

From: 800-171comments@list.nist.gov on behalf of [REDACTED]
To: 800-171comments@list.nist.gov
Cc: [REDACTED]
Subject: [800-171 Comments] AIA Comment Submittal for NIST SP-800-171 Rev. 3
Date: Friday, January 26, 2024 5:29:09 PM
Attachments: [AIA Comments - NIST SP 800-171 Rev 3 - 1.26.2024.pdf](#)
Importance: High

Dear NIST –

Please find attached AIA's comment submittal to the Final Public Draft of NIST SP 800-171 Rev 3.

Thank you for the extension to the comment period as we are also working through public comments to multiple FAR and DFARS cases.

V/R

- Jason

Jason Timm | *Director, Defense Policy & Integration*
AIA | 1000 Wilson Boulevard, Suite 1700, Arlington, VA 22209
[REDACTED]
aia-aerospace.org



January 26, 2024

National Institute of Standards and Technology
Computer Security Division
Computer Security Resource Center
Email to: 800-171comments@list.nist.gov

RE: Call for Comments: NIST Special Publication (SP) 800-171 Rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

Dear NIST:

On behalf of the Aerospace Industries Association (AIA)¹, I am pleased to offer the following comments and the enclosed comments matrix in response to the call for public comment to NIST SP 800-171 Rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*:

General Comments/Concerns/Recommendations

While AIA acknowledges that NIST is not a regulating body, many U. S. Government agencies use NIST Special Publications within their regulatory and/or policy frameworks. When NIST makes major changes to its Special Publications, they have a ripple effect throughout the aerospace and defense industry (A&D). They often increase costs significantly (contrary to many regulatory impact analyses) and, more importantly, reduce the overall security effectiveness of organizations that are subject to multiple frameworks. This situation will only continue until NIST better harmonizes the standards of these frameworks.

Regarding the instant matter, AIA understands NIST plans to get the CUI overlay through revision 4 or 5 rolled in as a complete overlay of NIST SP 800-53. AIA recommends that NIST develop the CUI overlay in partnership with the A&D and delay releasing final versions of NIST SP 800-171 and NIST SP 800-172 until completion of the overlay with respect to NIST SP 800-53.

AIA appreciates NIST's effort to narrow the organization-defined parameters (ODPs) in the latest draft of NIST SP 800-171 Rev. 3. The final publication should make it clear that only the nonfederal organization is responsible for setting these parameters. If federal agencies have the latitude to specify values for designated parameters on a contract-by-contract basis, it will undermine the standard itself by introducing non-standard controls. Some of these non-standard controls may be derived by federal agencies from NIST SP 800-53, contradicting the tailoring effort by NIST as quoted below from section *1.1 Purpose and Applicability* of the NIST SP 800-171 Rev 2 (and similarly in Rev. 1). This should not be changed now more than seven (7) years after the Department of Defense first incorporated NIST SP 800-171 into government contracts.

“The tailoring criteria described in Chapter Two are not intended to reduce or minimize the federal requirements for the safeguarding of CUI as expressed in the federal CUI regulation. Rather, the intent is to express the requirements in a manner that allows for and facilitates the equivalent safeguarding measures within nonfederal systems and organizations and does not diminish the level

¹ Founded in 1919, the Aerospace Industries Association (AIA) is the premier trade association advocating on behalf of over 330 aerospace and defense (A&D) companies for policies and investments that keep our country strong, bolster our capacity to innovate and spur economic growth. AIA's members represent nation's leading aerospace and defense manufacturers and suppliers of civil, military, and business aircraft and engines, helicopters, unmanned aerial systems, space systems, missiles, equipment, services, information technology, and other related components

RE: Call for Comments: NIST Special Publication (SP) 800-171 Rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

of protection of CUI required for moderate confidentiality. Additional or differing requirements, other than the requirements described in this publication, may be applied only when such requirements are based on law, regulation, or government-wide policy and when indicated in the CUI Registry as CUI-specified or when an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality. The provision of safeguarding requirements for CUI in a specified category will be addressed by the National Archives and Records Administration (NARA) in its CUI guidance and in the CUI FAR...”

Nonfederal organizations need to have predictability in their contracts to make informed investment decisions and ensure contract compliance. If a security requirement is subject to change on an *ad hoc* basis by any federal agency that incorporates NIST standards, the result for the A&D would be overlapping requirements causing conflict and confusion. Implementation of NIST controls would also be more difficult and costly. AIA recommends NIST define an acceptable range of values for each of the ODPs and/or let the nonfederal organizations define and defend the selected ODP values. This will provide consistency in how nonfederal organizations implement the security controls while also limiting additional costs.

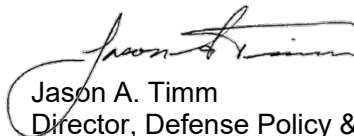
Both recommendations above assist with meeting the harmonization of requirements and frameworks as identified in Section 2(h) of Executive Order 14028, *Improving the Nation's Cybersecurity*:

“Current cybersecurity requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations, including cloud-service cybersecurity requirements. Standardizing common cybersecurity contractual requirements across agencies will streamline and improve compliance for vendors and the Federal Government.”

AIA believes that lessons learned demonstrate how requirements and processes in cybersecurity are mutually beneficial when shared through robust collaboration across sector business operations representing all stakeholders. AIA is committed to initiatives that secure information from cyber threats and we continually work to encourage collaboration between industry and government on cybersecurity matters to include innovation, agility, and flexibility across all businesses and government entities supporting national and international missions.

Thank you for the opportunity to provide the above comments and those in the enclosed comment matrix.

