From: '[redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: Mueller, James
Subject: [800-171 Comments] Comments on NIST SP 800-171r3 initial public draft
Date: Friday, January 26, 2024 11:07:13 PM
Attachments: image001.png
sp800-171r3-fpd-comments AWS Submission 01262024.xlsx

Dear NIST Personnel,

Attached are comments for NIST SP 800-171r3 initial public draft.

Regards,

Jim Mueller, CCSP, CSSLP, CISSP
Government Compliance Lead
[redacted]
Visit the RISE Wiki to Learn More.

aws

James Mueller / AWS Submission

Submit comments to 800-171comments@list.nist.gov
by January 26, 2024 (originally Jan. 12)

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Example R3 Identifier Reference	Comment (include rationale)*	Suggested Change*
1	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	45	03.04.10 + additional references security requirement narratives	A standard definition for the term 'component' is suggested to enable consistency and accuracy in the inventory management tracking. Incorrect classification by the organization could lead to missing, excessive, or unnecessary items in the inventory. Previous instances of NIST 800-171 requirements appeared to be more focused to on-premise solutions as opposed to cloud-based solutions and industry terminology.	Include the clear and concise NIST definition in a NIST 800-171 glossary and examples of components.
2	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	63	03.06.04	Recommend the organization should be allowed to determine the format of the incident response training. Examples could include webinars, written documentation, on-line or in-person training courses.	
3	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	120	03.14.08	A more specific definition of 'retention' could avoid confusion. Does retention refer to length of time, location, or both?	Include the clear and concise NIST definition in a NIST 800-171 glossary.
4	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	125	03.16.02	A standard definition for the term 'unsupported' is suggested to enable consistency and accuracy in implementation and assessment of the requirement along with examples. Confusion and inconsistent industry compliance could result as the term 'end-of-life' software/components could be confused as 'unsupported.'	Include the clear and concise NIST definition in a NIST 800-171 glossary.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Example R3 Identifier Reference	Comment (include rationale)*	Suggested Change*
5	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	126	03.16.03	A standard definition for the term 'external system services' is suggested to enable consistency and accuracy in implementation and assessment of the requirement along with examples. Without a clear and concise definition, confusion and inconsistent industry compliance could occur. The term such as 'managed service' is often used by providers and questions could arise whether a managed service is considered an external system service.	Include the clear and concise NIST definition in a glossary for NIST 800-171.
6	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	126	03.16.03 + additional references security requirement narratives	Is the usage of the term 'external provider' or 'external system provider' consistent throughout the requirement families? For example, does the use of these terms mean the same in the Supply Chain family as other requirement families throughout the document?	Include the clear and concise NIST definition in a NIST 800-171 glossary and examples.
7	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	21	03.01.20	Suggest more clarity in the definition of authorized users who are required to abide by the requirements. Does the requirement apply at the organization level, the individual user level, the administrative user, the external users/admins, or vendors?	Include the clear and concise NIST definition in a glossary for NIST 800-171.
8	James Mueller Amazon Web Services	Editorial	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	24	03.02.01	Is literacy training the correct requirement title? Or is the requirement related to training in a written format?	
9	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	27	03.03.01	Provide guidance on whether logs are considered CUI to enable consistency and accuracy in implementation and assessment of the requirement.	If meta-data is not considered CUI, please reference this distinction in the requirements documentation.

* indicate required fields

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Example R3 Identifier Reference	Comment (include rationale)*	Suggested Change*
10	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	61	03.06.02	Is meta-data considered CUI and does meta-data require the same security protections?	If logs are not considered CUI, please reference this distinction in the requirements documentation.
11	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	90	03.11.02	Are vulnerability scanning reports considered CUI and require the same security protections?	If vulnerability scanning reports are not considered CUI, please reference this distinction in the requirements documentation.
12	James Mueller Amazon Web Services	Editorial/Technical	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	107	03.13.11	Is the organization allowed to determine the cryptographic protection mechanism? The requirement states 'Implement the following types of cryptography' without identifying the allowed cryptographic protection types.	Recommend editorial changes to the requirement narrative.
13	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	114	03.14.02	The requirement as written states organization-defined frequency and real-time scans. Is the intent both or either?	Recommend editorial changes to the requirement narrative.
14	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	0	-	Recommend providing additional guidance on what requirements apply at the prime and/or subcontractor level. Clarify flow-down of obligations between DIB prime and sub-contractors could increase consistency and accuracy in the implementation and assessment of the NIST requirements.	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Example R3 Identifier Reference	Comment (include rationale)*	Suggested Change*
15	James Mueller Amazon Web Services	General	NIST SP 800-171 Rev. 3 (Final Public Draft)	1	0	-	With the DIB made up of hundreds businesses providing technology and professional services to all federal agencies, recommend NIST consider the impact on of medium and small size businesses and their ability to adopt the 800-171 requirements. Can accommodations be made for small service providers?	

* indicate required fields