From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Review Comments - 800-172r3 IPD
Date: Wednesday, December 18, 2024 1:47:32 PM
Attachments: 800-172-Rev3-241113-ipd-comment-DPF241217.xlsx

Here are some initial review comments.

--

Daniel Faigin, CISSP (He/Him, Pacific Time Zone)
Senior Engineering Specialist, The Aerospace Corporation
Cyber Engineering Department (CED) 5832/Cybersecurity and Advanced Platforms Subdivision (CAPS)

[redacted]

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Daniel Faigin The Aerospace Corporation	Technical	9	421	To what extent is this duplicative with other dual-authorization controls -- in other words, completing this could make the others redundant.	To fix this, consider narrowing the scope of the assignment.
2	Daniel Faigin The Aerospace Corporation	Technical	10	440	The phrase "to process, store, or transmit CUI" is problematic in the sentence, and makes the control hard to read.	How about "Restrict the ability to use … to … using …". The problem is "the use of …" is an awkward English construction.
3	Daniel Faigin The Aerospace Corporation	Technical	10	441	The assignment isn't restrictions; it appears to be restriction mechanisms.	Correct the domain of the assignment to be restriction mechanisms, and reword to make the clear in the introduction to the assignment (e.g., "using the following restriction mechanisms: [assignment…]").
4	Daniel Faigin The Aerospace Corporation	Editorial	11	464	When you have assignments, think in your head how the control might sound when completed.	In this case, it might sound better as "for the following accounts or account types", and move that assignment to the end of the control.
5	Daniel Faigin The Aerospace Corporation	Technical	11	481	"…to monitor and control…". With phrases like this, the question becomes: To monitor for what? What is being controlled? If this were turned into a requirement, how would you know it was being met.	Be clear in the control what is being monitored, and clarify what is being controlled.
6	Daniel Faigin The Aerospace Corporation	Technical	12	511	In this control, there are some implications for AU-02 and AU-12 that should be mentioned in the discussion.	Discuss the impact of this control on the completion of the assignment for auditing.

7	Daniel Faigin The Aerospace Corporation	Editorial	13	539	It might be better to word this as "enforce the following attribute-based access control policy …", as that gives more flexibility in specifying the policy.	
8	Daniel Faigin The Aerospace Corporation	Editorial	14	564	Move the assignment to the end, e.g., "the following information flow policies as a basis for flow control decisions: [assignment]"	
9	Daniel Faigin The Aerospace Corporation	Editorial	15	594	Swap items 2 and 3, so you can move the assignment to the end of the of 2, and use "the following".	
10	Daniel Faigin The Aerospace Corporation	Technical	16	619	It might be good to add metrics to this, and to monitor them to improve them, which would also support CSF2.0 subcategories.	
11	Daniel Faigin The Aerospace Corporation	Technical	16	635	For feedback, there needs to be metrics on the effectiveness of training.	
12	Daniel Faigin The Aerospace Corporation	Technical	17	665	This should discuss the permissibility of storing a copy in the physically separate system, such as using syslog to send audit to a remote system, in addition to the local copy. As worded now, this might preclude a local copy, which could result in loss of audit records if connectivity is lost.	
13	Daniel Faigin The Aerospace Corporation	Technical	18	686	Give some examples of alerts. Of particular interest, based on the NDcPP experiences, are running out of audit space, and inability to communicate with audit storage in the separate environment.	

14	Daniel Faigin The Aerospace Corporation	Technical	18	707	Note also the connection to 03.01.01E	
15	Daniel Faigin The Aerospace Corporation	Technical	20	747	This may be a broader comment, but don't bury requirements in the domain of the assignment (in this case, the requirement for automation). Make it clear by using a construction like "…using the following automated mechanisms: [assignment]".	
16	Daniel Faigin The Aerospace Corporation	Technical	21	774	This is another example of what I call "burying the lede": hiding the requirement in the domain of the assignment. Reword this to make the requirement for automation clear in the control text (…using the following automated mechanisms…).	
17	Daniel Faigin The Aerospace Corporation	Technical	21	800	Again, this is "burying the lede": hiding the requirement in the domain of the assignment. Reword this to make the requirement for automation clear in the control text (…using the following automated mechanisms…).	
18	Daniel Faigin The Aerospace Corporation	Technical	22	832	Note connection to 03.01.01E	
19	Daniel Faigin The Aerospace Corporation	Technical	23	855	Be more specific in the control: (1) Is testing on the operational system or a mirror (make that a selection); (2) make it clear that the last clause applies to the operational system.	

20	Daniel Faigin The Aerospace Corporation	Technical	24	881	Note that the specifics of the protocols and algorithms would be specified in SC-13. Is it worth mentioning CNSA 2.0?	
21	Daniel Faigin The Aerospace Corporation	Editorial	25	914	Font problems.	
22	Daniel Faigin The Aerospace Corporation	Technical	25	918	"Attestation is used to enforce…a trust profile": Where is the minimum required attestation defined -- that is, to what is the minimum that the device must attest?	
23	Daniel Faigin The Aerospace Corporation	Technical	27	982	What is the required connection between the SOC and the system under assessment? If there isn't one, then how does the SOC enhance security for *this* system? If there is one, it should be specified in the control.	
24	Daniel Faigin The Aerospace Corporation	Technical	29	1039	This is another "OK, now what?" control: So you analyze the behavior. Then what? There should be some associated action. Report to SOC? Notify someone? Do something?	
25	Daniel Faigin The Aerospace Corporation	Technical	29	1056	Should there be a connection here with the SOC?	
26	Daniel Faigin The Aerospace Corporation	Technical	30	1071	Are these updates and patches installed in the tool, or in the system? Right now, the control is ambiguous.	
27	Daniel Faigin The Aerospace Corporation	Technical	30	1085	Note the connection to 03.01.01E	

