From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] NIST SP80-171r3 Comments
Date: Friday, September 23, 2022 3:12:52 PM
Attachments: image001.png

I would like us to consider removing the "FIPS validation" requirement. This is a very difficult and oftentimes impossible bar to meet. Many companies who employ encryption in their software product leverage modules from other projects and are unaware of the status of their encryption. However, this doesn't mean that the encryption used is not viable. FIPS validation also places a security and compliance practitioner into conflict when discovering vulnerabilities that have patches but no longer FIPS validated. This ends up meaning that organizations have ongoing POAMs that must continually be updated and adds to the amount of work required to simply document things. My recommendation would be to take a more modern approach like Department of State has in simply stating use of modern encryption is required. This establishes protection of data while at the same time allow flexibility in how the requirement is met.

I would also like to recommend a control stipulating how an organization applies a Zero Trust methodology. While there will be many ways an organization implements ZT, I think it's important that the organization acknowledges this important security aspect and has an opportunity to describe what they are doing above and beyond simple security controls to protect their data and infrastructure. You could allow for partial scoring for no ZTA, 3 points for 3-5 ZTA components and 5 points for 6 or more ZTA components.

One other aspect of the standard that concerns me is that a separate FAQ site exists that explains how to meet controls but is not incorporated into the standard itself. I feel the FAQs should be added as a living appendix more easily found, especially for newer organizations who do not realize CUI protection criteria is scattered about the internet. One other thought on this is that FAQ tend to be more prescriptive in how a control is met when that takes away from the idea of what a control is. We should not be directing what solutions to use to meet criteria even if a brand or technology is not specifically mentioned.

Finally, the 800-171 is written in a more traditional perspective where network and data boundaries are well defined. We need to take SaaS/IaaS technologies into consideration when revising control descriptions. Many organizations use M365, Azure and AWS to store CUI.

Clarify requirements for MSSPs. Some organizations use MSSPs to help monitor event activity and respond to incidents. While there are no formally defined CUI accredited MSSPs (and arguably they are not handling CUI), how do we ensure we are meeting security requirements? Or perhaps this type of service is out of scope if the MSSP does not have access to CUI.

Please also include control scoring in the 171r3 so security practitioners do not need to refer to a separate document when looking at controls.

We should also be clear on what number or which actual controls are deal breakers in compliance. What score achieved allows CMMC certification now that 800-171 is now inextricably tied to

CMMC? Maybe there is an opportunity to take a scored approach vs a zero failure approach, allowing contracting officers to determine if company A is worth the risk if they only meet 65 controls because they have an emerging technology that was previously not considered CUI. Or for a small company with a small amount of CUI, it may not even be worth the expense to meet all 110 controls. If we allow POAMs, it may be needed to have enduring or longer term POAMs. For example a firewall is discovered to have a vulnerability but can be protected with compensating controls. It is not feasible for the company to immediately replace it but would expect to once it's lifecycle is over.

One final thought I have is that 800-171 does not take risk into consideration. A company with 1 billion CUI documents has a much larger risk exposure profile than a small business only handling one CUI contract with less than 100 CUI documents. I think we should be making some considerations for companies who cannot take advantage of more advanced security technologies or capabilities. For example, most businesses with 100+ employees can be hosted in Government Community Cloud-High which is accredited to handle CUI. However, small businesses are not eligible to enroll. So their only real choice is to have a costly on-premise solution and hire staff who can manage it. This put them at a cost disadvantage especially when they have a very small body of documents. Perhaps some controls should not be required for companies under 100 employees while larger companies are required to fulfill all 110 requirements to reflect the amount of CUI data in their holdings. Or perhaps we should actually stipulate volume of CUI data holdings which would require companies to then actually inventory the CUI data they have and where it is. If a company only has 1,000 or less CUI documents, they must do 65 select controls for example (or maybe just meet CMMC Level 1), and up to 1 million CUI documents, 90 controls (or CMMC Level 2). Anything more would require all 110 controls or require CMMC level 3. These are hypothetical numbers, I feel a risk assessment should be performed by DoD to help make this decision.

Kemal O. Piskin

CISO
2551 Dulles View Drive, Suite 200 | Herndon | VA 20171
[redacted] | www.linquest.com

This message and any attachments are intended only for the addressee and may contain information that is privileged and confidential. If you have received this message in error please do not read use copy distribute or disclose the contents of the message and any attachments. Instead please delete the message and any attachments and notify the sender immediately. Thank you.