From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] NIST SP 800-171 and NIST SP 800-171a Comments
Date: Tuesday, January 23, 2024 12:29:24 PM
Attachments: Outlook-qduzj5mw.png
Outlook-nke2rara.png
Archstone Security NIST SP 800-171- 800-171a Comments.xlsx

Attached, please find comments on both the NIST SP 800-171 and the NIST SP 800-171a.

Thanks again for all your hard work and the collaborative relationship NIST has with industry! I appreciate the opportunity to provide feedback for your consideration.

Karen Stanford

Archstone Security LLC, President

ARCHSTONE SECURITY

[redacted]

PO Box 287

Haymarket, VA 20169

http://archstonesecurity.com

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Karen Stanford/ Archstone Security	General	Analsys	All	All	You guys are doing a great job! Every iteration gets better and better.	
2	Karen Stanford/ Archstone Security	General	Publication	3	71	Because CUI isn't FISMA data, it doesn't get categorized. The FIPS 199 categorization requirements represented in NIST SP 800-53 were tailored out of 800-171, so confidentiality impact for CUI data is almost never categorized currently. NARA CUI categories do not list confidentiality levels in its marking guidance. Any CUI that has had its confidentiality ascertained is likely subject to 800-53 requirements, not the tailored 800-171 controls. My concern with leaving this in is that people can argue that their CUI was never categorized as having moderate confidentiality needs, so therefore, this publication is not applicable for them.	I think the simple assumption is that CUI requires confidentiality protections.
3	Karen Stanford/ Archstone Security	General	Publication	5	117-120	It may be worthwhile to suggest that the high watermark concept should be used here for organizations that have multiple standards to comply with.	Add, "When organizations are subject to multiple ODP requirements, the high-watermark standard of requiring the most stringent should be taken to fully facilitate compliance. "
4	Karen Stanford/ Archstone Security	General	Publication	7	107	Anything you could do with respect to the numbering format that would enable requirements to populate sequentially in Excel would be fantastic. The current numbering format is causing omissions and subsequent findings in practice (controls are being left out when converting to a different medium like Word)	If there are fewer than 26 subparts to any control maybe use letters instead of numbers.
5	Karen Stanford/ Archstone Security	General	Publication	10	299	"Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities."	Suggest adding "changing enterprise settings" to accommodate cloud technologies and security tools.
6	Karen Stanford/ Archstone Security	General	Publication	11	334-335	"Organizations consider whether a secondary use notification is needed to access applications or other system resources after the initial network logon."	I think this is missing a word, maybe "organizations should?" And if they should consider it, shouldn't they document their rationale in the SSP or something that's required to be reviewed annually so it could be revisited upon architecture changes? The vagueness here makes it difficult to test.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
7	Karen Stanford/ Archstone Security	General	Publication	11	345	"Retain the device lock until the user reestablishes access using established identification and authentication procedures." I think the word "established" should probably be changed to "authorized" for full clarity.	Suggest "Retain the device lock until the user reestablishes access using authorized identification and authentication mechanisms."
8	Karen Stanford/ Archstone Security	General	Publication	13	416	3.1.16. Wireless Access	Is FIPS-validated cryptography required for wireless? Lack of references here suggest it is not; however, products have emerged that provide it for wireless access points. Many wireless technologies do not offer FIPS validation. If FIPS validation of wireless is expected, some requirements should be articulated here.
9	Karen Stanford/ Archstone Security	General	Publication	15	478	3.1.20. Use of External Systems	External system usage got more complicated with work-from-home and this could be an opportunity for more guidance If usage of external systems is permitted, the boundary tends to get extended to the home unless the following are met: - forcing storage onto only CUI assets, prohibiting printing to any unauthorized printers - prohibiting the storage of CUI on removable media - ideally, logically, but at least by policy.
10	Karen Stanford/ Archstone Security	General	Publication	24	821-22	Part b, "disapprove such changes with explicit consideration for security impacts," seems redundant with Requirement 3.3.4, "Analyze the security impact of changes to the system prior to implementation."	Should the requirements to analyze and disapprove changes be combined into the same control vs. being present in both 3.3.3 and 3.3.4?

