From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Feedback
Date: Tuesday, January 16, 2024 11:22:39 AM
Attachments: sp800-171Ar3-ipd-comment-template.xlsx
sp800-171r3-fpd-comment-template.xlsx

Please see my feedback as requested.

Thank you,
Jake Williams

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Jake Williams	Technical	Source publication	15	478	This use of external systems should only be related to using CUI on external systems. If CUI is not being processed, stored, or transmitted, then the usage of external systems should not be part of this. As written, a corporation could require users to require authorization to use their personally owned devices that are not connected to the organizational system under A.03.01.20.a. Note that AC-20(a)(2) mentiones "organization-controlled information" as the focus of this control. Since 800-171 is focused on CUI, this should be the only data that is focused on.	Change title to "Use of CUI on External Systems"
2	Jake Williams	Technical	Source publication	16	517	AC-22c from 800-53 rev5 has been left out of this FPD, which would require authorized users to review content prior to posting. This is more important than AC-22d to prevent the posting of CUI in the first place. It's more important to review data prior to posting than to review it after it has been posted.	Add AC-22c as new section b and move existing section b to a new section c.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
3	Jake Williams	Technical	Source publication	28	1003	In the tailoring for 03.05.02, the ODPs from 800-53 rev 5 IA-3 were removed which expands the requirement. In this document, all devices must be identified and authenticated before access to the system, without determining if it is local, remote, or a network connection. In 800-171 rev 2, 3.5.2 had a lot more flexibility with the "or" statements to allow companies to determine what they wanted to authenticate prior to allowing access.	Add ODPs back in to match 800-53 rev5 so companies can define which devices require this identification and authentication.
4	Jake Williams	Technical	Source publication	35	1237	The title for section 3.7.4 is no longer focused solely on maintenance tools now that section (d) was added.	Rename section 3.7.4 to something more broad, such as "Maintenance Tools and Equipment"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
5	Jake Williams	Technical	Source publication	38	1354	MP-3(b) was tailored out from 800-53 rev5. This allowed for certain media to remain unmarked if it stays within a defined area (such as a room with physical controls on it) but the FPD tailoring this out requires all media to be marked, regardless of location. The clearest example of this is that "system media" includes drives installed in systems (such as in servers or desktops), where "removable media" is that which can be easily removed.	Add MP-3b back to 03.08.04 to give organizations the flexibility to determine what types of media are not required to have markings in specific areas.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
6	Jake Williams	Technical	Source publication	43	1567	The ODP was removed from 800-53 rev 5, which expands the requirements under 800-171 past the amount needed to protect CUI. If a company has an enclave for handling CUI, not all of their facility may be in scope for 800-171. This requirement as written expands the 800-171 controls outside of that enclave to everywhere in the facility, regardless of whether or not the distribution and transmission lines handle CUI. In addition, this should only apply to areas where CU is transmitted unencrypted. If the CUI is encrypted in line with other controls, then the lines should not need to be monitored. One example is shared office space, where the landlord and their staff along with the ISP will have access to areas that cannot be controlled by the tenant.	Add the ODP from 800-53 rev 5 PE-4 into 03.10.08[a] so companies can define the scope that needs to be protected.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
7	Jake Williams	Technical	Source publication	44	1606	Since the requirement includes remediation in 3.11.2b, the title should be updated to "Vulnerability Monitoring, Scanning, and Remediation".	Update title to "Vulnerability Monitoring, Scanning, and Remediation"
8	Jake Williams	Technical	Source publication	47	1688	The discussion lists additional types of agreements that could be in place, but these are not all listed in the text of the control.	Add "or other agreements" to the end of the selection list in (a).

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
9	Jake Williams	Technical	Source publication	49	1771	In 800-171 rev 2, SC-08 and SC-28 mapped to separate controls (3.13.8 and 3.13.16). By combining these into a single control and removing the ODPs from 800-53 rev 5, you have removed the option for companies to protect confidentiality via physical controls or alternative controls - encryption is a requirement at any point. In 800-171 rev 2 3.13.8 "alternative physical safeguards" were allowed, which my company and others used to not require encryption within the boundary of our building or network (ie if the transmitted data did not leave our local network, or if it was being held in a controlled room). The discussion for 800-53 rev 5 SC-8 discusses the use of physical controls for classified data, and CUI is less controlled than classified data. In 800-53 rev 5, SC-28(1) specifically has ODPs to determine what components or media require cryptography of data at rest. This	Include the first ODP from SC-28(1) so organizations can define with components or media need encryption at rest.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
10	Jake Williams	Technical	Source publication	55	2007	The discussion for 3.14.8 does not match the discussion for SI-12. It appears to be an attempt to reword it to be specific to CUI in nonfederal organizations, but is very unclear. There are no federal retention requirements for CUI from NARA, so this does not make sense as a requirement for safeguarding CUI. See the question in the Archives CUI FAQ related to retention at http<s>://www.archives.gov/cui/faqs.html	SI-12 should be tailored to NCO.
11	Jake Williams	Technical	Source publication	56	2043	The SSP is a description of a private company's implementation of security. As such, it is not legally required to be protected.	Remove 3.15.2c
12	Jake Williams	Technical	Source publication	59	2152	The SCRMP is a description of a private company's implementation of their processes. As such, it is not legally required to be protected.	Remove 3.17.1c
13	Jake Williams	Technical	Source publication	76	2796	The term "periodically" is not defined in 800-171. As such, a company could define their "period" to be every 10 years and it would still meet the legal definition.	If "periodically" continues to be used instead of redefining as ODPs, define "periodically" with a maximum timeframe of one year under 800-171.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
14	Jake Williams	Technical	Source publication	80	2894	AC-18(03) would be included in the other requirements for least functionality - either A.03.04.02.ODP[01] or A.03.04.06.ODP[04]. There is no reason for wireless to be specifically called out when wired, bluetooth, or other technologies are not.	Mark this as ORC and remove 03.01.16.c.
15	Jake Williams	Technical	Source publication	80	2895	AT-04 (Training Records) is marked as NCO, yet training records are needed to prove that training has been done. Without requiring training records, a company can have training available to users ("provided") but not required and have no record of users having taken the training, but still meet the requirements of 03.02.01 and 03.02.02.	Add 03.02.03 requiring training records.
16	Jake Williams	Technical	Source publication	82	2903	CP-7 is tailored out as NCO, but if an alternate processing site does not follow CP-7c ("Provide controls at the alternate processing site that are equivalent to those at the primary site.") then the confidentiality of CUI may be compromised.	Tailor CP-7(c) in to require confidentiality of CUI at alternative processing sites, similar to how CP-9 was tailored in but limited to confidentiality of backups with CP-9(8).