Sincerely,



Jason A. Timm
Director, Defense Policy & Integration
National Security Policy Division

Enclosure: AIA Comments Matrix for NIST SP 800-171 Rev 3 Final Public Draft

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay, 171A)	Starting Page #*	Starting Line #*	Comment (include rationale)*	Suggested Change*	Requirement #	Requirement Text
1	AIA	General	NIST SP 800-171r3 fpd	1	1	The requirements need to be rewritten to allow for understanding how to implement and what is expected including the relevant discussions to provide clarity of understanding.	The requirements need to be rewritten to allow for understanding how to implement and what is expected including the relevant discussions to provide clarity of understanding.		
2	AIA	General	NIST SP 800-171r3 fpd	1	1	Many of the new changes make it harder for small businesses to adequately and effectively meet the requirements due to some additional on-demand and automation requirements.	Review the intent of these requirements to be able to be met by small businesses in a cost effective and efficient manner		
3	AIA	General	NIST SP 800-171r3 fpd	1	1	Discussions should be more tailored and readable instead of a stream of inconsistent and incohesive sentences. Break down the discussion as the requirements are broken down for easier readability and understandability.	Break down the discussion as the requirements are broken down for easier readability and understandability.		
4	AIA	General	NIST SP 800-171r3 fpd	1	1	Further reviews of the discussions under each requirement need to be performed to provide references to the interrelated requirements which is done is a few but most do not contain.	Further reviews of the discussions under each requirement need to be performed to provide references to the interrelated requirements which is done is a few but most do not contain.		
5	AIA	General	NIST SP 800-171r3 fpd	1	1	The Discussions need to be reviewed to make sure they are consistent and adequately describe the intent and options of the listed requirements and remove all extraneous information that is not directly related to the requirements.	The Discussions need to be reviewed to make sure they are consistent and adequately describe the intent and options of the listed requirements and remove all extraneous information that is not directly related to the requirements.		
6	AIA	General	NIST SP 800-171r3 fpd	1	1	The discussions in every requirement should accurately reflect the intent of the requirement and be very specific on examples and definitions that relate directly to the requirement.	Update the discussions under every requirement to be more concise, identify the relationship to the other requirements, identify the intent and context of the requirement, and remove extraneous information the does not directly relate to the requirement.		
7	AIA	General	FAQ	3		Missing table and appendix from FAQ: Appendix E (Table 41) in NIST SP 800-171	Add the discussed Appendix and tables to the Final Draft document.		
8	AIA	General	FAQ	3		The question "Why did we add new security requirements to the catalog.." identifies that there should be an Appendix E (Table 42) in NIST SP 800-171 that describes the type of change that occurred for each requirement during the transition from Revision 2 to Revision 3 as well as a Table 40 that summarizes the number and types of changes that occurred. These seem to be missing within the 800-171 r3 Final Public Draft.	Add the discussed Appendix and tables to the Final Draft document.		
9	AIA	Editorial		6	136	"Enduring exception" is not defined in the glossary	Add the definition for "enduring exception" to the glossary.		
10	AIA	General	NIST SP 800-171r3 fpd	6	160	For any requirement with an ODP, the discussion should provide additional details on why it is important and examples.	Update the discussion to describe the importance of the ODP and examples of the ODP	3.1.1	
11	AIA	General	NIST SP 800-171Ar3 ipd	6	152	For F2, the ODP does not make sense if accounts use MFA and do not expire (which is an option per NIST documentation of accounts per SP 800-63B Section 5.1.1.2 paragraph 9) as it is covered by F4 and F5. the requirement F should have an ODP for "disable within timeframe" for all of the options except for "inactive" which can break many things as many users may not log in very often, especially if from a support team. Monitoring the accounts (E) should identify if F4/F5 occurs and then the account should be disabled within ODP timeframe. F2 should be removed and revert back to the F requirement in IPD.	Change F2 to "The accounts have been inactive for ODP if not configured to use multifactor authentication"	3.1.1	
12	AIA	Technical	NIST SP 800-171r3 fpd	6	156	G should have ODP that identifies timeframe for notification. Otherwise, could be 1 time per year review which adds significant risk. Revert back to IPD statement for Time Period but not the ODP for personnel or roles.	Either add "periodically" or change to ODP with timeframe for when to notify.	3.1.1	
13	AIA	General	NIST SP 800-171r3 fpd	7	189	The discussion does not discuss authorization enforcement but rather access enforcement.	Update the discussion to provide information on authorization enforcement and align with the requirement.	3.1.2	
14	AIA	General	NIST SP 800-171r3 fpd	9	261	For any requirement with an ODP, the discussion should provide additional details on why it is important and examples.	Update the discussion to describe the importance of the ODP and examples of the ODP	3.1.5	
