[redacted]

Subject: RE: Comments on NIST SP 800-171r2 and related documentation.

From: Kenneth Ingham [redacted]
Sent: Friday, July 29, 2022 2:09 PM
To: sec-cert <sec-cert@nist.gov>
Subject: Comments on NIST SP 800-171r2 and related documentation.

At CS2 DC, Victoria Pillitteri requested comments on NIST SP 800-171r2 and related documents.

Attached is a MS Word file containing comments from my work group about how we use and suggested improvements for NIST SP 800-171r2 and related documents.

I realize that comments are public, but I request that you remove my affiliation and email address from the public version of the comments. I cannot speak for anyone at my company other than those in my group.

I am happy to go into more detail in a discussion with you about any of our comments.

Thank you,
Kenneth Ingham

NIST SP 800-171r2 and related documentation comments

General comments

Because all security controls and actions take resources, it is easier to get C-suite support (and hence resources) for items that are explicitly required. Otherwise, we often get a response along the lines of, "if it is not explicitly required, we will not do it."

How we use NIST SP.800-171 and related documents

We are required by DFARS clause 252.204-7012 to meet the requirements specified in the version of NIST SP 800-171 current at the time of the contract award. Because we regularly get new contracts, we must track the requirements in the most recent 800-171 revision.

Within a given control, we find the discussion useful, although sometimes light in terms of details. We also regularly revisit the assessment objectives, which is why we would prefer to see them merged into 800-171 itself and not "hidden" in a separate document. We occasionally use the assessment methods and objects for the Examine, Interview, and Test.

We appreciate the links in the discussion to other NIST publications to better understand the background and additional details of the requirements.

How we integrate 800-171 with other frameworks

We reference parts of the NIST Risk Management Framework and NIST Cybersecurity Framework to better understand the background for the requirement.

We appreciate the linking to NIST SP 800-53 from the controls in 800-171. Sometimes we are able to answer our questions by looking at the underlying control. Please continue to provide this mapping.

800-171r2 itself

Regarding updates for consistency with 800-53r5 and similar documents, when 800-171r3 is final, we must update our SSP and all related documentation. This means that any change will result in work. As long as the changes are documented (for example, what moved to what), if the resulting labeling is "better" than the prior labeling (such as solving the sorting problem mentioned elsewhere), we are OK with the changes and resulting work.

Related, translating CMMC and 800-171 to 800-53 is messy. It would far better if we just had a list of 800-53 controls that we had to meet.

Other general comments about NIST SP 800-1712r are:

- Merge 800-171A into 800-171. Similarly, merge 800-172 and 800-172A. Using two documents to get the full information is wasteful of time. It makes much more sense to have everything in together, similar to the presentation in the CMMCv2 level 2 assessment guide (https://www.acq.osd.mil/cmmc/docs/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf).

- For the items listed in Appendix E as NFO, while it might seem obvious that organizations will do these items, it is better to be explicit. See the general comment above. You mention this as an option in your call for comments 7b (https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft#_ftn1).
- Related to the prior item, explicitly require the existence and approval of a policy and a set of procedures/practices to implement the policy. Provide guidance (in the discussion section?) on the level of detail required; we have seen examples ranging from so vague as to be unusable to so detailed that they must be updated every time the software is patched.
- Please add supply chain risk management (SCRM) requirements to the 800-171r3.
- It would help us if 800-171 was clear about if an employee-signed Acceptable Use Policy (AUP) or a Privileged AUP (PAUP) is required. Different sources provide different answers on if an AUP is absolutely required, or if the items that it addresses could be met through alternate means (such as policy, procedures, and/or training). Specifically, our DIBCAC assessors required a PAUP, but the absolute requirement for this was not clear, and we covered the material in role-based security training combined with demonstrating knowledge through a quiz.
- Please change the control labels (numbers) so they sort properly. For example, currently 3.1.1 is followed by 3.1.10 and all of the other 3.1.1x, then 3.2.2 is followed by 3.2.20 etc. This sorting problem could be remedied by using leading 0s where necessary such as changing 3.1.1 to 3.01.01. However, any labeling method that will sort properly is OK.
- Zero Trust Architecture is coming, but it cannot be instantly implemented. Start covering the prerequisites for ZTA such as requirements for authentication in a multi-cloud environment.
- 800-171r2 barely mentions cloud computing (3.01.20, 3.03.01, and 3.13.15), which is a major part of how many businesses operate today. Cloud services such as M365 GCC-High are in-scope for CUI processing, yet the exiting controls barely acknowledge this. The different forms of clouds (IaaS, PaaS, SaaS, etc.) are each different in terms of how we need to apply security controls to them. Nowhere in 800-171r2 does it mention the concept of a {customer,cloud} (shared) responsibility matrix (often called a CRM or SRM) that covers what the cloud service provider (CSP) covers in their cloud and what the customer must ensure is covered. Unfortunately, our experience is that most CSPs are clueless. The few that understand often require an NDA or other hoops to jump through just to get a copy of the matrix (can NIST do anything about this problem?).
- We understand the necessity for non-IT controls such as protecting paper media, and physically protecting digital media, other physical security controls, and personnel protection. However, the mixing of these (in particular 3.08.01 requires physical protection but it not under physical protection in section 3.10) makes it harder to split the responsibilities between IT and the people responsible for non-IT portions.
- In order to make our vulnerability assessments easier to perform on vendor-supplied software, please consider requiring a software bill of materials (SBOM). The SBOM needs to be in a standard machine-readable format and integrated into the software package or executable so we can automatically scan for known vulnerable executables and libraries (such as Log4j). Currently, this scanning is hit or miss, mostly miss.