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
17	Jake Williams	Technical	Source publication	83	2904	IA-05(06) was tailored out as ORC. It is unclear why this was marked as ORC rather than NCO. There are no controls which discuss protection of the authenticators, and no legal requirements to protect an authenticator at the same level as CUI.	Change tailoring decision to NCO.
18	Jake Williams	Technical	Source publication	84	2909	It makes no sense that MA-02 is NCO but the rest of the MA family is CUI. How can Controlling Maintenance be not applicable to the confidentiality of CUI, but the other portions of Maintenance be part of protecting the confidentiality?	Change the tailoring on MA-02 to be CUI not NCO.
19	Jake Williams	Technical	Source publication	86	2918	PS-7 was tailored from an explicit requirement in the IPD to an ORC in this version. I am unsure where other requirements would support this control being in place. Control 3.16.3 talks about external system services, but there is no requirement there for an external provider to notify an organization when a user leaves (PS-7d) which is the largest gap that is not covered by other controls.	Add 3.9.3 back in from the IPD, or include a requirement in 3.16.3 that explicitly calls out external system user accounts.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
20	Jake Williams	Technical	Source publication	87	2922	I strongly disagree with the decision to mark RA-7 as an ORC, since there is no requirement in 03.11.01 or 03.11.02 to respond to risk assessments. With no required risk response, companies will perform a risk assessment as required in 03.11.01 but are not required to take any steps to address the risk.	Change RA-7 from ORC to CUI, and add it back into the requirements.
21	Jake Williams	Technical	Source publication	89	2928	Setting SI-08 as ORC makes no sense, as there are no controls regarding spam protection or email flow elsewhere in 800-171 rev 3. This is either CUI or NCO, not ORC. Since a large amount of adversary activity is sourced through email, and that can lead to compromise of CUI, this should be set to CUI.	Change SI-08 from ORC to CUI and add it back into the requirements.
22	Jake Williams	Technical	Source publication	89	2928	Both SI-03 and SI-16 are in the moderate baseline, but SI-03 is CUI and SI-16 is NCO. Since these are both ways to protect the system, it seems like SI-16 should be ORC instead of NCO.	Recategorize SI-16 as ORC.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
23	Jake Williams	Technical	Source publication	90	2930	SR-08 has been marked as NCO, but this control is very important to protecting CUI when the supply chain is involved. Requiring notification from the supply chain of any actual or potential compromises ensures that the organization is aware of any potential adverse issues.	Recategorize SR-08 as CUI.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Jake Williams	General	17	825	This requirement should be renamed to "Use of CUI on External Systems" to match my feedback to the 800-171 rev3 FPD. The Assessment Objectives need to be updated to match the limitation to CUI.	Update A.03.01.20.ODP[01] to: "terms and conditions to be satisfied on external systems prior to allowing the processing, storage, or transmission on those systems by authorized individuals are defined." Update A.03.01.20.ODP[02] to: "security requirements to be satisfied on external systems prior to allowing the processing, storage, or transmission on those systems by authorized individuals are defined." Update A.03.01.20.a to: "the use of external systems to process, store, or transport CUI is prohibited unless the systems are specifically authorized." Update A.03.01.20.b[01] to: "the following terms and conditions to be satisfied on external systems used to process, store, or transport CUI prior to allowing the use of or access to those systems by authorized individuals are established: <A.03.01.20.ODP[01]: terms and conditions>. " Update A03.01.20.b[02] to: the following security requirements to be satisfied on
2	Jake Williams	General	18	866	As per my comments in the FPD, there is a missing requirement from AC-22.	Add AO to match the suggested update to 800-171 rev 3 FPD.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
3	Jake Williams	General	34	1431	There is no information about how to identify high risk areas, or who in the orgnization should identify high-risk areas.	Add "A.03.04.12.c: periodically review and update the list of organizationally-defined high-risk locations." Unless ODPs are re-implemented instead of the word "periodically" then add an ODP as well.
4	Jake Williams	General	35	1478	See comments in the 800-171 rev3 FPD form regarding the tailoring of IA-3.	Add ODPs to the Assessment Objectives.
5	Jake Williams	General	47	1919	See comments in the 800-171 rev3 FPD form regarding the tailoring of MP-3.	Add ODPs to the Assessment Objectives.
6	Jake Williams	General	55	2191	See comments in the 800-171 rev3 FPD form regarding the tailoring of PE-4.	Add ODPs to the Assessment Objectives.
7	Jake Williams	General	63	2461	See comments in the 800-171 rev3 FPD form regarding the tailoring of SC-28(1).	Add ODPs to the Assessment Objectives.