From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Cc:	[redacted]
Subject:	[800-171 Comments] Revised: 800-171 Rev 3 FPD Comments
Date:	Friday, January 26, 2024 8:29:06 PM
Attachments:	Security Council NIST 800-171R3 Comment Ltrfinal.pdf sp800-171r3-fpd-comments-FFRDC_SEC_COUNCIL.pdf sp800-171r3-fpd-comments-FFRDC_SEC_COUNCIL.xlsx

Revised submission with digitally signed letter.

Ron and Victoria, attached find:

- A letter of submission from the FFRDC UARC Security Council CUI Working Group
- 800-171 Rev 3 FPD public comments using NISTs Excel template & a PDF version as well

On behalf of the FFRDC UARC Security Council CUI Working Group, we appreciate the opportunity to provide comments.

Warmest regards,

NOTE: I routinely send and reply to emails at irregular times for my personal convenience. Please do not feel obligated to read, act or reply outside of your working hours.

Dawn Greenman, CISSP
JHU/APL
ITSD Cybersecurity Compliance and SCRM Program Manager
[redacted]

FFRDC/UARC

Security Council

January 26, 2024

Submitted via: 800-171comments@list.nist.gov

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: **Comments to NIST SP 800-171 Rev 3 Final Public Draft**

Dear Sir/Madam:

On behalf of the FFRDC/UARC Security Council and its CUI Working Group, we are respectfully submitting comments in response to the NIST SP 800-171 Rev 3 Final Public Draft.

The 20 FFRDCs and UARCs represented by this council thank you for the opportunity to provide comments.

Sincerely,

HAWK.JASON.K.1035285560 Digitally signed by HAWK.JASON.K.1035285560
Date: 2024.01.26 16:05:20 -05'00'

Jason Hawk
Chair
Board of Directors
https://ffrdc-uarc-sc.org/

The purpose of the FFRDC/UARC Security Council is to share information and best practices amongst its members (consisting of 20 FFRDCs and UARCs) across all security disciplines to promote effective and efficient risk management practices, and to also serve as a voice to government as to the modification of existing and the creation of new security policies and implementing guidance.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	2	31	Clarify the applicability statement. Should this be "AND" instead of "OR"?	Change "or" to "and" **Rephrase to**: “The security requirements in this publication are only applicable to nonfederal systems that process, store or transmit CUI, **and** the security components that provide protection for such components.”

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
2	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	2	31	Is this the same as CMMC's Security Protection Assets? If yes, please add definition and use the same term. Provide examples of components that "provide protection" similar to footnote 9 showing examples of components. In Discussion clarify if physical security systems are scope? Does the the applicability of "components that provide protection" include badging systems (physically isolated or not) that do not contain or process CUI are applications run on servers or workstations to provide a security function (PE). Or, does it apply only to components in footnote 9.	**Define**: Define components covered under this requirement (to include clarifying if physical access security control systems are in scope) **Create a new term if applicable:** Security Protection Assets

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
106	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	4	80	NIST should consider utilizing their existing approach for 800-53 comments when the 800-171 requirements are finalized. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/public-comments#/home This would allow for a more agile approach to address risk. Further, the ability to see new candidate proposed changes and public comments submitted should reduce the burden adjudicating comments that have already been submitted. An additional capability on the NIST website that may also could be a mechanism for the public to “like” certain comments and / or add risk ratings (with evidence) to add to the “priority” of the requirement.	Utilize existing 800-53 comment process to collect 800-171 comments: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/public-comments#/home

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
92	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	4	89	ODPs should not be left to be defined by federal agencies. DIB companies who work for multiple government agencies will be at the mercy of implementing the "most restrictive" requirements of the federal agency who decides to require "ODPs" that are burdensome and / or do not account for the differences of organizations	ODPs should be developed by committee of non-federal agencies who understand the complexities of different networks and environments.
5	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	5	118	3.13.11 - The phrase "context dependent" is unclear. None of the references in the draft provide any context, and this statement doesn't either.	Either remove the sentence "The meaning of the term…" OR be explicit about how the contractor can understand what values to use.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
6	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	5	119	3.13.11 - The term "nonfederal organization establishing the parameter values" is unclear. Can this be the contractor establishing its own values? Or is it always intended to be an organization who provides the contractor its information? If it's the former, it needs to be explicit so the contractor knows it is responsible for establishing these values. If it's the latter, the language should be explicit that this is NOT to be set by the contractor, but provided to the contractor.	Clarify the term "nonfederal organization" to indicate if this is a) never the contractor, b) sometimes the contractor and sometimes the sponsoring organization, or c) always the sponsoring organization.
7	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	6	152	3.1.1 - Inactivity alone is not a valid metric for determining whether an account is still needed. Emergency accounts may go unused for long periods of time, but are still valid and should stay enabled.	(f2) should read "The accounts have been inactive for [ODP] **AND are no longer needed."**