15	AIA	Technical	NIST SP 800-171r3 fpd	9	278	B should be more like what it was in 171r2 and rewritten for easier reading such as "Require that users or roles use non-privileged accounts when accessing nonsecurity functions or nonsecurity information"	Change to "Require users and roles to use non-privileged accounts when accessing nonsecurity functions or nonsecurity information"	3.1.6	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay, 171A)	Starting Page #*	Starting Line #*	Comment (include rationale)*	Suggested Change*	Requirement #	Requirement Text
16	AIA	General	NIST SP 800-171r3 fpd	10	280	For any requirement with an ODP, the discussion should provide additional details on why it is important and examples.	Update the discussion to describe the importance of the ODP and examples of the ODP	3.1.6	
17	AIA	Technical	NIST SP 800-171r3 fpd	10	296	3.1.7[B] "Logging the use of privileged functions..." this should be in 3.3.1[C], because logging is an auditing function and does not belong in the AC family. Logging of privileged function execution is also listed in the discussion for 3.3.1.	Please remove 3.1.7[B] and place into 3.3.1[C] as a requirement.		
18	AIA	Technical	NIST SP 800-171r3 fpd	10	315	This will be significantly harder to meet as it requires limiting ALL invalid logon attempts within a time period vs just a single user. Most applications and operating systems are by user not by system. How do you lock a system when X number of failed logons by XX number of accounts and then block legitimate users from logging in? Do you limit the number of logins per time period? This should be identified as a significant change.	Add "by a user" back into the requirement from 800-171r3	3.1.8	
19	AIA	Technical	NIST SP 800-171r3 fpd	10	315	This will be significantly harder to meet as it requires limiting ALL invalid logon attempts within a time period vs just a single user. Most applications and operating systems are by user not by system. How do you lock a system when X number of failed logons by XX number of accounts and then block legitimate users from logging in? Do you limit the number of logins per time period? This should be identified as a significant change.	Modify the requirement to replace to change "by a user" from the IPD to "to an information system". This would make the requirement "Limit the number of consecutive invalid logon attempts to a system to [Assignment: organization-defined time period]."	3.1.8	
20	AIA	Technical	NIST SP 800-171r3 fpd	12	381	Why is there no monitoring of remote sessions? Why removal of cryptographic mechanisms to protect confidentiality of remote sessions? Are these covered somewhere else? Is the removal of cryptographic mechanisms to allow for better monitoring/review of sessions?	Update to be more concise and identify assumptions and other requirement relationships.	3.1.12	
21	AIA	General	NIST SP 800-171Ar3 ipd	12	628	The 3 assessment objectives specifically call out login attempts by user but 800-171r3 3.1.8 removed "by a user" and thus is inconsistent with the requirement.	Add "by a user" back into the requirement from 800-171r3		
22	AIA	Technical	NIST SP 800-171r3 fpd	13	417	Why remove implementation guidance? Is it implied that implementation guidance is incorporated in configuration and connection requirements?	Update to be more concise and identify assumptions and other requirement relationships.	3.1.16	
23	AIA	Technical	NIST SP 800-171r3 fpd	13	417	Why was encryption removed? Is this supposed to be covered by 3.13.8?	Update to be more concise and identify assumptions and other requirement relationships.	3.1.16	
24	AIA	Technical	NIST SP 800-171r3 fpd	15	481	B should have the ODP removed and remove "following"	B should have the ODP removed and remove "following"	3.1.20	
25	AIA	Technical	NIST SP 800-171r3 fpd	15	481	B should be "Establish and maintain the terms," and remove C2 as it is redundant with B.	B should be "Establish and maintain the terms," and remove C2 as it is redundant with B.	3.1.20	
26	AIA	Technical	NIST SP 800-171r3 fpd	15	481	"Establish the following terms, conditions, and security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals"; this is vague, is NIST going to provide guidance 3.1.20[B]?	Explain what you are looking for in [B]. This is also tough to test because of internet based systems, what policy/terms and conditions is sufficient to define? The scope of the ODP is too large. Original requirement was to control CUI being posted to external systems.		
27	AIA	Technical	NIST SP 800-171r3 fpd	15	481	Why was policies dropped from C1 when moving to 3.1.20? C1 should be "security policies and plans"	Update to be more concise and identify assumptions and other requirement relationships.	3.1.20	
28	AIA	Technical	NIST SP 800-171r3 fpd	15	481	Why isn't D in Media Protection family instead?	Update to be more concise and identify assumptions and other requirement relationships.	3.1.20	
29	AIA	Technical	NIST SP 800-171r3 fpd	15	481	Why is 3.1.20 and External Systems in AC and not System and Communications Protection family?	Update to be more concise and identify assumptions and other requirement relationships.	3.1.20	
30	AIA	Technical	NIST SP 800-171r3 fpd	15	490	3.1.20[D] Why are you talking about restricting portable storage devices when they are discussed in 3.8.7? This does not belong in the AC Family.	Please have portable storage devices in one control and not have them spread about in multiple controls. Make this 3.8.7[C].		
31	AIA	Technical	NIST SP 800-171r3 fpd	16	525	What happened to control 3.1.23 Account Management - Inactivity Logout that was in IPD? There is no mention if it was incorporated into another control, or completely removed.	No recommendation		
