From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments - Jacob Horne
Date: Friday, January 26, 2024 10:18:31 PM
Attachments: Jacob Horne - 171r3 FPD Comments.docx
Jacob Horne - 171r3 Comment Matrix.xlsx

Greetings,

Please find my comments on the FPD of SP 800-171 and 171A attached.

Thanks,
Jacob Horne

Thank you for the opportunity to comment on the final public drafts of SP 800-171 and 171A revision 3.

Compared to previous revisions, both documents represent significant improvements.

However, there are three specific issues that I urge NIST to consider carefully in relation to improving understandability and usability of both documents:

1) The ORC tailoring category must be eliminated.
2) Individual 800-53 control items should retain the same tailoring category as the overall control.
3) The use of conjunctions to combine multiple controls, enhancements, and control items makes harms usability and adoption.

The ORC tailoring category must be eliminated.

The elimination of the NFO tailoring category is an extremely helpful and makes SP 800-171 much easier to use.

However, the creation of the ORC tailoring category is mistake that holds SP 800-171 back.

The tailoring decision tree should begin with deciding whether a given control from the SP 800-53 moderate baseline is a FED control or not.

Then, for each of the remaining controls in the moderate baseline that are not FED controls, a decision should be made whether the control is directly related to protecting CUI confidentiality (CUI) or not (NCO).

The primary problem with the ORC category is that it does not indicate whether the control is directly related to protecting CUI confidentiality or not. It seems necessary to assume that because ORC controls are not categorized as NCO, then they must be directly related to protecting CUI confidentiality.

This creates several difficulties during both implementation and verification.

First, the ORC controls are not sufficiently addressed by the control as indicated in the SP 800-171 revision prototype overlay. Simply comparing the corresponding 800-53A determination statements for the various controls immediately shows that the controls are distinct in nearly every case.

It's commendable that NIST would respond to public comment on the 171r3 IPD about the level of redundancy among various requirements. However, it seems clear that most of those public

comments pointed to redundancy without sufficient understanding the corresponding SP 800-53 controls from which the requirements are derived.

Almost by definition the controls within a given control family are highly related but that does not mean that they are redundant. Similarly, SP 800-53 documents many inter-family control relationships that do not constitute redundancy.

When control and enhancements are deemed redundant, the combination of controls should be reflected in SP 800-53 revisions and then in SP 800-171 revisions. Given that SP 800-53 was recently updated to revision 5 I find it astonishing that NIST would claim that 19 controls and enhancements are suddenly redundant.

Second, without clear direction that ORC controls are not directly related to protecting the confidentiality of CUI (thus categorized as NCO), implementers must assume that the items within those controls are directly related.

In situations where external, independent verification is used (such as DoD's CMMC program) it is obvious that verification teams will seek to check the ORC control items via ORC determination statements.

As you will see in the attached comment matrix, there is no way to verify that controls like PS-6 or PS-7 are addressed by SA-9. Nothing in SA-9 inherently addresses those items no matter how closely related the controls happen to be.

Suggestion: NIST must eliminate the use of the ORC category and categorize all ORC requirements in the FPD as either FED, NCO, or CUI.

Individual 800-53 control items should retain the same tailoring category as the overall control.

Perhaps the most puzzling aspect of the FPD are the numerous examples of individual control items within a CUI control being categorized as NCO.

With rare exception, the decision to tailor individual control items out of a CUI control make the resulting 171r3 requirement more less precise, more difficult to understand, and harder to use.

In some situations, such as IR-8, numerous critical elements of the control are tailored out of the final requirement. Deciding that an Incident Response Plan is directly related to protecting CUI confidentiality but the definition of a reportable incident or reviewing and approving the plan are not directly related is difficult to understand logically.

How can it be that AC-22 is categorized as a CUI control and reviewing content on a publicly available system for non-public information *after* posting is directly related to protecting CUI confidentiality, but reviewing proposed content ***before*** posting publicly is not directly related?

When customers use SP 800-171 and inevitably have questions, they should and do reference the corresponding 800-53 controls for a given requirement.

When multiple items in a source control are clearly important, if not critical, people must make a decision (or attempt to make a case to decision makers) about implementing control items that are not specified as requirements.

This recreates the same mistakes as the NFO tailoring category. Categorizing individual control items differently from the overall control blurs the line between assumption and specification.

Suggestion: NIST should categorize individual control items differently from the overall control only extremely limited circumstances. Where a control item tailoring decision is made that differs from the parent control, NIST must provide the reasoning for the decision. Simply populating a table with tailoring acronyms is not sufficient.

The use of conjunctions to combine multiple controls, enhancements, and control items into single requirement statements harms usability and adoption.

Almost any time a requirement contains the word “and” there will be multiple corresponding determination statements in SP 800-171A.

Due to the general lack of familiarity with SP 800-171A and requirements decomposition in general, the discovery of n+1 determination statements in SP 800-171A leads to the popular idea that 171A materially expands the requirements in SP 800-171.