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
8	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	6	154	3.1.1 - The phrase "organizational policy" here is unclear. Is this an ODP? What kind of organizational policies would there be that aren't covered in (f)?	Remove (f4) **or add clarity in discussion**
104	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	9	256	3.1.5 (b) is unclear. Authorize access to "the network"? Is this about role based access controls?	Provide examples in the Discussion to clarify what "authorize access to X" means e.g., "CUI Users are authorized access to the CUI enclave. (others are not)" or "Firewall Administrator accounts are authorized to access firewalls" (non Firewall Admins are not).
9	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	9	258	3.1.5 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically".
10	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	16	258	3.1.22 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
105	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	9	265	3.1.5 Discussion - "Security functions" in the document uses "installing software" as an example. Assumption this is not the same as "user accounts" permitted to install approved software.	Add to Discussion language from 800-171 R2 which helps clarify. "Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
11	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	9	278	3.1.6 - Recommend rewording the requirement as the double (and now triple) use of “non” ("non-privileged accounts", "nonsecurity functions", "nonsecurity information") has always been a point of confusion for our team and system owners we work with. We always need to take extra time to explain this requirement due to how it is worded. The addition of "nonsecurity information" does not help clarify this requirement.	Change language to something similar to: Require that users (or roles) with privileged accounts do not use those accounts to perform duties that do not require the elevated permissions.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
12	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	10	315	3.1.8 The number of invalid attempts may be different depending on the system. Using ODPs here might be OK for most logins, but need to be flexible enough that logins still accommodate user accessibility. ODPs would also force contractors with multiple sponsoring agencies to use the most restrictive value, affecting all users.	Remove ODP.
13	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	11	327	3.1.9 - Suggest adding "or banner" to clarify requirement	Change language to: "Display a system use notification message or banner…"
14	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	11	347	3.1.10 Are there any use cases where a device lock is engaged and CUI would still be viewable? We could not think of any.	If no use cases, recommend removing requirement c as it appears unnecessary/redundant.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
15	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	12	364	3.1.11 - Using an ODP is problematic for contractors who support multiple organizations, as the contractor would need to convert all access to the least restrictive values, even if mitigating controls are in place.	Remove ODP.
16	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	14	441	3.1.18 - Revert to prior language "organization-controlled mobile devices". Why was "organizationally controlled" removed? Was it intended for the control to apply to organizational AND user-owned mobile devices? If only the former, please clarify by re-adding the language.	Change "Mobile Devices" to "Organization-Controlled Mobile Devices".

