From: Antone, Nick [redacted]
Date: Wednesday, July 20, 2022 at 10:52:25 AM UTC-4
Subject: 171 rev 3 public comments
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

I know you are going to get several on this one, but I've got to submit my comments as well:

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

This topic is HUGE in every forum. It's been written about by numerous security companies, discussed in working group settings, and in DIB-DOD partnership programs. A quick browse of something as public as Reddit (just search for "CMMC FIPS" or "NIST FIPS") will illustrate how large this one is.

This control is nigh-unto unachievable for anyone but large enterprises because of three issues:

1) The FIPS process is far too slow with the pace of tech changing faster all the time. New versions, patches, vulnerability patches, etc. FAR outpace the NIST FIPS process. And most of us don't have the funds to buy expansive enterprise versions, or extra layers to compensate.

2) We are held accountable for keeping systems up-to-date on the latest security patches, etc. in other controls. We CANNOT do both 3.13.11, and security updates.

3) CMMC is all or none. Originally it was a "NO POA&M" scenario. Now it's a "POA&M under limited conditions" The two notable conditions are: time (6-months seems to be the benchmark so far), and "point value". NIST 800-171 3.13.11 is a 5-point control. Highest category, and therefore ineligible for POA&M at all. ADDITIONALLY, since we have to wait for OEMs as well as NIST on the FIPS validations, the 6-month rule is already well expired. So POA&M doesn't work there either. And yet DoD is telling everyone (including a direct response I received from DOD CIO office: That POA&M is the way forward.

Case in point: Windows 10 Pro. The crypto modules have not been validated since build 1809. That build went end-of-life in November 2019. There has been NO validated crypto modules in any build of Windows 10 since. The whole POA&M notion for 3.13.11 is moot since the timeline is measured in YEARS. Lastly, by the time the currently submitted build of Windows 10

is validated.... it's already superseded for security reasons. Even DoD itself has the FIPS 140-2 problem with this control.

MY POINT: We need some flexibility here. The State Dept approach is "FIPS 140-2 or equivalent encryption". Seems logical. OR... If we turn on "FIPS-mode" in Windows, or Aruba, or Sonicwall, or Red Hat, etc... Those things WERE FIPS validated, and are using all FIPS settings, algorithms, etc. Can this be noted as acceptable for this control? How is this not suitable enough for UNCLASSIFIED information?

Yes, CUI is sensitive, and must be protected, no question. But where the physical protections require a simple locked cabinet or locked drawer, or a taped up package via mail or Fedex.... It does not require a GSA approved safe. The digital equivalent should match. Suggest the use of "FIPS compliant" and not just "FIPS validated". That is something we can all meet, right now, without breaking the bank or disrupting work. Or worst case, allow for items that were FIPS validated but were superseded. So if Win10 build 1809 was validated, then Win10 build 21H1 in "FIPS-mode" is acceptable.

Just my input.

-[redacted]