From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Five desires for NIST 800-171 (and protecting CUI)
Date: Friday, September 16, 2022 9:15:43 PM

Good Evening,

While I am relatively new to cybersecurity (and therefore hope you take my recommendations with both a grain of salt as well as patience as some of these ideas may not be applicable to this forum), due to numerous pain points noticed during the march towards CMMC (which relies heavily upon NIST 800-171), I believe these items would assist the thousands of industry partners in securing our nations CUI.

Five things I would like to have considered for the next revision of the 800-171 are:

1. Inclusion of tailoring and scoping definitions and guidance.
    a. DFARS 252.204-7012 and CMMC's Level 2 Scoping Guidance are a great start, refined definitions and guidance that speak both to security, contractual requirements, as well as to tactical viability (e.g. number 5 below) in companies with complex infrastructures would be helpful.
2. NIST 800-171/FedRAMP Moderate equivalency matrix.
    a. DFARS 252.204-7012 says the use of Cloud services for CUI requires FedRAMP Moderate or equivalent. While I applaud equivalencies, without a definition of them, those in industry are left to choose between only FedRAMP Moderate, or risk that a Cloud service which they believe is equivalent may be determined by an assessor that it is not, which would require a time consuming and costly migration away from that solution.
3. FIPS 140-2 Validated equivalency alternatives.
    a. There are solid encryption methods and standards that may even provide better protection than the 140-2. Please consider an equivalency standard that is based on similarities with already validated methods (e.g. if the NSA determines that AES 128 is sufficient to protect classified data, then if you're using an non-validated AES 192 to protect CUI, it's sufficient) so that industry has sufficient options.
4. Reference the NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 within the NIST 800-171.
    a. Without the direct reference, justification of the Assessment Methodology's use becomes more difficult. It could also provide clarification during assessments with CMMC.
5. Level of separation definition.
    a. With the CMMC requirement to protect assets, which protect assets, which protect CUI, the question of how far that that can be carried is raised. Do we stop

at two levels of separation (as above), or do we stop at four (protect assets, which protect assets, which protect assets, which protect assets, which protect CUI)? Either a clear line in the sand or a method to determine where that line should be for different situations would be helpful.

Thank you very much for your time and consideration.

Regards,
-Jonathan Olson
IT/Cybersecurity Engineer
SimVentions, Inc.
