From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] NIST SP 800-171r2 Comments
Date:	Friday, September 16, 2022 8:17:26 AM
Attachments:	image001.png NIST.SP.800-171r2 comments.docx

NIST Wizards –

Thank you for allowing public commentary for NIST SP 800-171r2. Attached, please find some comments and suggestions for incorporation into the next draft.

Should you seek any industry-level support in any aspect of the work related to this update, I would be happy to help.

Thank you all for the good work you do to help secure this nation's infrastructure!

Karen Stanford, President, Archstone Security

E-mail: [redacted]
Cell: [redacted]

NIST SP 800-171 Comments

*Type: E – Editorial
G - General
T - Technical

Comments Due: September 16, 2022
E-mail Comments to: 800-171comments@list.nist.gov

#	Organization Name	Submitted By	Type*	Page #	Section #	Comment (including rationale for comment)	Suggested Change
1	Archstone Security LLC	Karen Stanford	G	Multiple	Multiple	Minimum requirements should be defined as the 800-171/CMMC implementation base expands. Many subs have multiple clients and do not have access to prime contractual requirement to help guide parameter selection. Further, organizations benefit from selecting insecure parameters.	Add minimally acceptable parameters for multiple controls within the framework; specifically: • 3.1.8 • 3.1.10 • 3.3.1 (90 days per 252.204-7012 3.e • 3.3.3 • 3.4.1. (Recommend NIST NCP Repository) • 3.5.5 • 3.5.6 • 3.5.7 • 3.5.8 • 3.6.3 • 3.11.1 • 3.11.3 • 3.12.1 • 3.12.3 • 3.14.1 • 3.14.4 • 3.14.5

#	Organization Name	Submitted By	Type*	Page #	Section #	Comment (including rationale for comment)	Suggested Change
2	Archstone Security LLC	Karen Stanford	G	Multiple	Multiple	The requirement to maintain an SSP was not introduced until 800-171 R2. As such, where we'd expect to see requirements to document certain parameters in many of these requirements, we do not. So, for example, with AC 3.1.7, "Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs," the 800-171 does not require that the organization define privileged functions or nonprivileged users; however, a failure to do so would result in the organization failing two separate tests defined in 800-171a. Organizations in the DIB are not expecting to find requirements in both 800-171 and 800-171a; and requirements are often not mirrored in the CMMC framework requirements.	Tests should explicitly match requirements. If the 800-171a expects a parameter to be documented, the 800-171 should require that the parameter be documented.
3	Archstone Security LLC	Karen Stanford	T	11	3.1.3	In Appendix D, 3.1.3 is mapped to AC-4, "Information Flow Enforcement." which is	Suggest evaluating intent of the control and updating wording as appropriate.

#	Organization Name	Submitted By	Type*	Page #	Section #	Comment (including rationale for comment)	Suggested Change
						commonly interpreted as requiring that internal traffic be segmented. That doesn't come across as the intent in 3.1.3, which is to "Control the flow of CUI in accordance with approved authorizations." The requirement seems to be the authorization vs. the need to adequately segment CUI traffic. NIST SP 800-171 does not introduce any new requirements to explicitly authorize data flow, and this requirement is not explicitly called out in the 800-53. If that is the intent, this control should be re-worded and should not map to AC-4 in Appendix D.	
4	Archstone Security LLC	Karen Stanford		13	3.1.12	This is a candidate for withdrawal and reincorporation into other AC, AU, and SC controls. This requirement was initiated over a dozen years ago when remote access was not common. For the last several years,	Candidate for withdrawal and reincorporation. Incorporate "remote access" language into existing AC (3.1.1, 3.2.1), AU (3.3.1, 3.3.2), and SC (3.13.1, 3.12.3, 3.13.4, 3.13.5, 3.13.8) requirements.

#	Organization Name	Submitted By	Type*	Page #	Section #	Comment (including rationale for comment)	Suggested Change
						remote access is processed as part of routine access almost exclusively. To fully address the requirements, AC should be updated to reference remote access for the applicable controls; AU should incorporate requirements to monitor remote access, and the SC family should outline requirements to require transmission encryption.	
5	Archstone Security LLC	Karen Stanford		Multiple	3.10.2 3.10.3 3.10.4 3.10.5 3.10.6	I think this wording could be revisited to make it clearer that the scope of this control is physical protections over components that store, process, or transmit CUI.	Suggest adding “*where CUI is housed or processed logically or physically*,” for example, “Provide adequate protective controls over spaces *where CUI is housed or processed logically or physically*.”
6	Archstone Security LLC	Karen Stanford		35	3.12.3	Almost all modern vulnerability scanning capabilities also offer the option to run configuration compliance scans against hosts. The data contained in those scans can be used to drastically reduce the cost of assessment activities and provide the	I strongly suggest expanding this requirement to include a reference to configuration compliance validation.

#	Organization Name	Submitted By	Type*	Page #	Section #	Comment (including rationale for comment)	Suggested Change
						organizations themselves with a simple means to validate that required controls are implemented.	