From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments on NIST SP 800-171r3 initial public draft - The MITRE Corporation
Date: Friday, July 14, 2023 12:26:05 PM
Attachments: MITRE response to SP800-171 comment_07072023_12PM_PRS_23-2351.xlsx

Greetings,

Attached please find MITRE's comments on NIST SP 800-171r3 initial public draft for public comment period on through July 14, 2023. Please let us know if you have any questions or issues with the file. Thank you for considering our feedback.

Best regards,
Mel

Mel Martin-Gordon
she | her | hers
Policy & Compliance Manager
InfoSec
[redacted]
MITRE | Solving Problems for a Safer World (R)

Approved for Public Release;
Distribution Unlimited.
Public Release Case Number 23-2351

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	The MITRE Corporation	General	analysis	iii		Consider revisions based on security value and implementation impact instead of their default presence in SP 800-53 rev 5 moderate baseline.	
2	The MITRE Corporation	General	analysis	iii		Organizational-defined parameters (ODP) will not be practicable if they must be defined by federal organizations. For non-federal contractors working with multiple agencies, this language opens the possibility that agencies could set contradictory parameters. If audits were conducted for content from multiple agencies in one system then this could make it impossible for the contractor to meet the requirements. For example, related to lines 647 and 648 for retaining audit records, one agency could have a maximum retention of 3 months and another could set a minimum retention of 6 months. Between months 3 to 6 the contractor could not comply with one while meeting another.	Recommend NIST set a standard ODPs or clarify that non-federal organizations may set their own ODPs.
3	The MITRE Corporation	General	analysis	3	65	The connection could be stronger for the reasoning that updates to SP 800-171 need to follow updated versions of 800-53 and the FISMA moderate baseline. In 32 CFR 2002, there are specific references to connections to SP 800-53 and SP 800-171 via 32 CFR 2002.2, which in turn references 800.53 Revision 4.	
4	The MITRE Corporation	General	analysis	3	65	It was not clear when 800-53 rev 5 was created that contractors subject to 800-171 should have been providing feedback on changes.	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
5	The MITRE Corporation	General	analysis	4	79	The original purpose of 800-171 was to develop a standard set of compliance requirements that contractors could adopt that would allow compliance to be met across multiple agencies. The use of Organization-Defined Parameters (ODPs) is often seen as complicating the compliance process; instead of protecting all CUI with one set of controls, contractors that support multiple agencies must set up separate environments with different control parameters. Consideration should be given to streamline this process.	
6	The MITRE Corporation	General	analysis	5	112	The expansion of 800-171 in the rev 3 draft represents a significant expansion in the number and scope of the requirements. This comes after 800-171 has already been embedded in 800-171 Department of Defense contracts. Consider coordination implementation of these revisions with the timing of the Cybersecurity Maturity Model Certification (CMMC) program to afford contractors the opportunity to reasonably adapt controls and compliance programs to the new requirements.	
7	The MITRE Corporation	Technical	analysis	5	116	This is a significant expansion of the requirements that may be duplicative.	Condense f2, f3, and h3 to remove duplicative requirements. Remove e because it is not relevant with account management.
8	The MITRE Corporation	General	analysis	5	117	The term "system account" can have different meanings, For example, in Linux, the term "system account" means non-interactive accounts used by system services.	Recommend using a more precise term than "system account" or provide a definition of the term to avoid confusion.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
9	The MITRE Corporation	Technical	analysis	5	125	It is not clear if f (disable account of individuals) is specific to user accounts, or if it also applies to service accounts that are owned by the user.	Change to "disable user accounts." If non-user accounts are in scope, a new bullet should be created to address them.
10	The MITRE Corporation	Technical	analysis	6	181	NIST states that the word "system" can be interpreted as either one system, a small group of systems, or all the systems that are in scope for the organization. This is an expansive scope in terminology. A narrowly defined and clear definition is critical for any requirement that includes the word "system" to ensure consistent compliance.	Revise the language to indicate whether "within the system" in this context is from two applications on the same server, or is two different servers, or is anywhere on the contractor's internal network.
11	The MITRE Corporation	General	analysis	7	214	3.1.4 states that duties must be defined and does not explicitly say that duties must be separated. It is unclear if enforcement meant to be inferred or has been omitted.	Suggest adding a bullet that says that duties requiring separation must be implemented.
12	The MITRE Corporation	Technical	analysis	10	320	Changing the terminology from "session" to "device" implies physical system. The term session could imply a virtual session or a physical session. With many environments consisting of only virtual systems this creates confusion.	Provide better clarity if this is a physical control or a logical control.
13	The MITRE Corporation	Technical	analysis	11	360	3.1.12 b, d, and e are redundant with other requirements.	Remove b, d, and e.
14	The MITRE Corporation	Technical	analysis	11	358	Due to most services becoming virtual, it is recommended that a more clear definition of "remote access" is applied.	Define "remote access" and make it clear whether "remote access" means any network-based access to the system or access from outside of the organization.
15	The MITRE Corporation	Technical	analysis	12	396	b and c are redundant with other requirements and do not need to be called out for wireless access.	Remove b and c.
16	The MITRE Corporation	Technical	analysis	13	455	The definition of "external system" is vague and should be better defined.	Clarify that "external system" means a system that is not owned by the organization.
17	The MITRE Corporation	Technical	analysis	14	479	The definition of "external system" is vague and should be better defined.	Clarify that "external system" means a system that is not owned by the organization.