32	AIA	Technical	NIST SP 800-171r3 fpd	18	602	As several other requirements have been combined, why not just combine 3.3.1, 3.3.2 and 3.3.3 into a single requirement for consistency with other changes in the draft?	Combine 3.3.1, 3.3.2, and 3.3.3 into a single requirement similar to 3.1.1	3.3.1	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay, 171A)	Starting Page #*	Starting Line #*	Comment (include rationale)*	Suggested Change*	Requirement #	Requirement Text
33	AIA	Technical	NIST SP 800-171r3 fpd	18	602	As several other requirements have been combined, why not just combine 3.3.1, 3.3.2 and 3.3.3 into a single requirement for consistency with other changes in the draft?	Combine 3.3.1, 3.3.2, and 3.3.3 into a single requirement similar to 3.1.1	3.3.2	
34	AIA	Technical	NIST SP 800-171r3 fpd	18	602	As several other requirements have been combined, why not just combine 3.3.1, 3.3.2 and 3.3.3 into a single requirement for consistency with other changes in the draft?	Combine 3.3.1, 3.3.2, and 3.3.3 into a single requirement similar to 3.1.1	3.3.3	
35	AIA	Technical	NIST SP 800-171r3 fpd	21	728	Should this be 1 or 2 a and b? Where a is currently 2 and b is currently 3. What is the point of 3.	Look at changing and/or rewording for clarity.	3.3.7	
36	AIA	Technical	NIST SP 800-171r3 fpd	21	728	Not sure an ODP is required here especially based on the discussion about varying based on the needs of the application/system.	Remove ODP and change to b to "b. Record time stamps for audit records that meet application and system granularity of time requirements and that:"	3.3.7	
37	AIA	Technical	NIST SP 800-171r3 fpd	22	771	Should have a ", " before "under configuration control on a.	Should have a ", " before "under configuration control on a.	3.4.1	
38	AIA	Technical	NIST SP 800-171r3 fpd	22	771	Why was "document" removed from a? Is this because of related/other control for documentation requirements? If so, then this should be explicitly identified in the discussion and other ways in the control.	Make sure consistent with other requirements that have "document" as part of the requirement.	3.4.1	
39	AIA	Technical	NIST SP 800-171r3 fpd	23	789	If removing "monitoring" with the assumption that it is handled within another requirement, make sure that the discussions reflects the associated requirements and/or dependencies.	Add relationships between requirements.	3.4.2	
40	AIA	Technical	NIST SP 800-171r3 fpd	24	820	Why remove "monitoring" from 3.4.2 but keep in 3.4.3 especially if assumption is monitoring covered by other requirements? Is this the requirement that covers 3.4.2? If so, then make sure to highlight dependencies and associations.	Add relationships between requirements.	3.4.3	
41	AIA	Technical	NIST SP 800-171r3 fpd	24	837	Why remove "after" (b) from assessment? Is this part of 3.4.3 "monitoring"? It would seem that (b) should be added to 3.4.3 as there still should be verification/validation after/during implementation. If in another requirement then make sure to identify dependencies and associations.	re-add b. from IPD back into the requirement or add a b. that requires validation and verification after system changes for impacted security requirements.	3.4.4	
42	AIA	Technical	NIST SP 800-171r3 fpd	25	868	This ODP (b) could be mis-interpreted/read if only looking at what is defined as it is defining the Prohibited and Restricted ports and could add confusion. Per the Overlay, 800-53 has "prohibited or restricted" in the ODP and recommend leaving as per 800-53.	Revert the ODP back to what is in the Overlay and 800-53	3.4.6	
43	AIA	Technical	NIST SP 800-171r3 fpd	25	868	Changing the wording from "and/or" to "and" changes the scope to require defining all of those vs. some.	Changing the wording from "and/or" to "and" changes the scope to require defining all of those vs. some.	3.4.6	
44	AIA	Technical	NIST SP 800-171r3 fpd	25	868	Change the order for b, c, and d to be in alphabetical order to help in finding easily in 171A	Change the order for b, c, and d to be in alphabetical order to help in finding easily in 171A	3.4.6	
45	AIA	Technical	NIST SP 800-171r3 fpd	25	868	Why the removal of "software"? Need to identify the relationships between controls.	Add relationships between requirements.	3.4.6	
46	AIA	Technical		25	872	3.4.6[D] seems redundant when you have [B] that says nearly the same thing.	Please remove 3.4.6[D].		
47	AIA	Technical	NIST SP 800-171r3 fpd	26	897	Why drop "authorized" from (b) when still listed in c?	Add "authorized" back to b. for consistency	3.4.8	
48	AIA	Technical	NIST SP 800-171r3 fpd	26	922	It doesn't seem that a nor c are addressed in any of the listed controls as where it is addressed.	Validate that all requirements withdrawn and implemented in other controls are actually there or describe why removed.	3.4.9	
49	AIA	Technical	NIST SP 800-171r3 fpd	27	944	Why not have "identify and document" on c to be consistent with a and b?	Add "identify and document" on c.	3.4.11	
50	AIA	Technical	NIST SP 800-171r3 fpd	27	950	What does "changes to the location" mean? Is this change management or config management?	Add to the Discussion section what "changes to the location" mean as well as examples to add clarity	3.4.11	
51	AIA	Technical	NIST SP 800-171r3 fpd	27	950	3.4.11[C] is this test a duplicate of 3.1.2?	Please clarify the differences between 3.4.11[C] and 3.1.2. Also, if you are doing [A], you are automatically doing [C].		
52	AIA	Technical	NIST SP 800-171r3 fpd	27	965	3.4.12[B] Please provide a real time list on NIST's website of countries that are considered "high risk" for business travellers who may have CUI on their laptop or mobile device.	Please provide a real time list on NIST's website of countries that are considered "high risk" for business travellers who may have CUI on their laptop or mobile device. Alternatively, provide in the discussion a reference to the government agency that maintains such list.		