- Please address IoT, SCADA, and related industrial control technologies either in 800-171r3 or a separate document. In 800-171r3 is preferred, because the requirements will be immediately required to be addressed. On the other hand, our experience is that these technologies are a security disaster and addressing their problems might not be feasible through a change to 800-171r3.

Specific 800-171r2 controls

- 3.01.01, split out devices into a separate control. User and process identification is effectively covered by all modern OSs assuming that they are well-configured (so this control is necessary). Device identification is normally covered by completely different technologies, such as Active Directory system entries, PKI, etc.
- 3.01.03, Before information flow control policies can be defined, you must first identify what information flow(s) is(are) expected and acceptable. We run into pushback from project managers who do not want to spend the time required to identify the expected flow which makes the sysadmin's job easier in helping to enforce this. Therefore, an objective before 3.01.03[a] should be something like: Acceptable (or approved) information flows are identified.
- 3.01.13 requires protecting CUI in motion. But 3.13.08 also requires this. And, effectively, the "transmit" part of 3.5.10. Merge these two (or more) controls into one similar to 3.13.16. It could be parallel by making the control "Protect the confidentiality of CUI in motion.". The discussion can then cover the various ways of protecting CUI in motion. [Our personal preference is to prohibit all unencrypted communication, but this might be overkill.]
- 3.01.18 How are mobile devices any different from laptops other than screen size? Mobile devices should be treated identical to any other computing device that can store, transmit, or process CUI.
- 3.04.08, please change "blacklist" and "whitelist" to "block list" and "allow list".
- 3.05.01, as with 3.01.01, please split devices into a separate control since they are identified through different technologies than users and processes are identified. The same could apply to 3.05.02, but that control seems to less need the separation.
- 3.05.03, simplify this control by requiring MFA everywhere. As the control is written, this is effectively the case.
- 3.05.04, in the discussion section, it is worth calling out that all versions of NTLM are subject to replay attacks. We are having a hard time killing this protocol; if NIST called it out as explicitly not allowed in the discussion for the control, it would help us remove its use.
- 3.05.07 and all of the other "password" controls need to better allow for passwordless authentication methods such as biometrics combined with a U2F (FIDO2) key. While we believe that passwords will be with us for a while, the fewer places they are used, the better. Please better support these other authentication mechanisms in the controls.
- 3.07.01 and 3.14.01 both appear to require patching. Please either merge these controls and objectives or better separate them in the control discussions. In other words, how is maintenance different from applying vendor patches?
- 3.07.04, Please add examples such as checking the cryptographic hash or (preferably) digital signature of all diagnostic and test programs and/or media. It is rare today to have separate media; instead the tools are downloaded when needed. We would not prohibit running an anti-

malware check of the resulting download (this is already covered by 3.14.05), but, since it is trivial to customize hostile code, the benefits of most anti-malware systems are small.

- 3.07.05, merge the MFA requirement into 3.05.03. The termination requirement is duplicated by 3.13.09. By expanding the discussion and assessment objectives, this control could be eliminated.
- If you add in a "Recovery" section similar to what was in CMMC v1.02, move 3.8.9 to that section so all backup requirements are near each other.
- 3.11.02 is part of 3.14.01 and should be merged into 3.14.01.
- 3.11.03 should reference the merged 3.14.01. Should it be moved to 3.14 to keep all of the maintenance/patching/vulnerability management in one place?
- 3.12.02, Vulnerability management and plans of action and milestones (POAMs) are unclear. Different federal agencies use POAMs differently, so the requirements that apply to organizations following 800-171 need to be clarified. Adding to the confusion, POAMs are implied or explicitly required in the following ways:
    - For required controls that are not yet met by the organization.
    - Tied into the regular risk assessment, where everything not mitigated or accepted should be a POAM.
    - For vulnerability management, where, for example, a vulnerability is known but the vendor has not yet produced patches or other updates that will address the vulnerability.