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
17	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	15	478	3.1.20 The previous draft had "access the system from external systems" and "process, store or transmit CUI using external systems". The new language in (a) and (b) indicates that just using an external system, for any reason, with or without CUI, is somehow a violation.	(a) and (b) should have the phrase "use of external systems to access organizational systems" in place of "use of external systems".
95	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	15	480	3.1.10 Use of External Systems a. Prohibit the use of external systems unless the systems are specifically authorized.	Clarify the definition of system in this control. Is this related to applications, devices, etc.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
96	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	15	481	3.1.20 b. Clarification requested: Organizational agreements and policies can address requirement; Example: contract, subcontracts, interconnection agreements, MOUs, NDAs, etc. which define required protection requirements, can be used to meet "terms, conditions, and security requirements" to be satisfied on external systems prior to allowing use of or access to those systems. b. Can a user login page with a banner satisfy the requirement?	Clarify definition of external system. Provide policy examples in guidance to include if a login banner with details will suffice.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
100	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	16	517	3.1.22 Recommend adding clarity to both 800-53 R5 and 800-171 R3 AND the assessment guides that the review is required on public systems owned or operated by the by the non-federal organization.	**Reword:** Review the content on organizationally owned and operated publicly accessible systems for CUI *periodically* and remove such information, if discovered. **Add to discussion**: Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication.
18	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	16	530	3.2.1 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
19	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	16	531	3.2.1 (a2) remove or allow organization policies to address the who and when its applicable. Enterprise security training is time-consuming and expensive (often utilizing a vendor), and not feasible on an ad hoc basis. Ad hoc training (based on events) is more appropriate for role-based training.	Remove (a2).
20	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	16	533	3.2.1 (a3), the "on recognizing" phrase doesn't make sense.	Change the phrase to something like "Training should include how to recognize and report potential indicators of insider threat."
21	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	16	535	3.2.1 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
22	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	17	576	3.2.2 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
23	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	17	579	3.2.2 (b), this should say "review and update" since it's possible the review will determine that no updates are needed.	Change (b) to "Review and update role-based…"
24	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	17	579	3.2.2 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
25	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	18	603	3.3.1 (a) ODP defined by federal agencies or sponsors would be extremely challenging for contractors who support multiple sponsors on the same system, since event types would have to include every type of event suggested by every sponsor. This control shouldn't be defined by the sponsoring federal organization, it should point to best practices to identify an adversary on the network or to an industry standard set of requirements.	Remove ODP.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
27	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	18	603	3.3.1 (a) clarify by providing logs recommended to collect, where technically feasible, and in accordance with regulations. Many small businesses will not understand what logs to collect that provide visibility during a cyber attack. Reference to need to adhere to logs required by various regulations (eg., Privacy, etc)	Add best practice reference for logs to collect to identify an incident on a network.
26	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	18	605	3.3.1 (b) "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Add clarity the non-federal organization defines the periodicty within an acceptable Define upper and lower paramaters around "periodically"
28	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	19	636	For (b), this language is extraneous and adds nothing to the underlying security control.	Remove (b).
29	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	19	651	3.3.3 (b) reference to "consistent with records retention policy" is a good example of how to address periodicity	change periodicity statements to say ***"...for a time period consistent with organizational policy."*** Discussion: organizational policy must be written to address regulatory requirements

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
30	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	20	686	3.3.5 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
31	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	21	711	3.3.6 (a), the language after "review" is unnecessary, as all of these things are just outcomes of review. Any audit records will support all of these things by default.	In (a), end sentence after "audit record review".
32	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	21	730	3.3.7 Is this (b1) OR (b2) OR (b3), or is it (b1) AND (b2) OR (b3)?	Change text to make it extremely clear where the or is intended to be applied.
33	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	22	751	3.3.8 (b) is clunky.	Change (b) to: "Restrict audit log management functionality to a subset of privileged users/roles." OR "Restrict management of audit logging to a subset of privileged users/roles."
34	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	22	774	3.2.2 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
103	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	23	790	3.4.2 (a) The level of detail should be flexible for the organization. The risk of government defining it when supporting multiple sponsors is problematic. It is unreasonable to specify every single setting on a large organizations hosting a myriad of devices. Rev 2 language was sufficient for this: Establish and enforce -- without fully documenting every setting.	**Remove ODP** **or** **Reword to Rev 2 language:** Establish and enforce security configuration settings for information technology products employed in organizational systems.
36	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	23	793	3.4.2 "Identify" is unnecesary in this sentence.	Remove "identify" and start sentence with "Document…"
37	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	25	867	3.4.6 - "Mission-essential capabilities" is overly DoD-focused.	Change "mission-essential" to "essential".

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
38	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	25	868	3.4.6 -For (b), the ODP is untenable for contractors with multiple sponsors, as it would require enclaves to support multiple ODPs. This is especially problematic as mechanisms for managing large networks require some degree of standardization, and applying customized restrictions is not feasible on a per-server basis. A reasonable baseline needs to be developed for enterprise deployments which cannot be overly restrictive.	Combine (a) and (b): "Establish and enforce organizational policies for prohibitions and restrictions on the use of functions, ports, protocols, connections, and services." Combine (c) and (d): "Periodically review and disable any functions, ports, protocols, connections and services that are unnecessary or insecure."
39	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	25	870	3.4.6 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
40	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	26	897	3.4.8 line 897 should rephrase back to Rev2 version with "deny or allow by exception"	Revert back to: Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software **or** deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
41	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	26	899	3.4.8 - "periodically" is not defined. Non-federal Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
42	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	26	927	3.4.10 - "periodically" is not defined. Non-federal Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
43	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	27	948	3.4.11 (b) is not relevant to a control for "Information Location", and is redundant with earlier access-related controls.	Remove (b).
44	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	28	997	3.5.1 - "periodically" is not defined. defined. Non-federal Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
45	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	29	1019	3.5.3 - Non-user accounts do not use MFA, whereas this requirement implies all access to system accounts will be via MFA.	Change to "for user access to system accounts."