**Approved for Public Release;
Distribution Unlimited.
Public Release Case Number 23-2351**

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
18	The MITRE Corporation	Technical	analysis	14	503	This is vague. It is not clear if this means that the organization's externally-facing systems need to be reviewed, or potential information on any external system should be reviewed for indications that it was leaked.	Revise language to state that the requirement is applicable "on the organization's publicly accessible systems."
19	The MITRE Corporation	Technical	analysis	14	479	The definition of "external system" is vague and should be better defined.	Clarify that "external system" means a system that is not owned by the organization.
20	The MITRE Corporation	Technical	analysis	18	645	a and b are not sufficiently distinct to merit separation.	Delete a, or merge a and b.
21	The MITRE Corporation	Technical	analysis	25	941	The language defining "system components" is vague. It is unclear if "system components" refers to the motherboard, disk drives, application licenses, or other items.	Recommend including clear, concise language to limit the scope of the phrase "system components."
22	The MITRE Corporation	Technical	analysis	26	959	The scope of "system" is vague. It is unclear if the intent is to identify every server/application that contains CUI or if the "system" can be identified as the corporate network.	Recommend clarifying whether the requirement refers to individual servers or the entire network.
23	The MITRE Corporation	Technical	analysis	28	1040	The definition of "system" is vague and the intent is unclear if "system" is the network, or if it is any given endpoint/server on the network.	Remove the word "system" and clarify whether this is intended as MFA for the network or MFA for a specific computing device.
24	The MITRE Corporation	Technical	analysis	29	1072	There may be COTS software where certain characters (including spaces and other obscure characters) cannot be allowed. The language is drafted so spaces and all printable characters must be allowed. This could limit access to certain types of software.	Remove b, and include a note in the Discussion section that long passwords and passphrases are now allowed per NIST guidance.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
25	The MITRE Corporation	General	analysis	29	1074	"C" may not be implementable in all circumstances. Consideration should be given to introduce SP 800-63 password language in a more seamless way, one that does not prescribe a certain method. Focus should be placed on viable methods and requirements unique to each.	Recommend remove c.
26	The MITRE Corporation	Technical	analysis	30	1116	All of these requirements are specific to passwords, and are not applicable to biometric or possessed authenticators.	Combine with 3.5.7.
27	The MITRE Corporation	Technical	analysis	35	1320	"Maintenance" appears to be a significant expansion of the requirement and one that is vague.	Recommend either removing "maintenance" or using the phrase "external maintenance."
28	The MITRE Corporation	Technical	analysis	46	1717	It is unclear if the independent assessor needs to be external.	Recommend clarifying if the independent assessor does or does not need to be external to the organization.
29	The MITRE Corporation	Technical	analysis	46	1731	The scope of "system" is vague and is unclear if the intent is for this control to be exchanged between organizational systems and external systems (as 800-53 implies).	Recommend clarifying that the exchange of CUI is intended here to be between the CUI system and external (to the organization) systems.
30	The MITRE Corporation	Technical	analysis	46	1751	The distinction between component and system is unclear.	Recommend a clear definition of "system" and how it affects this control.
31	The MITRE Corporation	General	analysis	46	1731	Agreements should not be required if both systems exchanging information are managed at the same level and fall under the same Authorizing Official.	Suggest to specify that agreements be required for only systems not managed at the same level.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
32	The MITRE Corporation	General	analysis	50	1904	This is a significant expansion of the number and depth of requirements for key management. While they make sense to be described in the Discussion section, they do not need to be described in the requirement text.	Recommend moving the language for key generation, distribution, storage, access, and destruction to the discussion section.
33	The MITRE Corporation	Technical	analysis	52	1973	It is unclear how this would work for servers that auto-patch and can be challenging for web traffic. This may not be feasible for many types of non-web traffic as it would break functionality (mutual authentication, SSH validation, etc.).	Consider de-centralizing this requirement to permit organizations to develop a list of traffic types for which this control would be implemented and allow for exclusions to non-web traffic where the control is not viable.
34	The MITRE Corporation	General	analysis	55	2080	The new additions (2, 3, and b) add limited value to the original control.	Remove 2, 3, and b.
35	The MITRE Corporation	General	analysis	59	2238	Agreements should not be required if both systems exchanging information are managed at the same level and fall under the same Authorizing Official.	Need Clarification when agreements are required.