  The requirements for each of these items need to be defined. We recommend that NIST come up with three separate names for these and use a separate control for each item.

  Additionally, the information required in the NIST POAM template is too light to be useful. But solving the other problems listed for this control might also solve this issue.
- 3.13.04, all modern OSs (Windows, Linux, MacOS) prevent information transfer through all of the example methods (registers, cache memory, main memory) except storage devices (800-171r2 calls these "disk drives"; solid-state storage is the norm, so that term is obsolete). A properly patched OS (covered by 3.14.01) covers all of the threats presented in this control. Unless we get into IoT devices (a separate comment), is this control even necessary? If it is necessary, please address the differences between an up-to-date OS and applications and what you are trying to cover with this control. How does this control in the storage portion relate to 3.01.03?

  Some control, if not this one, needs to address information remanence and other "set visibility to zero" approaches to making information appear to be deleted when it is not really. 3.08.03 sort-of covers this. NIST should address the basic problem that many applications are poor at actually deleting data that is no longer needed unless you really intend to limit the requirement to that in 3.08.03.
- 3.13.08, see the comment for 3.01.13.
- 3.13.10, recommending or at least mentioning using a password manager would be good. Worth noting though is that few password managers use FIPS-validated cryptography (3.13.11), and few encrypt all data in the vault, two issues that affect that can or should be used.

If you are mentioning laws, executive orders, etc., please provide references for the ones you have in mind.

- 3.13.11, while probably out of scope for 800-171 updates, the FIPS validation system is broken. As written, FIPS 140-2 prohibits patching and encourages hiding vulnerabilities (https://en.wikipedia.org/wiki/FIPS_140-2#Reception), even though DIBCAC and CMMC assessors are allowing previously validated libraries to be patched and used.

  The fact that the FIPS validation process takes so long that a library is obsolete by the time it is validated also limits the usefulness. According to Wikipedia, even though 140-3 was approved in 2019, no validations are yet final shows a substantial problem with the FIPS program.

  Another problem with the FIPS requirement is that, for many vendors, turning on FIPS compliance also disables many features that improve security. For example, with some VPN software, FIPS compliance requires pre-shared keys for authentication (which does not scale), but non-FIPS allows certificates (that can be revoked in personnel actions and lost/stolen systems).
- 3.13.13 Please separate these into products that are actively supported (e.g., PDF) from those that are end of life and/or deprecated (e.g., Flash). Actively supported products present a lower risk than obsolete ones, and the control methods should also be different. Unsupported applications and technologies should be isolated (e.g. on a separate network with access controls limiting connections between systems with unsupported applications and systems with only supported software). The differences should be either clarified in this control or the control should be split into two controls, one for actively supported technologies that is more generic, and one for obsolete products (not just mobile code products, but including them) that requires additional risk assessments for using unsupported software. This second control would also apply to, for example, Internet Explorer.

  This control is notable for listing products by name, which means that, for example, if PDF is replaced by a newer technology (as Flash was replaced by JavaScript + HTML5), the discussion becomes less relevant.
- 3.13.14 How is VoIP different from any other data stream? If someone is discussing CUI, then the data stream must be protected, just like any other data stream containing CUI.

Challenges in using the CUI series

800-171 is strictly about confidentiality. What about the other two legs of the triad, integrity (especially data integrity) and availability (including disaster preparedness and recovery from attacks)? We can imagine the challenges of requiring integrity and availability without also getting complaints about the cost of compliance, but balance is required here.

The NIST SSP template is not useful except for the identification and overview sections (Sections 1 & 2). Any assessor will require details on how each control is satisfied for each OS and environment. Cloud services make section 3 of the NIST SSP template even less relevant. At a minimum, this portion of the SSP template needs to be a spreadsheet, and even that is challenging to maintain, especially In complex, heterogenous environments. (Do you want to start pushing OSCAL? But high-level tools for using it are still probably a few years out.)

The content in the Cybersecurity and Privacy Reference Tool for 800-171r2 (https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_171_2_0_0/home) is identical to the 800-171r2 content, and similarly, it is missing the content from 800-171A. The result is that the tool is not useful. The same comment above about merging 800-171 and 800-171A; applies here. Additionally, the text in this tool is missing paragraph breaks in the original document.