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay, 171A)	Starting Page #*	Starting Line #*	Comment (include rationale)*	Suggested Change*	Requirement #	Requirement Text
53	AIA	Technical	NIST SP 800-171r3 fpd	28	1001	Why was "network" dropped? Is the assumption that a system connection can be either local or network? Make sure in discussion.	Update the Discussion to identify that this includes local and network connections.	3.5.2	
54	AIA	Technical	NIST SP 800-171r3 fpd	29	1017	This may require more MFA to devices due to changes in wording. Does this increase scope?	Add clarification to the Discussion to identify if this is for all accounts within a system which could be different per device.	3.5.3	
55	AIA	Technical	NIST SP 800-171r3 fpd	29	1017	Is this only to CUI systems or all systems as not explicitly called out for only CUI?	Add clarification to the Discussion to identify if this is for all systems or only those with CUI or support CUI	3.5.3	
56	AIA	Technical	NIST SP 800-171r3 fpd	29	1019	3.5.3 Please define "system accounts". This is unnecessarily vague.	Please be specific with what NIST considers a "system account". System accounts can be interpreted as being a "service account", which may not log on interactively for MFA. The discussion in line 164 regarding system accounts includes many types of accounts, which do not all typically support MFA.		
57	AIA	Technical	NIST SP 800-171r3 fpd	29	1032	3.5.4 provides limited value in the present day because modern business operating systems have this built in. Air gapped environments have a compensating control in meeting this control by not being connected to anything else.	Improve the discussion for this control to address air-gapped systems.		
58	AIA	Technical	NIST SP 800-171r3 fpd	29	1043	Why is "uniquely" in d and not as part of b? Shouldn't it be "Select and uniquely assign an identifier"?	Change to "Select and uniquely assign an identifier"	3.5.5	
59	AIA	Technical	NIST SP 800-171r3 fpd	29	1043	What does d mean "uniquely identify the status .. With identifying characteristic" mean or provide? Per discussion, identifying characteristic is contractor, that is not unique to a certain person as there will be multiple contractors in an org. There should be a better word and/or remove uniquely from d.	Reword for better clarification of the intent such as "Uniquely identify the employment status and type of employment of each individual with identifying characteristics" as this would be in line with the Discussion.	3.5.5	
60	AIA	Technical	NIST SP 800-171r3 fpd	30	1047	3.5.5[B] is this the same as 3.5.1[A]? What is being asked for is confusing.	Please explain what you're looking for with 3.5.5[B] because it is vague.		
61	AIA	Technical	NIST SP 800-171r3 fpd	30	1062	Why did a get moved to f?	Changes to ordering from previous versions, even drafts, should be explained for the intent.	3.5.7	
62	AIA	Technical	NIST SP 800-171r3 fpd	30	1062	Why was wording of f changed from "password composition and complexity rules" to "composition and complexity rules for passwords"?	Changing the wording should be explained even if supposed to help with clarity.	3.5.7	
63	AIA	Technical	NIST SP 800-171r3 fpd	30	1064	3.5.7[A] where are we supposed to get this from? If this is a service which needs to be subscribed to and connected to AD to prevent these passwords from being used, it will be difficult to achieve for SMBs and will increase the maintenance overhead for all DIB members.	Remove this test. It does not provide cyber value for organizations to maintain and update a list of passwords. The risk of password compromise is mitigated by the use of MFA. The use of complexity is also a compensating control to mitigate the risk.		
64	AIA	Technical	NIST SP 800-171r3 fpd	31	1112	Does this mean if not during the authentication process then obscuring feedback does not need to be performed?	Explain why the additional context was added or revert back to the original.	3.5.11	
65	AIA	Technical	NIST SP 800-171r3 fpd	34	1205	3.6.4 seems to be duplicative of what is being called out in 3.2.2. Especially since this training is for end users and not CSIRT personnel.	Please add this to the AT Family as a new control, there is no reason to have training in multiple families		
66	AIA	General	NIST SP 800-171Ar3 ipd	34	1456	Being uniquely identified and authenticated are two distinctly different objectives.	Split this assessment objective into two separate assessment objectives. One that looks for "uniquely identified" and one that looks for "authenticated" to be consistent with other assessment objectives		
67	AIA	Technical	NIST SP 800-171r3 fpd	35	1237	How would I inspect maintenance tools (especially digital) for improper or unauthorized modifications effectively?	Explain in discussion if this is for only internal maintenance tools or also for external/vendor tools and provide additional discussion relating to how to inspect external/vendor maintenance tools against a hash or signature when the organization doesn't control or have that information.	3.7.4	
68	AIA	General	NIST SP 800-171Ar3 ipd	35	1480	Being uniquely identified and authenticated are two distinctly different objectives.	Split this assessment objective into two separate assessment objectives. One that looks for "uniquely identified" and one that looks for "authenticated" to be consistent with other assessment objectives		