* indicate required fields

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
46	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	30	1048	3.5.5 - Controls c and d should be reversed (as in 800-53 Rev 5). This ensures that organizations managing SSPs for 800-53 and 800-171 can keep responses in order for templates	Flip controls c & d
47	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	30	1049	3.5.5 - (d), is not clear what a "status" is. Employment status? Online status? What does this have to do with the identifier that matches the individual to an account? HR should definitely know the status of personnel, but that's out of scope for this control.	Remove (d).
48	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	30	1065	3.5.7 - "periodically" is not defined. Non-federal Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
49	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	30	1066	For (b), this is viable for enterprise passwords, but cannot always be implemented on COTS systems.	Change (b) to: "Where feasible, verify that new passwords are not found on the list from 3.5.7a.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
50	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	30	1069	For (d), this is redundant with the new language in 3.5.12f Authenticator Management.	Remove (d), or incorporate into 3.5.12.
51	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	32	1119	3.5.12 - "periodically" is not defined. Non-federal Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
52	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	32	1121	3.5.12 - For (f), this control is redundant with (d) in 3.5.7.	Remove (f), or incorporate with 3.5.7.
53	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	33	1170	3.6.2 - For (b) and (c), this may be impossible for contractors with multiple sponsors to comply with, since incidents with one sponsor's data should not necessarily be reported to another's sponsors sources.	Remove ODP, or note in (c) that only incident information relevant to an organization's data is relevant for reporting to the organization-defined authorities.
54	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	33	1194	3.6.3 - "periodically" is not defined. Non-federal Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
55	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	34	1212	3.6.4 - "periodically" is not defined. Non-federal Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
56	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	34	1213	3.6.4 - "periodically" is not defined. Non-federal Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
57	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	35	1240	3.7.4 - (b) is unrealistic. How would the inspecting person know if there were unauthorized or improper modifications?	Remove (b).
58	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	36	1307	3.8.1 - The second half of the control is redundant with 3.8.3.	End the sentence after "containing CUI."
59	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	38	1364	3.8.5 - This control feels like it should be paired with 3.8.1.	Move to 3.8.1 and change title to "Media Transport and Storage".
60	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	40	1457	3.9.2. A sponsor should not be defining a contractor's "transfer or reassignment" actions. These should be defined by the contractor.	Remove the first ODP from (b2).

