From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] DOD CIO Comments for 800-171
Date: Friday, September 16, 2022 6:48:03 PM
Attachments: DoD CIO Comment Matrix-Pre-Draft NIST SP 800-171_20220916.xlsx

---

Good Evening,

Please see attached Pre Draft comments for NIST SP 800-171 from the DOD CIO's Director of Risk Assessment and Operational Integration (RA&OI) and mission partners.

Tara Holcomb
Cyber Supply Chain Risk Management
ICT SCRM DOD CIO RA&OI
Office [redacted]
Cell: [redacted]

Comment Matrix - Pre-Draft NIST SP 800-171

Comment Number	Date	Commenter Name	Comment	Location of Change (Page number, Section, Header, Paragraph, Line #)	Critical, Substantive, or Administrative Comment	Suggested Language, if Appropriate
1	9/16/2022	DoD CIO / POC Michele Iversen [redacted]	The draft 171 should update the baseline references to NIST SP 800-161 to be to the new NIST SP 800-161 Revision 1. This will cause a new 171 Appendix D to reflect the updated NIST SP 800-161r1 Appendix B, Table B-1 "C-SCRM Baseline" that reflects the updated NIST SP 800-53B Moderate baseline of controls, which will also reflects the new supply chain risk management (RA) controls from NIST SP 800-53r5. Besides consistency between the control baselines and C-SCRM, this will ensure that 171 non-federal protection of CUI includes appropriate consideration of supply chain risk management.	Global	Critical	
2	9/16/2022	DoD CIO / POC Michele Iversen [redacted]	The changes in technology adoption with services are advancing and there is increased use of cloud services that should be considered more specifically. Section 2.2 specifically tailored out the SA "System and Services Acquisition" family (except SA-8 in footnote 18). The SA family should be revisited to factor in the security necessary to protect CUI in these services. Examples include SA-9 and SA-4. At the very least the inclusion of NIST SP 800-53B Moderate baseline controls in SA.	Section 2.2 and Appendix D	Critical	
3	9/16/2022	DoD CIO / POC Michele Iversen [redacted]	Addition of SR-4 to 171 Appendix D. A key risk aspect determined from DoD analysis of foreign intelligence entity threat within the supply chain is a lack of supply chain illumination and understanding of supply chain components. Provenance activities, including the enhancements SR-4(1-4) are necessary to ensure knowledge of the supply chain and to ensure CUI protection. Provenance is also critical to generating necessary SBOM content under EO 14028 and subsequent guidance. SBOMs are specifically called out for SR-4 in the NIST SP 800-161r1 Appendix A guidance. The final aspects of 171 guidance should specifically call out SBOM needs for not only a whole of government approach, but to also include supporting nonfederal systems and organizations.	Appendix D	Critical	
4	9/16/2022	CMMC PMO Working Groups/ POC Dana Mason [redacted]	Addition of PM-1 to 171 Appendix D. Establishing an Information Security Program Plan is an extremely important activity; CERT has data across more than 650 assessments across critical infrastructure that shows that organizations with established policies perform more than 79% of technical cybersecurity practices while organizaitons without established policies perform less than 38% of technical cybersecurity practices. This maps to all -1 controls for the NIST SP 800-171 Families that align with CMMC.	Appendix D	Critical	
5	9/16/2022	CMMC PMO Working Groups/ POC Dana Mason [redacted]	Addition of PM-16 to 171 Appendix D. Suggest adding this to 171 with consideration that there are 172 practices that build upon it. There is a modern need to receive and act upon cyber threat intelligence from information sharing forums and sources and communicate to stakeholders. Recommend discussion includes: Ensure you are looking at "current" information from reputable sources.	Appendix D	Critical	
6	9/16/2022	CMMC PMO Working Groups/ POC Dana Mason [redacted]	Addition of PM-6 to 171 Appendix D. Measuring activities for effectiveness is an extremely important activity; CERT has data across more than 650 assessments across critical infrastructure that shows that organizations that measure activities for effectiveness perform more than 83% of technical cybersecurity practices while organizaitons that do not measure activities for effectiveness perform less than 20% of technical cybersecurity practices.	Appendix D	Critical	
7	9/16/2022	CMMC PMO Working Groups/ POC Dana Mason [redacted]	Addition of SA-22 to 171 Appendix D. SA-22 is now part of the moderate baseline and managing products at end of life is important for security. SA-22 only covers support and does not address the last sentence addressing the case of providing mitigations and restricting usage in lieu of support when no internal or external support is available. Recommend discussion includes: Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or provide either in-house or external support from an ESP for unsupported components. If no internal or external support is available, the organization provides mitigations and restricts usage of the product.	Appendix D	Critical	

8	9/16/2022	CMMC PMO Working Groups/ POC Dana Mason [redacted]	Addition of AU-12(1) and AU-6(4) to 171 Appendix D. Centralized log management is essential to cyber operation and any advanced audit reviews. It is a CISA recommendation against the Russian adversaries targeting the DIB. Yes, it is currently in the high baseline, but is necessary to carry out any audit analysis. CISA Advisory Mapping - Recommendation to unify audit logs and to establish centralized log management	Appendix D	Critical	
9	9/16/2022	CMMC PMO Working Groups/ POC Dana Mason [redacted]	Addition of CP-9 and CP-9(1) to 171 Appendix D. Backups are essential for protection from ransomware. The current 171 requirements cover protection of backups, but do not require the backups themselves. Need to ensure systems can be rebuilt from scratch from information on backups. CISA Advisory Mapping - backup listed as additional best practice	Appendix D	Critical	
10	9/16/2022	CMMC PMO Working Groups/ POC Dana Mason [redacted]	Addition of IR-4(12) and IR-4(4) to 171 Appendix D. 800-53 Rev 4 more closely addressed root cause analysis, it is not addressed as directly in Rev 5 however it's still important to train organizations to get to the bottom of issues versus just treat the symptoms. CA-7 CONTINUOUS MONITORING and AU-2 EVENT LOGGING facilitate a "security capability" that links to examples in the 800-53 content about root cause analysis. Recommend discussion includes: Analyze malicious code and other residual artifacts remaining in the system after the incident, correlate information to identify adversary TTPs, and determine if the failure of one security control can be traced to the failure of other controls.	Appendix D	Critical	