[redacted] [redacted]

From: Rebecca Conner [redacted]
Date: Tuesday, September 13, 2022 at 10:20:56 AM UTC-4
Subject: Feedback on 800-171 Rev 2
To: Rebecca Conner [redacted], 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

Feedback on NIST 800-171, Rev 2

General Feedback

- Define External Service Providers separate from Cloud Service Providers. This could provide some clarification for CMMC (and ultimately, inheritance allowances).
- Include definition of common controls and inherited controls
- Clarity needed for what's in scope when CUI is shared on a virtual machine
- Contractor Risk Management Assets & SPAs - will NIST better clarify the controls that are still applicable to these items?

Document I reference the most?

CMMC Assessment Guide L2

I heavily rely on the additional details available under the Discussion and Further Discussion sections of the document as well as the Example and the Potential Assessment Considerations sections. The requirements can be difficult to align with your environment and the additional details are incredibly helpful. I see no comparable sections in the NIST 800-171 or 800-171A documentation though I do appreciate appendix D in the 800-171A document.

Managing Controls which are "Not Applicable"

Everyone tells me to never mark a control "Not Applicable" as it is next to impossible to get approved. Instead, I am told to mark a control as "Met" with a comment stating that we have met XYZ requirement because we don't allow it. Honestly, that seems ridiculous and we should be able to accurately mark items as "Not Applicable" and have them assessed accordingly.

NFO Controls

1. Appendix E calls out NFO controls which are noted as, “The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification”. *It is difficult to garner management support for requirements that won’t be “assessed” but are “expected to be satisfied*”.
    a. If you expect NFO Controls to be routinely satisfied, then bring them into the requirements.
2. *Many of the NFO controls did not apply to our organization but those that would prove prudent in the future for any organization might include:*
    a. A generic policies and procedures requirement

        i. I believe the DIB has a handle on this but if you feel like we need it called out then including it once would be much easier. Having one for every category did not prove helpful!!!!

2.
    b. AT-4 : Security Training Records – again, I think the DIB will have this as a matter proving that we are conducting training
    c. CM-8(5) – incorporated into CM-8 – do not have duplicative accounting of components – no input except to say this seems to be self-explanatory
    d. CM-9 – configuration management plan
    e. PE – 16 – delivery and removal
    f. PL-4 – rules of behavior
    g. PL-4(1) – rules of behavior
    h. PS-6 – access agreements
    i. PS-7 – external personnel security
    j. PS-8 – personnel sanctions
    k. RA-5(2) – update vulnerabilities to be scanned
    l. SA-2 – allocation of resources
    m. SA-3 – system development lifecycle
    n. SA-9 + (2)
    o. SA-10
    p. SC-20
    q. SC-21
    r. SC-22
    s. SC-39
    t. IR-8
3. ***NFO Controls that are more costly/painful for small teams/organizations or seem to already by covered in other sections of NIST 800-171 include:***
    a. CA-2(1) – Outside of our CMMC assessments every 3 years, our organization is not large enough to pay for external assessments and we don’t have qualified team members in the company who are cleared for the CUI environment to conduct an “external assessment”.

        i. If this is covered with the CMMC assessment every 3 years that would be totally good – it would be helpful if that were clear. Conducting another external assessment is costly for many small companies.

3.
    b. CA-3.b “Document, as part of each exchange agreement, the interface

characteristics, security and privacy requirements, controls, and responsibilities for each system…"

i. Per the discussion section for this control, "Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information...Authorizing officials determine the risk associated with system information exchange and the controls needed." From this, it seems that we should be managing the risk as part of RA.3.11.1, Risk Assessment. CA-3.b places undue burden on small organizations who may not have the resources to tackle the detailed agreements as called out here. The organization should be given leeway to manage the risk of these connections as they see fit, which may or may not include documenting specific requirements as part of the agreement.