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay, 171A)	Starting Page #*	Starting Line #*	Comment (include rationale)*	Suggested Change*	Requirement #	Requirement Text
69	AIA	Technical	NIST SP 800-171r3 fpd	36	1305	Was the intent to drop physical/non-digital media due to being encompassed in another requirement or that only digital/system media is relevant?	Provide additional information in the discussion and relationships to other requirements.	3.8.1	
70	AIA	Technical	NIST SP 800-171r3 fpd	37	1334	Why remove maintenance?	Either add "maintenance" back in, provide references to the relationships where maintenance is covered in other requirements or identify why it was removed.	3.8.3	
71	AIA	Technical	NIST SP 800-171r3 fpd	38	1350	Why drop the exemptions?	Either add exemption tracking requirements back in, provide references to the relationships where maintenance is covered in other requirements or identify why it was removed.	3.8.4	
72	AIA	Technical	NIST SP 800-171r3 fpd	38	1365	Assuming that dropping the cryptographic requirements for digital media is encompassed in another requirement but needs validation and should also be identified in the relationships and discussion of this requirement.	Discuss why cryptography requirements dropped and identify the relationships between requirements	3.8.5	
73	AIA	Technical	NIST SP 800-171r3 fpd	38	1365	Discussion identifies cryptographic mechanisms but the requirement no longer requires cryptography	Update discussion or update the requirement for consistency	3.8.5	
74	AIA	Technical	NIST SP 800-171r3 fpd	38	1370 - 1382	3.8.5 there is no mention of keeping a log of media being transported, except in the Discussion section. Our assessors are trained to ask for a log of media sent out or received. Additionally, the control does not make a distinction between media where cryptographic mechanisms are used to protect confidentiality, versus unencrypted media.	This control should explicitly state a requirement to keep a log of media transport that can be provided to an auditor upon request, if the intent of the control is that accountability includes "tracking or obtaining records of transport".		
75	AIA	Technical	NIST SP 800-171r3 fpd	39	1422	Discussion point of "Backup storage locations may include system-level information and user-level information." seems to be discussing the information that may contain CUI, and not the backup storage locations themselves.	Change to describe backup storage locations (data center, offsite storage, onsite secure storage).		
76	AIA	General	NIST SP 800-171Ar3 ipd	39	1629	Established and implemented are two different objectives and should be separated.	Split the assessment objective into one that reviews "established" and one that reviews "implemented" as they are two different things and makes consistent with other assessment objectives		
77	AIA	General	NIST SP 800-171Ar3 ipd	39	1631	Established and implemented are two different objectives and should be separated.	Split the assessment objective into one that reviews "established" and one that reviews "implemented" as they are two different things and makes consistent with other assessment objectives		
78	AIA	General	NIST SP 800-171Ar3 ipd	39	1633	Established and implemented are two different objectives and should be separated.	Split the assessment objective into one that reviews "established" and one that reviews "implemented" as they are two different things and makes consistent with other assessment objectives		
79	AIA	Technical	NIST SP 800-171r3 fpd	40	1434	Concerns depending on who identifies the conditions requiring rescreening and need to define within our own documentation.	Remove ODP and make the requirement "Rescreen individuals in accordance with organization defined conditions requiring rescreening" so that it can be defined by the organization.	3.9.1	
80	AIA	Technical	NIST SP 800-171r3 fpd	40	1437	3.9.1 is vague and it can be interpreted as all employees, including corporate employees who do not handle CUI, which is an administrative burden and does not provide significant cyber value. Is the intent to allow the organization to develop risk-based criteria for rescreening only certain individuals in certain conditions, such as privileged users changing roles?	Please be more specific with who needs to be re-screened.		
81	AIA	Technical	NIST SP 800-171r3 fpd	40	1448	Change B2 ODP to "transfer or reassignment actions"	Change B2 ODP to "transfer or reassignment actions" for consistency with the requirement.	3.9.2	
82	AIA	Technical	NIST SP 800-171r3 fpd	42	1501	Why remove "upon occurrence of defined or potential events" especially when the digital side still requires them? Recommend re-adding for consistency.	Modify b to contain "upon occurrence of organization-defined events or indication of events".	3.10.2	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay, 171A)	Starting Page #*	Starting Line #*	Comment (include rationale)*	Suggested Change*	Requirement #	Requirement Text
83	AIA	Technical	NIST SP 800-171r3 fpd	42	1501	Why remove coordination? Is the assumption that this is part of the other requirements for incident response? Make sure comments in Discussion.	Discussion still gives information on incident response and thus the coordination requirement should be re-added or the discussion should be updated to remove incident response discussion and identify the relationship with the incident response requirements	3.10.2	
84	AIA	Technical	NIST SP 800-171r3 fpd	42	1521	Model states 3.10.7 not 3.8.7 so need to fix the analysis spreadsheet	Model states 3.10.7 not 3.8.7 so need to fix the analysis spreadsheet	3.10.3	
85	AIA	Technical	NIST SP 800-171r3 fpd	42	1523	Model states 3.10.7 not 3.8.7 so need to fix the analysis spreadsheet	Model states 3.10.7 not 3.8.7 so need to fix the analysis spreadsheet	3.10.4	
86	AIA	Technical	NIST SP 800-171r3 fpd	42	1525	Model states 3.10.7 not 3.8.7 so need to fix the analysis spreadsheet	Model states 3.10.7 not 3.8.7 so need to fix the analysis spreadsheet	3.10.5	
87	AIA	Technical	NIST SP 800-171r3 fpd	42	1527	Why remove "document"? Assuming that documentation is part of the requirement implicitly?	Readd "and document" for consistency with other requirements or identify the relationship with other requirements.	3.10.6	
88	AIA	Technical	NIST SP 800-171r3 fpd	43	1542	Change a2 to "systems, devices" by replacing the slash with a comma.	Change a2 to "systems, devices" by replacing the slash with a comma.	3.10.7	
89	AIA	Technical	NIST SP 800-171r3 fpd	44	1606	Assumption that removal of d is due to ODP for security functions previously.	Identify why d was removed	3.11.2	
90	AIA	General	NIST SP 800-171Ar3 ipd	44	1808	multi-factor and replay resistant are two different and distinct requirements and should be separated into two distinct assessment objectives	separate the assessment objective into 2; one for MFA and one for replay resistance for consistency with other assessment objectives		
91	AIA	Technical	NIST SP 800-171Ar3 ipd	46	1653	3.12.2[A1] and 3.12.2[A2] do not make this control stronger, it seems like excess text. This would be better off in the discussion (line 1661) instead of a test.	Remove these tests and add them to the discussion for 3.12.2.		
92	AIA	Technical	NIST SP 800-171Ar3 ipd, NIST SP 800-171r3 fpd	46	1658	The requirement for independent audits and reviews was removed as a requirement in the FPD that existed in the IPD but 3.12.2 requires that POAMs are to be periodically updated based on security assessments, independent audits/reviews AND continuous monitoring activities and thus adds an additional requirement per 171A that is implied in 171.	Remove "independent audits or reviews" from the requirement since independent audits are no longer required.		
93	AIA	Technical	NIST SP 800-171r3 fpd	47	1686	b could have some major impacts on getting a satisfied for the control as most SLAs do not get to that level of detail. Therefore, new documentation will likely need to be created when CUI is involved.	b could have some major impacts on getting a satisfied for the control as most SLAs do not get to that level of detail. Therefore, new documentation will likely need to be created when CUI is involved.	3.12.5	