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
11	Karen Stanford/ Archstone Security	General	Publication	25	868	This wording in "3.4.6. Least Functionality" introduces a requirement in the nist SP 800-171 that differs than terminology used in NIST SP 800-53: "functions, ports, protocols, ***connections,*** and services." NIST SP 800-53 has consistently referred to "functions, ports, protocols, and services." Given that discrepancy between the language in the NIST SP 800-171 and NIST SP 800-53, can the requirement to document conections be assumed to be a requirement unique to CMMC? If so, FedRAMP reciprocity may become more challenging. The word "connection" is not currently defined in the NIST Glossary, so I'm uncertain as to what the intent there is, or if system interconnections are required or redundantly referenced here. Device identification and authentication is addressed in 3.5.2.	Evaluate if changes are required. Given the information in the description, it appears that the word connections is redundant. Bluetooth and wireless are services.
12	Karen Stanford/ Archstone Security	General	Publication	27	949-50	3.4.11 Document changes to the location (i.e., system or system components) where CUI is ***processed and stored.***	Add "transmitted" unless the intent is to remove firewalls, network devices, VPNs, etc. from the change control process for this requirement. Can we modify 3.4.10 to indicate that any components storing CUI should be designated as such in the inventory?
13	Karen Stanford/ Archstone Security	General	Publication	28	981	3.5.1. User Identification, Authentication, and ***Re-Authentication*** . The addition of "reauthentication" seems redundant, because of the requirements in session disconnect and network disconnect. How does this requirement differ from those controls? The NIST control this is derived from does not include ***"re-authentication;"*** this language seems unique to NIST SP 800-171.	Consider the removal of re-authentication or the incorporation into session/network disconnect requirements. Re-authentication and session disconnect seem connected.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
14	Karen Stanford/ Archstone Security	General	Publication	28	1064-1067	"3.5.7 A. Maintain a list of commonly-used, expected, or compromised passwords and update the list periodically and when organizational passwords are suspected to have been compromised." and "Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords." This requirement does not have a counterpart in NIST SP 800-53; which presents a challenge in reciprocity with a comparable control set; and is a new requirement with little technological support with standard products and cloud offerings.	I would prefer to not see this rolled out as a new requirement starting at the Federal contractor level without reviewing its incorporation at the Federal level first. The introduction of new requirements in the NIST SP 800-171 vs. the NIST SP 800-53 causes continuity problems for reciprocity between CMMC and FedRAMP.
15	Karen Stanford/ Archstone Security	General	Publication	33	1192-1194	**3.6.3. Incident Response Testing** REQUIREMENT: 03.06.03 Test the effectiveness of the incident response capability ***periodically.***	Should this be an organizationally-defined parameter?
16	Karen Stanford/ Archstone Security	General	Publication	38	1350-1351	3.8.4. Media Marking: REQUIREMENT: 03.08.04 Mark system media containing CUI to indicate distribution limitations, handling caveats, and security markings.	Suggest adding an organizationally defined parameter to indicate the authority for marking. Per NARA, not all of this is required for marking. Basic CUI can just be labeled as "CUI." There are often no distribution or handling instructions necessary. Recommend altering to state "system media that contain CUI are marked in accordance with NARA guidelines." Ostensibly, the requisite CUI category should be communicated from the Feds. I think the CUI data types should be defined and documented.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
17	Karen Stanford/ Archstone Security	General	Publication	43	1546	3.10.7. Physical Access Control **2. Controlling ingress and egress with physical access control systems/devices or guards.** Manufacturing facilities present some challenges here. The current NIST guidance related to physical security seem specific to office workspaces and data closets/centers; however, plants have significantly different architectures that may include large vents because there is no air-conditioning, barriers intended to block only vehicles, etc. This is the most challenging control to assess for manufacturing environments, and while the physical and envrionmental security best practices requirements are reasonable for standard IT environments, the cost of implementing those for manufacturing is extremely high.	Has NIST considered developing any guidance on workshop-floor physical security requirements?
18	Karen Stanford/ Archstone Security	General	Publication	43	1547	**3.10.7. Physical Access Control** **b. Maintain physical access audit logs for entry or exit points.** This also becomes challenging in manufacturing environments, where CUI may be present in external work lots on paper during stages of the manufacturing process. Not all manufacturing work is conducted inside. There are no references available to establish industry best practices for these requirements.	Has NIST considered developing any guidance on workshop-floor physical security requirements?
19	Karen Stanford/ Archstone Security	General	Publication	43	1565	3.10.8. Access Control for Transmission and Output Devices	"Output devices" can become challenging when the CUI is parts, not data. Can this be reworded to specific that the CUI requiring protection is data, not parts?
