From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments on 800-171 Rev 3
Date: Friday, July 7, 2023 3:51:26 PM
Attachments: 800-171-Rev3-230510-ipd-comment-template.xlsx

Here are some comments on 171.

(Note that I'm doing my deep dive review on Rev 5 for my tool. When done, I can share the updated guidance and such, as well as a set of controls we've identified as missing controls)

Daniel

--
Daniel Faigin, CISSP (He/Him, Pacific Time Zone)
Senior Engineering Specialist, The Aerospace Corporation
Cyber Operations & Resilience Department/Cybersecurity and Advanced Platforms Subdivision

Work @ El Segundo: [redacted]
Work @ Home: [redacted]
[redacted]
Mailing: The Aerospace Corporation MS M1/055 | P. O. Box 92957 | Los Angeles CA 90009-2957

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Daniel Faigin The Aerospace Corporation	Technical	Publication	3	63	I'm still concerned at the focus *only* on confidentiality. Even for CUI, integrity can be equally if not more important. Ron always used to give the example of blood types in a hospital database. There may not be a big impact from disclosing them. But there would be a life-threatening impact of someone was to come in and silently change them. This is essentially acknowledged in footnote 7 on page 7, where it is acknowledged this publication protects from both unauthorized disclosure and modification. As such, the assumptions later should be consistent with this footnote.	Add a minimum integrity level for the assumptions and baseline selections. Further, modify line 69 based on footnote 7, to indicate "Not directly relating to protecting the confidentiality or integrity of CUI". In general, unless we are specifically indicating protection *from disclosure* , the term protection should imply protection from disclosure and modification.
2	Daniel Faigin The Aerospace Corporation	Technical	Publication	6	164	I'm not sure about the inclusion of AC-17 as a reference here. There are other CUI requirements that cover remote access, and the requirement in 165/166 really focues on information, and not the type of access (and indeed, "system access" is only really addressed in the discussion, and not in the requirement text. "System resources" as used in the requirement text is really read more as devices, capabilities, functions, etc, and not the system itself.	Remove AC-17 as a reference, and remove system access from the discussion (or make it more explicit in the actual requirement text).
3	Daniel Faigin The Aerospace Corporation	Technical	Publication	9	276	Re: Log the execution of privileged functions. In actually, most of these requirements should produce some sort of log that they were done. So calling this one out in particular seems off. Instead, in the requirement that parallels AU-2/AU-3, make it clear that all controls should be producing some records.	The purpose of audit is accountability for actions and after the fact forensic analysis. This should be done for all cybersecurity related actions.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
4	Daniel Faigin The Aerospace Corporation	Technical	Publication	9	304	The mention of posters in the discussion made me realize that something was missing here: A requirement that the user acknowledge reading the system use banner (i.e., an OK button). As written here, the banner could be displayed for one second and the requirement would be met. To be effective, the banner must be read (and that's the problem with using posters or printed materials).	Require an acknowledgment of some form that the banner has been read.
5	Daniel Faigin The Aerospace Corporation	Technical	Publication	14	478	Mightn't there be something here relating to attestation – some confirmation that the external system is configured properly through exchanging of a digital hash or something like that.	This is common for mobile devices or VPNs: an examination that the system is configured properly and secure as part of connection establishment.
6	Daniel Faigin The Aerospace Corporation	Technical	Publication	21	766	Should consideration be given to including an SBOM as part of the configuration. Having this information improves the ability to perform vulnerability searches.	
7	Daniel Faigin The Aerospace Corporation	Editorial	Publication	25	927	There's an odd font change in item c.	
8	Daniel Faigin The Aerospace Corporation	Technical	Publication	27	1010	Consider as part of device authentication the inclusion of PKI and certificate revocation checking for the certificates exchanged as part of X509 authentication.	Many devices and services use X509 for authentication, yet PKI and certificate checking is not part of 171.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
9	Daniel Faigin The Aerospace Corporation	Technical	Publication	40	1515	With the post-pandemic use of telework, esp. for U and U//CUI work, I think the discussion here should be beefed up with respect to telework and the types of physical access controls and contingency planning (incident response) that should exist in the telework environment. For example, the next requirements discuss visitor access control, but what does that mean in a telework environment?	
10	Daniel Faigin The Aerospace Corporation	Technical	Publication	42	1577	There should also be an assessment of the risk of unauthorized modification of the CUI. Depending on the nature of the CUI, this could be an even greater risk to mission than disclosure.	
11	Daniel Faigin The Aerospace Corporation	Technical	Publication	43	1599	There should be a connection between vulnerability scanning and SBOMs … in particular, knowing the libraries and components that go into a piece of software can make vulnerability scanning for that software stronger.	
12	Daniel Faigin The Aerospace Corporation	Technical	Publication	49	1884	When referencing only enhancements, you should reference the base control as well as those are required for the enhancements.	
13	Daniel Faigin The Aerospace Corporation	Technical	Publication	79	3011	NCO, CUI: Again, integrity should be integrated into this.	
14	Daniel Faigin The Aerospace Corporation	Technical	Publication	83	3024	IA-5(2). Arguably, this should be in the CUI set, as it is often the basis for doing certificate revocation (which should be part of X509 and PKI based authentication).	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
15	Daniel Faigin The Aerospace Corporation	Technical	Publication	34	1272	MA-5 (and its enhancements) tends to focus on traditional access, clearances, and such. There needs to be some specific discussion regarding PII and CUI – in particular, regarding maintenance personnel and their authorization to access CUI and PII.	
16	Daniel Faigin The Aerospace Corporation	Technical	Publication	5	138	In the discussion for account management, have some words as to how this might be adapted to a zero-trust, on-demand account creation environment, as we are encouraging organizations to move to zero-trust models	
17	Daniel Faigin The Aerospace Corporation	Technical	Publication	27	1010	Consider modifying this to include service authentication (or adding a new category), giving the growing use of software as a service from a cloud.	
18	Daniel Faigin The Aerospace Corporation	Technical	Publication	40	1492	There should also be consideration to protecting the physical access logs from both disclosure and modification (based on similar requirements for the audit logs)	
19	Daniel Faigin The Aerospace Corporation	Technical	Publication	49	1867	In light of footnote 7, and the fact that the discussion references integrity, this should talk about transmission confidentiality and integrity (especially as most solutions will protect integrity as well).	
20	Daniel Faigin The Aerospace Corporation	Technical	Publication	55	2077	There should be something about protecting collected monitoring information (again, analagous to audit protection)	