3.

c. CA-3(5) now CA-7(5) – Isn't this covered under SC.3.13.7?
d. CA-7(1) – is this not covered under CA.3.12.1?
e. CA-9 – is this not covered under AC.3.1.1, CM.3.4.6, CM.3.4.7 & RA.3.11.1? AC.3.1.1 authorizes devices; CM.3.4.6/7 should be limiting functionality to what you need; and, as part of risk assessment, you would review the connections in your organization and validate their benefit vs. risk.
f. CM-2(1) – covered under CM.3.4.1 AO.c
g. CM-2(7) – covered under 3.10.6
h. CM-3(2) – this may prove difficult in some organizations to test every change before implementation. Teams should do this to every extent possible but not all changes are financially feasible to test prior to implementation. This should be a risk-based determination for each organization.
i. MA-4(2) – incorporated into MA-4 – covered under MA.3.7.5
j. PE-6(1) – covered under PE.3.10.2
k. PE-8 – covered under PE.3.10.4
l. PL-2(3) – incorporated into PL-2 – covered under 3.12.4
m. PL-8 – it is prudent for every organization to have a security architecture though it may prove difficult for smaller businesses to have a solution detailed enough for an audit
n. RA-5(1) – incorporated into RA-5 – covered under SI.3.14.4
o. SA-4 +(1, 2, 9, 10) – I don't readily see this being accepted in all contracts.
p. SA-5 – it seems like this is covered under procedures and a variety of other areas. Creating this documentation for every system would be exceptionally onerous for a small organization.
q. SA-11 – isn't this covered in 3.12.1 and 3.12.3?
r. SC-7(3) – covered in 3.4.7
s. SC-7(4) – covered in 3.13.1
t. SI-4(5) – isn't this the entire point of the audit and accountability section?
u. SI-16 – not sure how we would do this

3.13.11 - FIPS validated encryption

A FIPS 140 validated module is based on the exact version of the software used during the *validation process. Any patching or update to the software means the encryption module is no longer validated.*

Example: In an extreme example the last version of Windows 10 workstation that as validated is 1809 but has been end of life since May 11, 2021.

https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation

https://docs.microsoft.com/en-us/lifecycle/announcements/windows-10-1803-1809-end-of-servicing

Any security update to Windows 10 1809 also means that the version is no longer validated.

Suggestion:

NIST provides acceptable use of system or software that was FIPS 140 validated, but the version was incremented to mitigate a security vulnerability or to use a new security feature to enhance the security capabilities of the information system.

Also – ask yourselves – why aren't companies maintaining their FIPS encryption? Something in the process needs to change if you expect the DIB to maintain an effective security posture against attackers that are constantly improving and changing. This environment is too dynamic to have companies trying to maintain old solutions which are likely less secure than current solutions. We are spending too much time in areas that should be a straight-forward for the sake of a certification vs. effectively preparing for the future.

4b - look at the ITAR alternatives, re: international company use

https://www.federalregister.gov/documents/2019/12/26/2019-27438/international-traffic-in-arms-regulations-creation-of-definition-of-activities-that-are-not-exports

"...For large entities, the security boundary may be managed by IT staff, who will encrypt the data before it leaves the entity's secure network and decrypt it on the way into the network. However, in all instances, the means of decryption must not be provided to any third party and the data must not have the cryptographic protection removed at any point in transit."

"The encryption must be accomplished in a manner that is certified by the U.S. National Institute for Standards and Technology (NIST) as compliant with the Federal Information Processing Standards Publication 140–2 (FIPS 140–2), or must meet or exceed a 128-bit security strength. At the time of publication of this rule, that criterion is expressed in ''Table 2: Comparable strengths'' of NIST Special Publication 800–57 Part 1, Revision 4.

Additionally, the technical data may not be intentionally sent to a person in or stored in a § 126.1 country or the Russian Federation, even in its encrypted state. This will allow for transmissions and storage of encrypted data in most foreign countries, so long as the technical data remains continuously encrypted while outside of the United States or until decrypted by an authorized intended recipient."