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
61	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	41	1484	3.10.1 0 (a), the phrase "physical location where the system resides" is awkward, since the components of the system (e.g. servers) could reside in multiple locations.	Either change to "locations" or change to "system components reside".
62	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	41	1487	3.10.1 - "periodically" is not defined. Non-federal Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
63	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	42	1505	3.10.2 - "periodically" is not defined. Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
64	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	42	1530	3.10.6 (b) is beyond the scope of original control. Remove "b". If not feasible, remove the ODP. Control (a) seems makes some sense; contractors should maintain a list of alternate work sites, (b) is not necessary, as any site the contractor uses should meet all basic requirements, and have documented controls. If this is focused on telework, organizational policies would mandate the same requirements the organization must meet. This would also put telework / employee homes in scope for assessments which may have legal consequences.	Remove (b). And if focused on telework - employee homes could come into scope in assessments, which could be problematic.
65	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	44	1591	3.11.1 - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically" or provide a definition in the glossary for "periodically" duration bounds, e.g., up to 1 year.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
66	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	44	1608	3.11.2 - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically" or provide a definition in the glossary for "periodically" duration bounds, e.g., up to 1 year.
67	FFRDC/UARC Security Council CUI Working Group	Editorial	NIST 800-171R3 Final Draft	45	1611	3.11.2 - Typo.	In (c), replace "to be scanned" with "to be scanned for".
68	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	45	1611	3.11.2 (a) - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically" or provide a definition in the glossary for "periodically" duration bounds, e.g., up to 1 year.
69	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	45	1638	3.12.1 - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically" or provide a definition in the glossary for "periodically" duration bounds, e.g., up to 1 year.
71	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	46	1658	3.12.2 - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically" or provide a definition in the glossary for "periodically" duration bounds, e.g., up to 1 year.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
72	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	46	1670	3.12.3 - The term "continuous monitoring" in a security context usually refers to network monitoring. In this language, it appears to be referring to the need to document and review security controls in an ongoing manner.	Rename to "Security Controls Review" and start sentence with "Develop and implement a system-level security control documentation and review strategy…"
73	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	47	1688	3.12.5 - It's not clear if the owners of the other systems need to sign or agree to something in these agreements. The language seems to imply a mutual agreement, but the current language could be interpreted as just an internally-stored document with exchange details. The language needs to specify whether there is some kind of organization-to-organization agreement, or if it is simply documentation that an information exchange is occurring with another organization.	Rather than naming types of agreements, the language needs to specify whether the agreements need to be mutually accepted between organizations, or just documented by the contractor.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
74	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	47	1688	3.12.5 - This control is inappropriate for an organization that handles data from multiple sponsors. A sponsor may want to have its data protected in some sort of exchange agreement, but it would not be appropriate to dictate how other org's data is tracked and managed.	Remove ODP.
102	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	47	1688	3.12.5 When a collaboration involves formal agreements to purchase services (eg. I am hiring AWS to use the Cloud) the agreement should include what is expected of both parties to include how to protect the data. As written - this may be interpretted that any time someone sends CUI to another party - as part of a team under an NDA - the involved party or an assessor may look for an MOU or ISA anytime an email is exchanged.	**Reword**: Approve and manage the exchange of CUI between the system and other systems using when organizations procure services, approve and manage the formal exchange of CUI when appropriate.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
75	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	47	1694	3.12.5 - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
76	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	49	1773	3.13.8 - Encrypting information in storage has a massive cost and performance impact. Every server, every database, every file on every media. Requirements already exist to protect transportable media with encryption, which includes USB, files sent externally, phones, end user laptops. While encrypting servers is obviously preferred, the cost and performance impacts make this control unrealistic.	Remove "and while in storage".

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
77	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	49	1773	3.13.8 - Specifies encryption in storage and transmission. Does this remove alternative physical safeguards which was an option in NIST 800-171 R2 for addressing encryption at rest needs? Alternate means are required for cost reasons and older devices which must keep running but encryption may not be possible based on destination systems that cannot be modified.	Remove "and while in storage". Add back allowance for "alternative physical safeguards" as in alignment with prior Rev2 for encryption at rest.
78	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	49	1773	3/13/8 - Does this set the bar to require FIPS 140-2/3 or if this now creates less specificity opening up more options which will assist smaller organizations in general. If the intent is to broaden options, be clear with examples. Too many in industry have struggled to understand the FIPS 140 requirement vs. anything that is encrypted.	Provide clarity (state if FIPS 140-2/3 or explain alternates with examples)