This creates unnecessary confusion, delay, and inaction. In many cases, the idea of 171A expansion forms the premise of arguments against the use of 171A or independent verification at all.

Suggestion: NIST should reverse the numerous decisions to combine base controls and enhancements into individual requirements. If those controls and enhancement aren’t combined in SP 800-53, then they should not be combined in SP 800-171.

Thank you again for the opportunity to comment.

Assuredly,
Jacob Horne

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Jacob Horne	General (Tailoring)	171r3 FPD	79	2893	AC-2(4) is not adequately addressed by AC-11	Categorize AC-2(4) as CUI, NCO, or FED
2	Jacob Horne	General (Tailoring)	171r3 FPD	80	2893	AC-18(1) is not adequately addressed by AC-18, IA-02, IA-02(01), IA-02(02), IA-03, SC-08, SC-08(01)	Categorize AC-18(1) as CUI, NCO, or FED
3	Jacob Horne	General (Tailoring)	171r3 FPD	82	2901	CM-4(2) is not adequately addressed by CA-02, CA-07	Categorize CM-4(2) as CUI, NCO, or FED
4	Jacob Horne	General (Tailoring)	171r3 FPD	82	2901	CM-7(2) is not adequately addressed by AC-03, AU-06, CM-02, CM-03, CM-05, CM-06, CM-07, CM-07(05)	Categorize 7(2) as CUI, NCO, or FED
5	Jacob Horne	General (Tailoring)	171r3 FPD	82	2901	CM-11 is not adequately addressed by AC-03, AU-06, CM-02, CM-03, CM-05, CM-06, CM-07, CM-07(05)	Categorize CM-11 as CUI, NCO, or FED
6	Jacob Horne	General (Tailoring)	171r3 FPD	83	2904	IA-5(6) is not adequately addressed by IA-05, PE-03	Categorize IA-5(6) as CUI, NCO, or FED
7	Jacob Horne	General (Tailoring)	171r3 FPD	87	2918	PS-6 is not adequately addressed by SA-9	Categorize PS-6 as CUI, NCO, or FED
8	Jacob Horne	General (Tailoring)	171r3 FPD	87	2918	PS-7 is not adequately addressed by SA-9	Categorize PS-7 as CUI, NCO, or FED
9	Jacob Horne	General (Tailoring)	171r3 FPD	88	2922	RA-5(5) is not adequately addressed by AC-06, AC-06(01), AC-06(05), AC-06(07), AC-06(09), AC-06(10), AU-09(04)	Categorize RA-5(5) as CUI, NCO, or FED
10	Jacob Horne	General (Tailoring)	171r3 FPD	88	2922	RA-7 is not adequately addressed by CA-05, CA-07, SR-03	Categorize RA-7 as CUI, NCO, or FED

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
11	Jacob Horne	General (Tailoring)	171r3 FPD	88	2924	SA-11 is not adequately addressed by CA-02, CA-07, CM-04, SI-02, SR-05, SR-06	Categorize SA-11 as CUI, NCO, or FED
12	Jacob Horne	General (Tailoring)	171r3 FPD	88	2924	SA-15 is not adequately addressed by SA-04, SR-03, SR-05, SR-06	Categorize SA-15 as CUI, NCO, or FED
13	Jacob Horne	General (Tailoring)	171r3 FPD	89	2926	SC-2 is not adequately addressed by AC-02, AC-02(03), AC-02(13), AC-03, AC-04, AC-05, AC-06, AC-06(01), AC-06(02), AC-06(05), AC-06(07), AC-06(09), AC-06(10), AU-09(04), CM-07, SC-07(03), SC-07(05)	Categorize SC-2 as CUI, NCO, or FED
14	Jacob Horne	General (Tailoring)	171r3 FPD	89	2926	SC-7(3) is not adequately addressed by CM-07, SC-07(05)	Categorize SC-7(3) as CUI, NCO, or FED
15	Jacob Horne	General (Tailoring)	171r3 FPD	89	2926	SC-7(4) is not adequately addressed by AC-04, AC-17(03), SC-07, SC-07(05)	Categorize as SC-7(4) CUI, NCO, or FED
16	Jacob Horne	General (Tailoring)	171r3 FPD	89	2926	SC-7(7) is not adequately addressed by AC-04, AC-17, AC-17(03), AC-17(04), CM-06, CM-07, SC-07(05)	Categorize as SC-7(7) CUI, NCO, or FED
17	Jacob Horne	General (Tailoring)	171r3 FPD	89	2926	SC-7(8) is not adequately addressed by SC-07(05)	Categorize as SC-7(8) CUI, NCO, or FED
18	Jacob Horne	General (Tailoring)	171r3 FPD	89	2928	SI-8 is not adequately addressed by SC-07, SI-03, SI-04	Categorize as SI-8 CUI, NCO, or FED

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
19	Jacob Horne	General (Tailoring)	171r3 FPD	90	2930	SR-12 is not adequately addressed by MP-06	Categorize SR-12 as CUI, NCO, or FED