From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: Oaks, Amy E.
Subject: [800-171 Comments] 800-171 Rev3 Draft 1 Comments - from JHU APL
Date: Wednesday, July 12, 2023 1:55:17 PM
Attachments: 800-171Rev3Draft1_PublicCommentResponse-JHUAPL.xlsx

---

Greetings!

Attached are comments from Johns Hopkins APL.

Respectfully,
Molly

Molly Hennick
Senior Professional Staff II
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Rd
Laurel, MD 20723

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	JHU/APL	Technical	800-171r3 ipd	Varies	Varies	The use of ODPs while providing flexibility for Federal organizations that choose to establish non-standard formulations for use in their specific contracts ultimately renders the 171r3 neither a standard nor scalable. Scalability is crucial to implementation of these requirements at the contractor level. The ODP construct means that a contractor with 1 000 contracts may have 1 000 different implementations they are required to meet simultaneously many on the same enterprise network. Even if said contractor took the approach of meeting the most stringent version of each requirement they would likely need to employ fulltime staff just to track the requirements across contracts and determine which version of each requirement to meet and when to change implementations in real time as new contracts are acquired. Contractors would still run the risk of a government organization rejecting that approach and insisting on implementation of their exact ODP thus "breaking" the network with respect to other contracts. Lack of scalability is crippling the supply chain which is why Government contractors have been begging for consistency in requirements across the Federal organizations for years the ODP approach expands inconsistency and is the exact opposite of what is needed.	Given that NISTs charter is to provide Standards recommend replacing all ODPs with a standard wording. NIST may also elect to overlay that baseline by signifying which elements are most appropriately subject to enhancement by an individual Federal organization. In this way both a standard is established and flexibility is indicated should the Federal organization wish to apply it.
2	JHU/APL	Editorial	800-171r3 ipd	Varies	Varies	The use of the term "organization" is ambiguous throughout this document. Sometimes it means the government sometimes it means the NFO and sometimes it means a sliding scale from the government down to the NFO. This is a major clarity issue which renders many requirements ambiguous. Need a clear definition for organization that cannot mean different things at different times.	Either use an adjective before the word "organization" throughout to specify when it means government organization versus contractor/implementing/NFO organization. Or use different terms for each.
3	JHU/APL	General	800-171r3 ipd	Varies	Varies	The several (15) FAR 204.21(b)(1)(i - xv) requirements related to required security for Federal Contract Information (FCI) were incorporated into the parallel (17) items in the 800-171r2 nearly verbatim other than conversions such as for FCI to CUI and information systems to systems. That allowed appliers (Federal organizations) and users of the 800-171r2 to have clearer confidence that meeting the 800-171r2 requirements also meant substantially meeting the FAR requirements at least in cases where all FCI resided on platforms and networks that meet the CUI requirements. Additionally it allowed contractors to reference the 800-171A document for additional guidance. With the change of the FAR-related language in 800-171r2 to the language in 800-171r3 this coverage is no longer clear and is potentially no longer as complete.	Preferably include in 171r3 language that clearly parallels the FAR requirements and provide a mapping. Minimally add language to assert the coverage of the (15) FAR requirements are met for any systems and networks compliant with 800-171r3.
4	JHU/APL	Technical	800-171r3 ipd	Varies	Varies	Many requirements are written as if NFOs will all use enclaves many organizations want to apply this on their enterprise network to satisfy contracts broadly. Many requirements need revision to make this feas ble.	Make all requirements achievable at the enterprise level.
5	JHU/APL	Editorial	800-171r3 ipd	Varies	Varies	Object to the varied density of requirements. 3.1.1 is extremely dense while 3.2.3 is simple direct and straightforward. From an assessment perspective these cannot be scored in the same way. For a contractor trying to manage these requirements to variation in density is complex and unwieldy. The focus should be on security not distracted by the way requirements are presented.	Review all requirements to provide a more equivalent set with uniform density that allows for un form scoring assessment and management.
6	JHU/APL	Editorial	800-171r3 ipd	Varies	Varies	Object to the use of "123" levels below "abc" levels. The lack of uniformity between requirements will make them harder to manage. Contractors use spreadsheets and databases and many tools to manage their requirement tracking this new construct adds confusion and complexity unnecessarily already. Would prefer we removed the abc construct but minimally please limit to first level lists.	Remove enumerated lists and write as single requirements with uniform complexity between them. At a minimum remove second level list sets ("123") and use no more than first level list sets ("abc").
7	JHU/APL	General	800-171r3 ipd	Varies	Varies	Many requirements (e.g. 3.5.1) are too much of a leap from R2 to R3 for the community. What if the first step was this sort of structure that's closer to 800-53 but does not use ODPs? Get the community stabilized on that figure out how to manage their tools assess and score. Then the next rev could go toward ODPs. This revision is just a bridge too far.	Take a smaller step between R2 and 800-53 structure. Remove ODPs but keep this structure is one way to achieve that.