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
79	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	50	1808	3.13.10 - Remove ODP. Organizations supporting multiple government agencies will be challeged to comply with different ODPs. Establishing and managing keys should include key generation, distribution, storage,	Remove the ODP and change to "Establish and manage a cryptographic key management program that takes into account the following topics: key generation, key distribution, key storage, key access, and key destruction."
97	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	50	1825	3.13.11 Clarify the cryptography requirements. FIPS validated is not always possible. However without clarity on the requirement it is left to the nonfederal organization to decide	Reword suggestion: "Employ FIPS validated cryptography **when technically feasible** to protect the confidentiality of CUI."
80	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	52	1885	3.14.1 (b) Remove ODP. Government should be suggest timeframes for remediation, but should not be dictating remediation schedules, especially for specific vulnerabilities.	Remove ODP.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
81	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	53	1910	3.14.2 (c1) is not viable because it relies on traditional virus scanning methodologies. This invalidates new vulnerability solutions (e.g. Crowdstrike) which do not perform periodic scans of the system for malicious code, but instead looks for unexpected behavior on the system and acts accordingly. The initial public draft didn't include the scanning requirement, but the language added back in the final public draft once again invalidates tools that do not perform periodic file scanning.	Remove (c1), or change the "and" in (c1) to an "or".
82	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	54	1964	3.14.6 - (b) should be first, and should focus having the contractor define what constitutes unauthorized access. Then the new (b) should combine the current (a) and (c), monitoring the system to detect attacks and indicators of potential attacks.	Delete and replace with: (a) Define indicators of unauthorized access and potential attacks. (b) Monitor the system and inbound/outbound communications traffic for identified indicators.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
83	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	56	2019	3.15.1 - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
84	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	56	2041	3.15.2 (a7) is excessive. It should be assumed that the SSP will include all details needed relevant to protecting information.	Remove (a7).
85	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	56	2042	3.15.2 - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"
101	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	57	2061	3.15.3 (b) Organizations typically have training and inbrief materials available on the information system that contains CUI. **Remove the "and the system"**	**Reword**: Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI.
86	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	57	2066	3.15.3 - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
87	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	57	2077	3.16.1 - This is out of scope for 800-171. Contract negotiation details are not part of security controls. This would also make contracts auditable as part of an 800-171 review. The DFARS 252.204-7012 clause defines the requirements for security controls required in organizational system use. To maintain compliance, organizations would be required to acquire systems with the appropriate safeguards.	Remove 3.16.1
88	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	58	2096	3.16.2 - If (a) is true, but you do (b), are you now compliant? The way it reads now, if I can't meet (a), I fail the control. 3.16.2 needs to clearly describe what a compliant state is. "Risk mitigation" is unnecessary here, as that should always be in place and there is no way for it to be assessed.	Remove (b). If "alternative sources for continued support" will make the control compliant, then add that part fo the end of (a).

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
89	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	58	2121	3.16.3 – Remove control or remove ODP. - Organizations execute contracts with External Service Providers. As part of the contract, if CUI is involved, contract should define the security requirements the ESP must follow. -If the control remains, the ODP should be reviewed. The ODP makes it almost impossible for a contractor to service multiple government agencies. If each agency defined its own requirements, the contractor would have to segregate all the agencies' data, or apply all the ODP requirements to all external system services.	Remove 3.16.3 alternately remove ODP
90	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	59	2151	3.17.1 - "periodically" is not defined Non-federal organizations and assessors may have varying interpretations.	Define upper and lower paramaters around "periodically"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
91	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	59	2152	3.17.1 - There is no need for (c), protecting the plan is not a security requirement and should be no different from handling any other business sensitive information. Consider moving this requirement to 800-172. Many companies do not have extensive supply chains.	Remove (c).
98	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	76	2791	Recommend creating an overlay for a low baseline for FCI by mapping NIST 800-171R to FAR 52.204-21. The overlay would contain any tailoring to correct the intent defined in FAR -21.	Specify FCI protection variances or create an FCI overlay to tailor the requirements down to a low baseline.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
93	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	iii	N/A	There is no reference to the Assessment Guide in the document except in the outline of changes. Organizations need to completely understand what is required to achieve a requirement	Consolidate 800-171 and 800-171A into one document. Many companies seem to be unaware 800-171A exists. 800-171A is critical for companies to understand completely what is required of them. At a minimum, reference the assessment guide and if there are multiple versions, please ensure they align with the version number (since the CMMC Proposed Rule is aligned to Rev 2 - the assessment guide for Rev 2 must also be retained. Each assessment guide should align with his security requirements guide (if not embedded into it).

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
94	FFRDC/UARC Security Council CUI Working Group	General	NIST 800-171R3 Final Draft	xi	N/A	NIST should consider creating an Industry Council for Federal Government to partner with Industry to collaborate on future revisions of NIST SP 800-171 (and companion documents) and cybersecurity best practices. Such a partnership will allow NIST insight into security measures that are implementable on industry networks. Such a Council could be instrumental to "harmonize" the security requirements across federal and nonfederal partners while improving cybersecurity. Examples of existing councils performing similar functions include: 1. The National Industrial Security Program Policy Advisory Committee (NISPPAC). The NISPPAC	Create across sector Federal Government and Industry Council for creation of future 800-171 revisions and defining ODP recommendations.