificate
3. Customers purchase the product and establish FIPS mode to comply with the DFARS requirements which in turn calls out 800-171 3.13.11 as required to pass
4. 6 months later (so 24 months since the initial version that was submitted to the lab was compiled) a vulnerability with a CVSS score of 9.8 is discovered.
5. The vendor publishes a patch/update

6. The Customer that installed the product is faced with a choice: update to close the vulnerability…which will now violate 800-171 and thus DFARS requirements or maintain compliance and expose CUI to the vulnerability.
7. Of course the Customer is going to update, but now has a compliance issue to document in a POAM.
8. Now suppose the vendor does go through the expense end effort to submit the newer version to the lab and NIST to update the certificate. As those months tick by, other vulnerabilities come and go, actual product updates as opposed to bug fixes are introduced, etc.
9. Eventually the customer is going to find themselves many version behind and having to weigh each and every CVE in the product against the need to remain compliant in order to even get contracts. The POAM can never be closed and compliance with the control is forever broken.

It is a given that some of this is brought on by the DoD and the way in which DFARS 252.204-7012 and CMMC are worded, the root still comes back to the 800-171 and its broken relationship with the FIPS validation process.

Suggested Remedy:
Reword the control as follows:

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI where validated means a vendor has been issued a FIPS validation certificate or a vendor will attest in writing that the cryptographic functions or modules of their product have not deviated from the last FIPS validation certificate issued for the product that has been certified.

The additional wording will allow vendors to update firmware/software as needed to quash security vulnerabilities and bugs without jeopardizing their clients' Implementation of the controls in 800-171.

Thanks for accepting the comment, I look forward to version 3 and the relief it will hopefully bring to this broken control.

Joshua Barton

Joshua Barton
CISSP,MBA,ITIL,CCNP,CCDP
Director, ECS Engineering and Identity
Huntington Ingalls Industries
1000 Jerry St Pe' HWY | Pascagoula, MS 39567

[redacted]
[redacted]

Achiever – Intellection – Strategic – Relator – Responsibility

Upcoming Out of Office:
Dec 22-Jan 4
April 7-15, 2023