8	JHU/APL	Editorial	800-171r3 ipd	Varies	Varies	Many ODPs require the definition of "personnel or roles" which the govt will not be able to define for a third-party company. Any ODPs that require this should be removed and referenced to 3.15.1. It's disruptive to the govt to include these ODPs which they cannot define.	Remove ODPs that require definition of personnel or roles and reference to 3.15.1 instead.
9	JHU/APL	Technical	800-171r3 ipd	5	116	3.1.1 Requirement is too dense and cannot be scored the same as a single statement requirement. 3.1.1[b] govt will not be able to assign this ODP. Reference to 3.15.1 and remove ODP. 3.1.1[e] does not belong in this control family. 3.1.1[f] accounts need to be disabled the same day. 3.1.1[h] needs to be moved before [f] logically they have to have notification before they can disable. 3.1.1[h] is incomplete they need notification of when a user has violated the organizational policy and notification when the risks identified in [g] have occurred otherwise no one knows to disable the accounts.	[b] Reference to 3.15.1 and remove ODP. [e] Move to Security Assessment and Monitoring. [f] Set to same day and remove ODP. [h] Move before [f]. [h] Add two more items to notify when a user has violated organizational policy and when any of the risks identified in [g] have occurred.
10	JHU/APL	Technical	800-171r3 ipd	7	229	3.1.5 is too broad. 3.1.5[b] does not have enough information to understand what to do. Govt cannot assign this ODP. Reference to 3.15.1 and remove ODP. 3.1.5[c] is not scalable when you consider multiple contracts. Govt cannot assign this ODP. Reference to 3.15.1 and remove ODP. [d] discusses reassigning or removing privileges but nothing is mentioned about a timeline required or ODP to make sure privileges are reassigned or revoked in a timely manner. It is highly recommended that a periodicity be set as part of the requirement of least privilege to make sure privilege levels are checked on given timeline. Without a timeline in place this adds risk to an environment.	3.1.5 revert to the R2 wording and use the discussion for explanation. [b] and [c] need to reference back to the NFO policies and procedures in 3.15.1 versus being an ODP. [d] Assign a time period.
11	JHU/APL	Technical	800-171r3 ipd	8	252	3.1.6[a] govt will not be able to assign this ODP. Reference to 3.15.1 and removed ODP.	3.1.6[a] Reference to 3.15.1 and remove ODP.
12	JHU/APL	Technical	800-171r3 ipd	9	293	3.1.8 the concept is fine but the ODPs are a black hole and thus not scalable across multiple contracts. There need to be minimums defined.	Set to industry standard of 3 attempts in 10mins for a 30min lockout.
13	JHU/APL	Technical	800-171r3 ipd	10	314	3.1.9 last sentence of the discussion needs to be removed it's not realistic for contractors to be contacting OGC for approval of their banner.	Remove last sentence of discussion "Organizations consult with the Office of General Counsel for a legal review and 314 approval of warning banner content."
14	JHU/APL	Technical	800-171r3 ipd	10	341	3.1.11 It doesn't seem possible for the govt or NFOs to come up with an exhaustive list of conditions.	Remove the ODP and say what is meant.
15	JHU/APL	Technical	800-171r3 ipd	11	360	3.1.12[b] Should be in monitor family or reassess whether monitor family should exist or have reqts farmed out to other appropriate places.	[b] Move to Monitor family.
16	JHU/APL	Technical	800-171r3 ipd	12	418	3.1.18 Bring your own device (BYOD) needs to be included discussion should clarify this. [c] Fu l-device encryption will protect outsiders when device is locked but container-based encryption is needed to protect one app from accessing the another app when the phone is in use. Largely available to most companies.	Clarify that organization-controlled devices includes BYOD. [c] Remove selection and set to container-based encryption (not full-device encryption which is not sufficient when the phone is in use).
17	JHU/APL	Technical	800-171r3 ipd	13	453	3.1.20 The selection/ODP is too complicated to even understand what the requirement is supposed to do. Please don't use selection/ODP on the verb part of requirements. Is the requirement saying create a CUI system and everything else is external? Requirement is very unclear.	Use R2 wording.
18	JHU/APL	Technical	800-171r3 ipd	14	478	3.1.21 This requirement is a total departure from the R2 version of 3.1.21 and should not repeat the number. [b] It doesn't seem possible for the govt or NFOs to come up with an exhaustive list of conditions and to scale across multiple contracts.	Provide a new number for the requirement. [b] Remove the ODP and say what is meant or remove the requirement.