20	Karen Stanford/ Archstone Security	General	Publication	44	1587-1605	3.11.1. Risk Assessment	While the NIST S_ 800-53 has the 800-37 as a corollary guiding assessments, NIST SP 800-171 doesn't. As a result, there is no requirement to communicate recommendations as a result of an independent assessment. This lack makes POA&M remediation more challenging, as no specific recommendations have ever been made.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
21	Karen Stanford/ Archstone Security	General	Publication	45	1638	03.12.01 Assesss the security requirements for the system and its environment of operation ***periodically*** to determine if the requirements have been satisfied.	Should this be an organizationally defined parameter?
22	Karen Stanford/ Archstone Security	General	Publication	57	2066	3.15.3. Rules of Behavior c. Review and update the rules of behavior ***periodically.***	Should this be an organizationally defined parameter?
23	Karen Stanford/ Archstone Security	General	Publication	81	3146	confidentiality, integrity, and availability of the system and its information. [2]	Given that 800-171 doesn't include availability requirements, sugguest "confidentiality, integrity and availability (as applicable) of the system and its information."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Karen Stanford/ Archstone Security	General	Publication	1	279	"Prioritizing risk mitigation decisions and activities;" While it's clear from this and the prior iterations of 800-171 publications that the 800-171 allows for risk management activities, the DoD does not appear to have a mechanism to address risk mitigation. CMMC systems do not have federal ISSOs or federal system owners to accept the risks, and the DIBCAC is not planning to participate in ongoing POA&M management. As assessors, we are unable to issue risk ratings per finding for 800-171 assessments.	Codify the need to report findings based on their risk - low, moderate, high - to facilitate some sort of POA&M management process.
2	Karen Stanford/ Archstone Security	General	Publication	10	554	A.03.01.05.ODP[02]: security-relevant information for authorized access is defined.	This requirement is a little confusing. I think the intent here is for organizations to define which system processes require administrative access. Suggest, "system processes requiring privileged access is defined" or similar.
3	Karen Stanford/ Archstone Security	General	Publication	30 31	1284 1289 1299 1311	This wording in "3.4.6. Least Functionality" introduces a requirement in the nist SP 800-171 that differs than terminology used in NIST SP 800-53: "functions, ports, protocols, ***connections*** , and services." NIST SP 800-53 has consistently referred to "functions, ports, protocols, and services." Given that discrepancy between the language in the NIST SP 800-171 and NIST SP 800-53, can the requirement to document conections be assumed to be a requirement unique to CMMC? If so, FedRAMP reciprocity may become more challenging. The word "connection" is not currently defined in the NIST Glossary, so I'm uncertain as to what the intent there is, or if system interconnections are required or redundantly referenced here. Device identification and authentication is addressed in 3.5.2.	Evaluate if changes are required. Given the information in the description, it appears that the word connections is redundant. Many connections are services.
4	Karen Stanford/ Archstone Security	General	Publication	33	1394- 1406	A.03.04.11.a[01]: the location of CUI is identified and documented. A.03.04.11.a[02]: the system components on which CUI is processed are identified and documented. A.03.04.11.a[03]: the system components on which CUI is stored are identified and documented. A.03.04.11.b[01]: users who have access to the system and system components where CUI is processed are identified and documented. A.03.04.11.b[02]: users who have access to the system and system components where CUI is stored are identified and documented. A.03.04.11.c[01]: changes to the location (i.e., system or system components) where CUI is processed are documented. A.03.04.11.c[02]: changes to the location (i.e., system or system components) where CUI is stored are documented.	Could we possibly alter 3.4.10 to include identifying components that store, process, or ***transmit*** CUI? Transmission is omitted, but I would want to see network devices like firewalls and switches in the inventory.
5	Karen Stanford/ Archstone Security	General	Publication	34	1451	3.5.1. User Identification, Authentication, and ***Re-Authentication*** . The addition of "reauthentication" seems redundant, because of the requirements in session disconnect and network disconnect. How does this requirement differ from those controls? The NIST control this is derived from does not include ***"re-authentication;"*** this language seems unique to NIST SP 800-171.	Consider the removal of re-authentication or the incorporation into session/network disconnect requirements. Can re-authentication be combined with session termination? There seems to be redundancy currently.
6	Karen Stanford/ Archstone Security	General	Publication	57	1919-1921	A.03.08.04[01]: system media that contain CUI are marked to indicate distribution limitations. A.03.08.04[02]: system media that contain CUI are marked to indicate handling caveats. A.03.08.04[03]: system media that contain CUI are marked to indicate security markings.	Per NARA, not all of this is required for marking. Basic CUI can just be labeled as "CUI." There are often no distribution or handling instructions necessary. Recommend altering to state "system media that contain CUI are marked in accordance with NARA guidelines." Ostensibly, the requisite CUI category should be communicated from the Feds. I think the CUI data types should be defined and documented.
7	Karen Stanford/ Archstone Security	General	Publication	57	2248	A.03.11.02.a[03]: the system is scanned for vulnerabilities periodically.	Should this be an organizationally defined parameter?
8	Karen Stanford/ Archstone Security	General	Publication	57	2248	A.03.11.02.c[01]: system vulnerabilities to be scanned are updated periodically.	Should this be an organizationally defined parameter?