94	AIA	Technical	NIST SP 800-171r3 fpd	47	1712	Is connecting to external services considered an external system?	Add "and services" after "external systems" in c.	3.13.1	
95	AIA	Technical	NIST SP 800-171r3 fpd	49	1771	Crypto at rest is major uplift for many. The requirement in rev2 had limitations and alternatives but now requires that all "at rest" data on the systems in scope with CUI be encrypted regardless of location and will add significant cost.	Re-addd "unless otherwise protected by alternative physical safeguards"	3.13.8	
96	AIA	Technical	NIST SP 800-171r3 fpd	50	1806	Is this assuming that cryptography is implemented everywhere based on other requirements?	Change "in the system" to "used in the system"	3.13.10	
97	AIA	Technical	NIST SP 800-171r3 fpd	51	1832	Where are exeptions handled? Is this part of the overall configuration guidance/management? If so, then should be in discussion.	Either add exemption tracking requirements back in, provide references to the relationships or put the information in the Discussion relating to them.	3.13.12	
98	AIA	Technical	NIST SP 800-171r3 fpd	51	1846	Why the change of order of control and monitor from ipd?	Describe the change.	3.13.13	
99	AIA	Technical	NIST SP 800-171r3 fpd	52	1882	Why drop b?	Either add back in or describe why changed.	3.14.1	
100	AIA	Technical	NIST SP 800-171r3 fpd	53	1903	Isn't c2 redundant with a? If want to keep in, remove "eradicate" from a and leave in c2.	Isn't c2 redundant with a? If want to keep in, remove "eradicate" from a and leave in c2.	3.14.2	
101	AIA	Technical	NIST SP 800-171r3 fpd	56	2032	For a1, what is the point of "constituent system components"? Rewords to "Defines all system components"?	For a1, what is the point of "constituent system components"? Reword to "Defines all system components" or make sure concise definition exists in the glossary and Discussion.	3.15.2	
102	AIA	Technical	NIST SP 800-171r3 fpd	58	2094	Removal of "or" means both have to be done now.	Put the "or" back into the requirement per IPD.	3.16.2	
103	AIA	General	NIST SP 800-171Ar3 ipd	59	2328	developed and implemented are two different objectives and should be separated.	Split the assessment objective into one that reviews "developed" and one that reviews "implemented" as they are two different things and makes consistent with other assessment objectives		
104	AIA	Technical	NIST SP 800-171r3 fpd	60	2175	Why the reordering of identify and protect against?	Document why the change was made.	3.17.2	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay, 171A)	Starting Page #*	Starting Line #*	Comment (include rationale)*	Suggested Change*	Requirement #	Requirement Text
105	AIA	General	NIST SP 800-171r3 fpd, 3.17.03b	60		The control listed is just an example. But for ANY control with an ODP what is preventing the "organization" from defining the ODP as something that is inherently way more restrictive than the intent of 800-171. Specifically for 3.17.03b you could be required to force supply chains to meet all of 800-53 r5.	1. PREFERRED - Remove ODP Requirements. 2. Provide guidance on how and ODP should be identified and defined by the "organization." It would also be good to create a list of generally accepted ODPs.		
106	AIA	General	NIST SP 800-171Ar3 ipd	60	2358	approved and managed are two different objectives and should be separated.	Split the assessment objective into one that reviews "approved" and one that reviews "managed" as they are two different things and makes consistent with other assessment objectives		
107	AIA	General	NIST SP 800-171Ar3 ipd	77	3003	All 3 of these assessment objectives should be split into their respective items instead of combining them. Acquisition strategies, contract tools, and procurement methods are 3 distinct items and should be separated to be consistent with other requirements such as with the ports, protocols, and services.	Split the 3 assessment objectives into 9 assessment objectives that coincide with "acquisition strategies", "contract tools", and "procurement methods" to be consistent with other requirements.		
108	AIA	General	NIST SP 800-171Ar3 ipd	78	3034	Identifying and addressing are distinct and should be separated into separate assessment objectives for consistency.	Split the assessment objective into 2. One for "identifying" and one for "addressing".		
109	AIA	Technical	NIST SP 800-171r3 fpd			Controls added or removed	Make sure documentation of why controls were added or removed is described in the missing Appendix		
110	AIA	General	sp800-171r2-to-r3-fpd-analysis		88	Control 3.10.08 is listed as having an ODP requirement, but I do not see any ODP in the r3-fpd document.			
111	AIA	General	FAQ			Many requirement changes remove monitoring and controlling and others remove cryptographic requirements and assuming that is because they are covered by other requirements such as 3.13.1 and 3.13.8 but without anything in the FAQ, it seems that they are not longer required.	FAQ needs to be updated to include why the removal of control and monitoring for external as well as cryptographic protections were removed from specific requirements as they are covered by other requirements such as 3.13.8		
112	AIA	General	NIST SP 800-171r3 fpd			It is hard to find reasons why something changed or modified since the primary search information is based on 800-53 numbering and not 800-171 and since the overlay only lists the current version of 171r3 draft and not the IPD nor r2, comparisons are not available.	When releasing drafting documents, the review and changes should be documented compared to the prior final release version and any prior draft releases to help reviewers identify the changes quickly and efficiently for better comments.		
113	AIA	General	NIST SP 800-171r3 fpd			In some controls, there are references to other controls but not in others that seem like they should such as for cryptography and external/remote access requirements.	Go through requirements and add consistency by relating requirements to each other.		
114	AIA	General	NIST SP 800-171r3 fpd			Relationships of controls is not documented very well.	Go through requirements and add consistency by relating requirements to each other.		
115	AIA	General	NIST SP 800-171r3 fpd			Discussions should identify relevance to ODPs	Any control/requirement that has an ODP should have a portion of the Discussion section that specifically discusses the intent and importance of the ODP		
116	AIA	General	NIST SP 800-171r3 fpd			Discussions should identify control relationships.	Go through requirements and add consistency by relating requirements to each other.		
117	AIA	General	Overlay			The filtering and identifications of the different tailoring criteria is confusing and doesn't show comparisons to previous versions.	Update the Overlay to provide additional details or an additional sheet for anyone who is moving from an old version (or comparing an older version) so that additional insights can be gained. This should include adding and/or removing of sub-requirements (a, b, c) as well as changing of words/wording (add/remove/etc.)		
118	AIA	General	NIST SP 800-171r3 fpd			Why is ORC only used in conjunction with tailoring and not within 171 as many of the controls are covered by others, and/or are related?	Go through requirements and add consistency by relating requirements to each other and highlight ORC.		
119	AIA	General	NIST SP 800-171r3 fpd			Many ODPs were changed to "periodically" but this is not defined anywhere within the document/glossary.	Define "periodically" as "at most yearly or annually" to set expectations and identify what is required from other requirements.		
120	AIA	General	NIST SP 800-171Ar3 ipd			The reasoning for splitting of the requirements into assessment objectives seems to be inconsistent.	Go through all of the assessment objectives and make consistent by splitting out several that have distinct "and" objectives for requirements that are different for evaluating.		