19	JHU/APL	Technical	800-171r3 ipd	14	501	3.1.22[a] Belongs in awareness and training. [b] What is the scope? Does this include people posting anywhere (personal social media) or just where the company posts? This is our interpretation - is this correct in terms of the scope? If so update to state this... "Only government officials can be authorized to release CUI to the public. Do not allow CUI to become public – always safeguard the confidentiality of CUI by controlling the posting of CUI on company-controlled websites or pub ic forums and the exposure of CUI in public presentations or on public displays. It is important to know which users are allowed to publish information on publicly accessible systems like your company website and implement a review process before posting such information. If CUI is discovered on a publicly accessible system procedures should be in place to remove that information and alert the appropriate parties."	[a] Move to Awareness and Training. [b] Update to specify the scope.
20	JHU/APL	Technical	800-171r3 ipd	15	513	3.1.23 Requirement is too broad and will not be able to be scaled across contracts due to the ODP. If this is not going to be automated than really belongs in Policy.	Reword for more specificity and to allow for scaling across contracts on the enterprise network. Move to Policy if this is not going to be automated.
21	JHU/APL	Technical	800-171r3 ipd	15	524	3.2.1[a][1] At least annually is the industry standard. By setting to this and using "at least" contractors are free to do it more frequently. [a][2] The discussion can describe the circumstances when you might change your policy the requirement only needs to state to do it when policy changes. Change to required by system or policy changes and remove the ODP. [b] ODP doesn't add value just set to annually and when policy changes.	[a][1] Set to at least annually and remove ODP. [a][2] Change to required by system or policy changes and remove the ODP. [b] Change to - Update training and awareness content at least annually and following policy changes.
22	JHU/APL	Technical	800-171r3 ipd	16	553	3.2.2 ODPs unnecessarily overcomplicate this and make them not scalable for companies with many contracts and sponsors.	Change ODPs to at least annually and upon policy changes.
23	JHU/APL	Technical	800-171r3 ipd	16	578	3.2.3 for consistency this requirement should have a time period. Annually would be standard.	Add "at least annually."
24	JHU/APL	Technical	800-171r3 ipd	17	604	3.3.1[a] The list of event types is really important need to specify it rather than use an ODP.	3.3.1[a] Remove ODP and set to "password changes successful logons failed logons or failed accesses related to systems administrative 613 privilege usage or third-party credential usage." OR end requirement at "Specify the following event types for logging within the system." and then provide the list of necessary event types in the discussion. OR change requirement to "Capture all available event types for logging within the system."
25	JHU/APL	Technical	800-171r3 ipd	17	630	3.3.2 ODP can be removed. Providing a list of what the audit records need to contain does not limit the organization from adding additional things if they want to. Removal of ODPs makes the entire document more useful.	Remove ODP.
26	JHU/APL	Technical	800-171r3 ipd	18	644	3.3.3 Lost the point from R2 where you have to REVIEW the logs. [c] There are too many different actual laws for different types of data this is not scalable across contracts. If the intent is for cyber forensics then need to specify a value - 3 years is best but no less than 12 months.	Include the need to review the logs in the requirement. Set a time of no less than 12 months for the ODP.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
27	JHU/APL	Technical	800-171r3 ipd	18	662	3.3.4[a] govt will not be able to assign this ODP. Reference to 3.15.1 and remove ODP. Providing an ODP for time allowed to fix an audit log failure is very dangerous. If a timeline is allowed to go too long then if a cyber attack causes the audit log failure then the attack could continue to perform malicious actions without the actions being noticed. [b] This is really an overly complex way of saying that if you have a logging process failure fix it. Discussion - remove the last sentence ("Organizations may decide to take no additional actions after alerting designated roles or personnel.") they have to fix it.	[a] Reference to 3.15.1 and remove ODP. Any system that fails to perform audit logging the system should send an alert to the user and be shutdown or taken offline immediately [b] Simplify statement to say Fix the logging process failure. Discussion - Remove the last sentence if they have a failure they at least have to fix it.
28	JHU/APL	Technical	800-171r3 ipd	19	683	3.3.5[b] govt will not be able to assign this ODP. Reference to 3.15.1 and remove ODP.	[b] Reference to 3.15.1 and remove ODP.
29	JHU/APL	Technical	800-171r3 ipd	20	724	3.3.7[b] Is unnecessary it's really in the weeds to tell people what time they need to use and does nothing to improve CUI confidentiality.	[b] Remove requirement entirely.
30	JHU/APL	Technical	800-171r3 ipd	21	769	3.4.1[b] needs to include review and update when components are modified and when a vulnerabi ity is identified.	[b] Add when components are modified and when a vulnerability is ident fied.
