From: "Albert Ingram - QT3A1" via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] SP 800-171 Comments
Date: Wednesday, July 12, 2023 10:40:03 AM
Attachments: Draft NIST SP 800-171 Rev 3 - RMASS Review 05Jul2023.xlsx

---

SP 800-171 R3 comments attached.

--

U.S. General Services Administration

Albert Ingram
IT Security Subcategory
Risk Management and Analysis Support Services (RMASS)
Information Technology Category (ITC)
Federal Acquisition Service (FAS)
[redacted]

Comment #	Submitted By	Type (General / Editorial / Technical)	Starting Page #	Starting Line #	Comment (include rationale)	Suggested Change
1	RMASS Team	Editorial	iii 79	N/A 3011	In the Note to Reviewers; Appendix C, Tailoring Guidance; and Appendix D, Change Log, the designation for "Not Applicable" is noted as "NA;" however, the acronym is usually commonly written as "N/A."	Recommend updating the acronym designation of "Not Applicable" from "NA" to "N/A" in the Note to Reviewers; Appendix C, Tailoring Guidance; and Appendix D, Change Log.
2	RMASS Team	Technical	5	111	Section 3, The Requirements, provides control requirements for each of the 17 control families in the SP-171 Revision 3, Initial Public Draft. However, the requirement for an organization to develop specific policies and procedures is not listed for each of the individual control families, except Section 3.15 Planning, which provides a general statement "Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements." Policy and procedure development and review should be listed as a requirement for each control family, to emphasize the importance of security policies and procedures for each control family.	Recommend including the development and review of policies and procedures as a requirement for *each* control family, in addition to the Planning family. Control requirements do reference necessary actions in accordance with "policy" or "procedure" but do not specify an individual control family requirement to develop the policy or procedure.
3	RMASS Team	Technical	9	292	3.1.8. Unsuccessful Logon Attempts - The control Discussion states the response to logon attempts may be implemented at the system and application levels. However, the control does not contain the appropriate response action. Recommend the response action be an additional organization-defined parameter (ODP).	Recommend including an ODP to describe the action when the maximum number of unsuccessful attempts is exceeded. For example, automatically lock the account for a specified time in minutes/hours when the maximum number of unsuccessful attempts is exceeded.
4	RMASS Team	Technical	4	79	Organization-defined parameters (ODP) help increase the amount of flexibility to manage risk. However, it should be understood that ODPs still must meet minimum security requirements. So how is a System Owner of a nonfederal system who has never used RMF supposed to figure out what values to fill in?	Suggest referencing CNSSI 1253 which contains a list of organization-defined values for some of the controls or NIST develop a plan to publish ODPs for NIST SP 800-171 Rev3. It is also highly recommended that the System Owner document the organization-defined values (and the rationale for their choice) in the System Security and Privacy Plan.
5	RMASS Team	Technical	5	111	The increased specificity for security requirements is a welcome change, as it removes ambiguity and makes it easier to implement the requirements effectively. However, some of the requirements may still be difficult to implement for smaller organizations with limited resources.	Suggest providing more guidance on how to implement the requirements in a cost-effective manner. Also suggest providing more guidance on how to interpret the requirements for non federal system owners who have never implemented RMF.
6	RMASS Team	Technical	79	3004	The updated tailoring criteria provides more flexibility in how organizations can implement the requirements. However, smaller organizations with limited resources may still have issues with implementing certain more complex requirements.	Suggest providing more guidance on how to tailor the requirements to specific organizational needs, especially for smaller organizations with limited resources.
7	RMASS Team	Technical	16	577	3.2.3. Advanced Literacy Training requires training on recognizing and reporting potential and actual indicators of insider threat, social engineering, and social mining. However, a frequency for this training is not specified. Frequent awareness and training about these indicators are important for effective security.	Recommend specifying the frequency of this literacy training or at the least include the frequency as an ODP.
8	RMASS Team	Technical	19	705	3.3.6. Audit Record Reduction and Report Generation specifies audit records are to be preserved. However, a retention time period is not specified. This is important to provide support for after-the-fact investigations of incidents and also to meet regulatory and organizational information retention requirements.	Recommend to specify a time period or at the least include the time period as an ODP. For example, retain for 12 months online and 18 months in cold storage.
9	RMASS Team	Technical	20	741	3.3.8. Protection of Audit Information states to protect audit information and audit logging tools. However, there is not a reference to the method of protection.	Recommend the use of cryptographic mechanisms should be referenced for this protection.
10	RMASS Team	Technical	23	831	3.4.4. Impact Analyses states to analyze the security impact of changes to the system prior to implementation. However, there is not a reference to test the changes prior to implementation.	Recommend 3.4.4 include testing as a requirement.
11	RMASS Team	Technical	27	1025	3.5.3. Multi-Factor Authentication states to implement multi-factor authentication for access to system accounts. The term "system accounts" is ambiguous and can have multiple interpretations. For clarity, describe the meaning of "system accounts" and require multi-factor authentication for access to privileged and non-privileged accounts.	In addition to describing the meaning of "system accounts" also require multi-factor authentication for access to privileged and non-privileged accounts.
12	RMASS Team	Technical	28	1039	3.5.4. Replay-Resistant Authentication states to implement replay-resistant authentication mechanisms for access to system accounts. The term "system accounts" is ambiguous and can have multiple interpretations. For clarity, describe the meaning of "system accounts" and require replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.	In addition to describing the meaning of "system accounts" also require replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.
13	RMASS Team	Technical	32	1193	3.6.3. Incident Response Testing does not include a requirement to report the testing results. The incident response (IR) test report is an important requirement of the IR testing, for reporting the status and results of the testing.	Recommend including a requirement to report the testing results and identify who in the organization should receive the report. The report recipient(s) could be an ODP.
14	RMASS Team	Technical	32	1206	3.6.4. Incident Response Training does not specify the required frequency of the training. For clarity, effectiveness, and completeness the frequency should be specified.	Recommend specifying the training is required within a determined number of days when assigned an incident response role and the frequency thereafter.
15	RMASS Team	Technical	33	1230	3.7.4. Maintenance Tools and 3.7.5. Nonlocal Maintenance do not reference a recordkeeping requirement. Records should be maintained to report the maintenance timeframe, performance, results, etc., for management and administration of the system maintenance program.	Recommend including a recordkeeping requirement for all system maintenance.
16	RMASS Team	Technical	33	1230	3.7.4. Maintenance Tools and 3.7.5. Nonlocal Maintenance do not reference a timeframe parameter for "timely maintenance," within which maintenance support or spare parts for system components should be performed or acquired. A maximum timeframe should be specified for effective management and administration of the system maintenance program.	Recommend specifying the maximum maintenance timeframe/time period from the time of failure. This timeframe/time period should be determined in accordance with the system Contingency Plan and Business Impact Analysis.
17	RMASS Team	Technical	35	1295	3.8.1. Media Storage states to, "Physically control and securely store digital and non-digital media containing CUI" but does not specify or recommend the methods in the control requirement. The control Discussion provides examples. For clarity, the methods listed in the Discussion or similar should be included in the control requirement.	Recommend specifying the minimum methods to physically control and securely store media.
18	RMASS Team	Technical	39	1457	3.9.3. External Personnel Security, Part b states to require external providers to comply with the personnel security policies and procedures established by the organization. But, the "established by the organization" term could be rather ambiguous and possibly interpreted as not intended. This could be interpreted as established by the external provider (organization) and not as intended, by the organization using the external provider.	Recommend clarifying by stating, or similar, "established by the organization using the external provider" to clarify the intent is not to comply with the external provider's policies and procedures.
19	RMASS Team	Technical	42	1575	3.11 Risk Assessment does not include a requirement for conducting Privacy Impact Assessments (PIA). PIAs should be conducted and are useful for identifying CUI within an organization.	Recommend requiring Privacy Impact Assessments (PIA) and Privacy Threshold Assessments (PTA) to be conducted and updated annually.
20	RMASS Team	Editorial	45	1690	3.12.2. Plan of Action and Milestones includes the designation for the acronym as "POAM;" however, the acronym is usually commonly written as "POA&M."	Recommend updating the acronym designation of Plan of Action and Milestones from "POAM" to "POA&M."
21	RMASS Team	Technical	46	1750	3.12.7. Internal System Connections does not include a requirement to terminate non-persistent connections after a duration of inactivity. Connectivity termination enhances security.	Recommend including a requirement to terminate non-persistent connections after a duration of inactivity; e.g., 15 or 30 minutes, etc.
22	RMASS Team	Technical	47	1769	3.13.1. Boundary Protection does not include a requirement to document, approve, and maintain documentation about the boundary interfaces. Security and network architecture documentation should be developed, reviewed, and maintained.	Recommend including a requirement to develop, approve, review, and maintain security and network architecture boundary interface documentation.
23	RMASS Team	Technical	57	2143	Section 3.15.2. is titled, "System Security Plan" however, the updated title for NIST SP 800-53 Rev 5 references "Privacy" as in System Security and Privacy Plans. Section 3.15.2 shows three (3) requirements and the SP 800-53 shows 15, which includes much more detail.	Recommend changing the Section 3.15.2 title to "System Security and Privacy Plan" and include more specific requirements from the SP 800-53 control PL-2.