28	Daniel Faigin The Aerospace Corporation	Technical	31	1111	Note the connection to 03.01.01E	
29	Daniel Faigin The Aerospace Corporation	Technical	31	1111	How does this work in relationship to automatic backup schemes, such as those that only keep "n" prior versions, or that do incremental backups.	
30	Daniel Faigin The Aerospace Corporation	Technical	33	1176	For this control, and the similar one earlier, consider an assignment for other access requirements. The discussion makes clear that this is a "may" (see line 1179) -- meaning in some cases it may be reasonable for a non-citizen to have access. On the other hand, the discussion could be incorrect -- in which case, the discussion should be fixed to be consistent with the control.	
31	Daniel Faigin The Aerospace Corporation	Technical	34	1195	There's an interaction here with privacy. Do these records need to be trated as PII? What other rules come into play? Consider adding a (d) Protect visitor access records as PII.	
32	Daniel Faigin The Aerospace Corporation	Technical	34	1195	This should provide clarification on what constitutes an anomaly.	
33	Daniel Faigin The Aerospace Corporation	Technical	35	1209	"Monitor physical access…". Why are you monitoring? Include the purpose in the control, and what should be done if a problem is noted.	
34	Daniel Faigin The Aerospace Corporation	Technical	35	1227	"Authorize and control…". Are there any specific notions of control that can be given as examples?	

35	Daniel Faigin The Aerospace Corporation	Technical	38	1319	For all the withdrawn items, it would be better to keep the original title, and move "withdrawn" to the discussion, and possibly a "(Withdrawn)" added to the title. As it is now, there is no real content or context.	
36	Daniel Faigin The Aerospace Corporation	Technical	38	1328	Again, this buries the lede in the domain of the assignment. Consider "…using the following means: [assignment]".	
37	Daniel Faigin The Aerospace Corporation	Technical	39	1344	Again, this buries the lede in the domain of the assignment. Consider "…using the following sources: [assignment]".	
38	Daniel Faigin The Aerospace Corporation	Technical	40	1370	This buries the lede in the domain of the assignment. Consider "…at the following points in the SDLC: [assignment]".	
39	Daniel Faigin The Aerospace Corporation	Technical	40	1374	"For example, …": How is the rest of the sentence an example?	
40	Daniel Faigin The Aerospace Corporation	Technical	41	1411	This should mention the AC family control that deals with what information is public.	
41	Daniel Faigin The Aerospace Corporation	Technical	41	1427	Is any automated mechanism acceptable? Is there a minimum level of automation required?	
42	Daniel Faigin The Aerospace Corporation	General	44	1507	Why are these sometimes hyperlinked and sometimes not?	

43	Daniel Faigin The Aerospace Corporation	Technical	44	1515	This buries rquirements -- specifically, that compliance, effectiveness, and change monitoring are are of continuous monitoring. Instead, reword this as "Implement a continuous monitoring strategy that includes risk monitoring, effectiveness monitoring, compliance monitoring, and change monitoring"	
44	Daniel Faigin The Aerospace Corporation	Technical	45	1561	"…technologies for the…". Is it "for" or "in" or both?	
45	Daniel Faigin The Aerospace Corporation	Technical	45	1565	What is the acceptable minimum diversity?	
46	Daniel Faigin The Aerospace Corporation	Technical	46	1581	This is poorly written, and will confuse people. Into which component or operations? What is acceptable randomness?	
47	Daniel Faigin The Aerospace Corporation	Technical	47	1603	Consider moving this before 03.13.02E	
48	Daniel Faigin The Aerospace Corporation	Technical	48	1644	Is this mandatory or optional? In general, it might be good to have an indication (e.g., (M), (O)) for ESRs that should be present in all systems with a need for enhanced protection (M), or ones that can be optionally added (O).	
49	Daniel Faigin The Aerospace Corporation	Technical	50	1723	This needs to be reworked to put the assignment at the end.	

50	Daniel Faigin The Aerospace Corporation	Technical	56	1893	The discussion doesn't discussed the difference between refresh and generate.	
51	Daniel Faigin The Aerospace Corporation	Technical	59	2005	This may be impossible for *all* error messages, so there needs to be a way to scope it down.	
52	Daniel Faigin The Aerospace Corporation	Technical	59	2005	There may also be an issue of who can see what details -- for example, it might be OK to show more information to administrators. I'd suggest something like "show appropriate information for the role", but that then raises the question of how to define what is appropriate.	
53	Daniel Faigin The Aerospace Corporation	Technical	60	2026	Note: I like that you've gone back to "safeguards". Use of "controls", as was done in 800-53r5.1, implies use of specific controls from the catalog, which I don't believe was the intent.	
54	Daniel Faigin The Aerospace Corporation	Technical	62	2077	"…if organizational data…": All data? Specific data items? Consider an assignment here.	
55	Daniel Faigin The Aerospace Corporation	Technical	63	2130	Give some examples of the automated mechanisms contemplated.	
56	Daniel Faigin The Aerospace Corporation	Technical	65	2186	What about Zero Trust architectures?	

57	Daniel Faigin The Aerospace Corporation	Technical	66	2232	The discussion needs to describe the differences between each of the various optiosn in the assigment, and the strengths and weaknesses of each. Don't assume that readers are familiar with the nuances of these terms.	
58	Daniel Faigin The Aerospace Corporation	Technical	67	2255	"…organization-defined information": Any, or just CUI?	