Alternate link: https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=1d508454db82c8505c3070808c961968

Assessment Objective Clarifications

Some of the assessment objectives in 800-171 are more prescriptive than the assessment objectives in the 800-53 and some assessment objectives requirements are very difficult if not impossible to satisfy.

Suggestion:

Use the 800-53 assessment objectives instead of creating new objectives that are more restrictive. Remove assessment objective wording that requires a method of validation difficult if not impossible to achieve.

Example 1:

NIST 800-171A

3:1:15[a] privileged commands authorized for remote execution are identified.

3:1:15[c] the execution of the identified privileged commands via remote access is authorized.

These two assessment objectives require the organization to identify the privileged commands that are authorized.

The 800-53A (AC-17(4)) does not specify a requirement for the identification of privileged commands instead it states the needs are defined, privileged commands are authorized, and it is documented.

AC-17(04)_ODP[01] needs requiring execution of privileged commands via remote access are defined;

AC-17(04)(a)[01] the execution of privileged commands via remote access is authorized only in a format that provides assessable evidence;

AC-17(04)(a)[03] the execution of privileged commands via remote access is authorized only for the following needs: <AC-17(04)_ODP[01] needs requiring remote access>;

AC-17(04)(b) the rationale for remote access is documented in the security plan for the system.

Note: Alternatively reword assessment objectives to identify a role that is authorized to execute a type of privileged command (Domain Administrators are authorized to remotely execute privileged PowerShell commands)

Example 2:

NIST 800-171A

3:4:1 [f] the inventory is maintained [reviewed and updated] throughout the system development life cycle.

Including [review] as part of the assessment objective suggests that there is requirement to audit at an interval organization inventory.

NIST 800-53a

CM-08b the system component inventory is reviewed and updated <CM-08_ODP[02] frequency>

Note: Reviewing entire inventories based on a frequency is not practical when there could be hundreds of thousands of systems. Even in a small organization that has a thousand different systems it a significant task to verify inventory at specified frequency.

NIST 800-171 applicability (Organizational Owned System and Cloud System)

It is understood by many, but not all, that the NIST 800-171 was written to configure and assess systems that are owned by the organization. Cloud Service Providers (CSP) cannot be directly assessed for all requirements. The DoD has authorized Controlled Unclassified information to store in a CSP if it can meet the FEDRAMP Moderate requirements by the CSP going through FEDRAMP authorization or the organization attesting to meeting the FEDRAMP Moderate requirements. There is confusion on how the 800-171 can be used when CUI is stored in a cloud environment. When creating a requirement, the intent on scope can impact intended results if not properly discerned during the writing of the requirement.

Suggestion:

Clarify applicability of NIST 800-171 to assess cloud service providers and managed service providers.

CMMC Version 1 Delta 20

In CMMC version 1 there were an additional 20 requirements added beyond the NIST 110 requirements. There are recommendations in the Defense Industrial Base that those 20 additional requirements are added to the NIST 800-171. Some of these additional requirements went beyond the protecting the confidentiality of CUI or implemented controls that the Federal Government is not required to enforce through the 800-53 controls.

Example:

CMMC Version 1 RE.2.137 Regular perform and test data backups

This requirement is primarily for business continuity and availability. Some will argue that this is also a defensive mechanism for a ransomware attack. At best it may be a preventive measure IF the adversary knows there is backup strategy, but it is mostly a responsive action by the business to restore capabilities.

Recommendation:

The 800-171 is a set of requirements for protecting the confidentiality of CUI. It is not a security program that takes into consideration all information security business risks such as availability. The 800-171 is also an extension of only the requirements the Government is expecting to maintain based on their own specified requirements to protect CUI. Adding requirements the Government is not enforcing on their own systems is not reasonable. **Recommend that only security requirements directly related to the confidentiality of CUI and is only required by the Government as stated in the 800-53 is extended to CUI in nonfederal system organizations.**

Regards,

Rebecca Conner