24	RMASS Team	Technical	59	2224	Part (requirement) b of Section 3.16.3. External System Services references documentation of user roles and responsibilities for external system services. However, there is not a requirement for system documentation. System documentation is important for descriptions of configuration, installation, and operation of the system, component, or service; use and maintenance of security and privacy functions, and known vulnerabilities, etc.	Recommend including a requirement for obtaining and maintaining system documentation of external systems and services.
25	RMASS Team	Technical	60	2227	3.17.2. Acquisition Strategies, Tools, and Methods references development and implementation of acquisition strategies, contract tools, and procurement methods. However, the inspection of systems or system components for tampering or counterfeiting is not specifically referenced, and is important to protect against, identify, and mitigate supply chain risks.	Recommend requiring the inspection of systems or system components for tampering, counterfeiting, or whitelisting to protect against, identify, and mitigate supply chain risks.
26	RMASS Team	General	72	2755	Basic Security Requirement is identified as a keyword on page i; however, it is not defined in Appendix B, Glossary.	Recommend adding an entry for Basic Security Requirement in Appendix B, Glossary.
27	RMASS Team	General	73	2765	Contractor Systems is identified as a keyword on page i; however, it is not defined in Appendix B, Glossary.	Recommend adding an entry for Contractor System (or Contractor Systems) in Appendix B, Glossary.
28	RMASS Team	General	73	2788	Derived Security Requirement is identified as a keyword on page i; however, it is not defined in Appendix B, Glossary.	Recommend adding an entry for Derived Security Requirement in Appendix B, Glossary.
29	RMASS Team	General	78	2981	Security Requirement is identified as a keyword on page i; however, it is not defined in Appendix B, Glossary.	Recommend adding an entry for Security Requirement in Appendix B, Glossary.
30	RMASS Team	General	76	2915	The inclusion of organization-defined parameters (ODPs) is noted significant to NIST SP 800-171 Rev. 3 in the Note to Reviewers on pages iii and iv; however, it is not defined in Appendix B, Glossary.	Recommend adding an entry for Organization-Defined Parameter (ODP) in Appendix B, Glossary.