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay, 171A)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*	Requirement #	Requirement Text
121	AIA	General	NIST SP 800-171Ar3 ipd			There are many instances where the assessment objective requires "defined and documented" while there are others that only state "defined". What is supposed to be the difference between the two?	Make consistent throughout the document. Either set as "defined" or as "defined and documented" and not have a mix of both.		
122	AIA	General	NIST SP 800-171Ar3 ipd			There are many instances where the assessment objective requires "identified and documented" while there are others that only state "defined". What is supposed to be the difference between the two?	Make consistent throughout the document. Either set as "identified" or as "identified and documented" and not have a mix of both.		
123	AIA	General	NIST SP 800-171Ar3 ipd			the lack of the overarching requirement(s) from 800-171 not residing in 800-171A can make it difficult to identify/understand what is being asked and to verify against the original requirement.	put the original 800-171 requirements in the 800-171A document next to the requirement number for ease of reference and review		
124	AIA	General	NIST SP 800-171r3 fpd			All of the discussions should include a section/area that describes the "Impact if this requirement is not yet implemented" similar to what was in the DoD document "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 11-6-2018.pdf".	Update the descriptions to describe the impact if not yet implemented as well as what attack vectors that are being minimized/blocked.		
125	AIA	General	NIST SP 800-171r3 fpd			The categorization of the requirements is based off of their requirement family (as in previous publications), though would it be possible to categorize the requirements based on the similarities in their processes for obtaining compliance? For instance, which requirements are accomplished from utilizing the system resources v.s. which are fulfilled with physical resources? Are their processes that can be aggregated based on the "How" they accomplished, v.s. which requirement family they belong to?	Look into the processes for each security requirement family and aggregate which processes require a digital solution (using system resources) v.s. processes that can only be accomplished physically (potentially in 3.9 and 3.10). Thinking this could be a way to suggest automation for the digital solution requirements to align with digital transformation capabilities in order to hasten compliance processes.		
126	AIA	General	NIST SP 800-171r3 fpd			Is there any way that data is collected to see how the different requirements are met across different industries within the DIB? I would imagine this might be a helpful resource when updating documentation of 171. Comments are qualitative support for update, but where are we collecting quantitative support for how to better update these policies in order to better meet the needs of the organizations following these guidelines?	Recommend looking into a survey or metrics collection from the DIB community that would help provide quantitative measurements on how to best update the 171 policy in order to capture wholistic and diverse feedback from the DIB v.s only qualitative comments.		
127	AIA	General	NIST SP 800-171r3 fpd			CISA CRR (Cyber Resilience Review) is an interesting resource that seems to aggregate the requirements of an assessment at a high level. --- https://www.cisa.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf --- I wonder if there was a way to show the comparison of each resource from a tacticle standpoint so that the barrier to entry for protecting CUI is lower for small to medium sized companies. NIST provides the details needed for more mature businesses to follow, but what about the 60% of our supply chain that is comprised of SMEs? How can we better support them?	Leverage material from other agencies that address protecting CUI and cyber maturity so that SMEs can uplift (assuming they have little to no experience in doing so) so that basic requirements are easier understood and we can better meet the SMEs at their level.		
128	AIA	General	NIST SP 800-171r3 fpd			Is there a better way to collect comments so that comments can be aggregated and automated to save time for NIST staff review and quicken the turn-around time?	Explore digital transformation in the ways in which NIST publications (171) are updated with DIB feedback. Consider solutions that enable automation in order to keep up with the rapidly evolving landscape of technology.		
129	AIA	General	NIST SP 800-171r3 fpd + 171A			Industry often criticizes the government generally for too much variance in cyber guidance. Thank You for aligning assessment procedures in NIST SP 800-171A more closely with the requirements in NIST SP 800-171.			
130	AIA	General	NIST SP 800-171r3 fpd			Small, medium and large businesses all appreciate the efficiencies in Rev 3. However, the assessment objectives appear to have increased significantly. Highly recommend removing any perceived excessive or duplicative assessment objectives in final version to get ahead of industry concerns; as you know, industry is also responding to proposed FAR rules and (hopefully) CMMC final proposed rule. Industry is very supportive of consistent cyber requirements to monitor/reduce pertinent risks in the ecosystem. We appreciate NIST's commitment to helping their customers succeed.			