31	JHU/APL	Technical	800-171r3 ipd	21	785	3.4.2[a] It's not obvious what would go into the ODP besides the STIGS. How do you fill it out when you aren't based on a STIG? STIGs are not always the best answer. Have to consider that companies will be implementing this on their enterprise network - not an appropriate thing to try to impose on a company universally. Could end statements after operational requirements.	[a] End requirement after "operational requirements" and eliminate ODP.
32	JHU/APL	Technical	800-171r3 ipd	23	832	3.4.4 This is really hard to assess. [b] The addition of "verify" is a large ask for small companies. It requires a person with deep knowledge of the organization's systems and is very expensive every time that individual changes. Changing verify to re-assess would be a little less of a burden.	[b] Change "verify" to "re-assess".
33	JHU/APL	Technical	800-171r3 ipd	23	863	3.4.6[a] "only mission-essential capabilities" is too strong this means they can't have a well configured app to order from their cafeteria or buy from their company store. This is written as if organizations will all use enclaves - have to understand that organizations want to apply this on their enterprise network. [b] This ODP needs to be specified at the contract level and that's not scalable for large organizations with thousands of contracts. The ability to impose requirements at the contract level exists anyway no need to muddy 171 with this ODP. [c] This should be allow listing restrict everything and then be intentional about each thing allowed. [d] Just put a default time.	[a] Change to "minimize non-essential capabilities with a documented risk assessment". [b] Change to "prohibit and restrict use of ports protocols software and services based on risk assessment." [c] Change to "Implement allow listing for program execution in accordance with the risk assessment." [d] Provide a default time.
34	JHU/APL	Technical	800-171r3 ipd	24	896	3.4.8 This is allow listing which overrides 3.4.6c. No need for an open ODP here just set the time.	Delete 3.4.6c. [c] Define the time.
35	JHU/APL	Technical	800-171r3 ipd	25	927	3.4.9[c] No need for an open ODP here just set the time.	[c] Define the time.
36	JHU/APL	Technical	800-171r3 ipd	25	942	3.4.10 Good add just define the time in [b].	[b] Define the time.
37	JHU/APL	Technical	800-171r3 ipd	26	962	3.4.11[c] Remove- the location will be the enterprise or enclave and they aren't allowed to go outside of that without breaking all their other requirements so [c] is irrelevant.	[c] Remove requirement.
38	JHU/APL	Technical	800-171r3 ipd	26	972	3.4.12 Think the point is that a typical system should not travel in an adversary's hands it te ls them too much about the network configuration. Second point is that any system that travels to high risk areas must be destroyed upon return and cannot connect to the network while traveling or upon return. One way to do this is to issue a temporary burner system before they go and block primary systems from traveling.	Remove ODPs and rewrite requirement to meet the point that a typical system should not travel and that a traveling system should not connect to the network while traveling or upon return.
39	JHU/APL	Technical	800-171r3 ipd	27	993	3.5.1[a] - typo should be "users" [b]- too open ended not scalable for organizations with many contracts.	[a] Fix typo first "user" should be "users." [b] Remove ODP and define what is needed.
40	JHU/APL	Technical	800-171r3 ipd	27	1011	3.5.2 Authenticate is too strong change to authorize. ODP is unnecessary just say "organization-defined devices".	Change authenticate to authorize. Replace ODP with "organization-defined devices."
41	JHU/APL	Technical	800-171r3 ipd	28	1040	3.5.4 R2 was limited to "network" and this expands to "all access" which only adds in local access. Local access is not relevant to the replay-resistant problem. The change adds nothing and is very difficult to validate at assessment. How is replay-resistance proven for local access?	Revert to R2 wording.
42	JHU/APL	Technical	800-171r3 ipd	28	1054	3.5.5[a] govt will not be able to assign this ODP. Reference to 3.15.1 and remove ODP. [b] Something is missing in the wording. Not sure what action they're supposed to do. Minimum - replace "an" with "each". Is that what was intended? Otherwise a company could just do one and pass. Remove "select" just "assign." [c] ODP is unnecessary could just end after identifiers. [d] Intent is unclear. Could end requirement after "individual." Easier implementation to look at everyone equally rather than setting filters for only select people. Also more secure. Cheaper and better and passes the HR sniff test.	[a] Reference to 3.15.1 and remove ODP. [b] Remove "select" and just leave "assign." Change "an" to "each" if this was the intention. [c] Remove ODP and end requirement after "identifiers." [d] End requirement after "individual" and remove ODP.
43	JHU/APL	Technical	800-171r3 ipd	29	1070	3.5.7 Requirement is too complex was better as separate requirements. Overall more uniform requirements for accessibility and scoring. Lost the concept of restricting password reuse since 3.5.8 was dropped but is not included here. [a] Set minimum of 12 characters with a l 4 character types required. [b] Remove everything after the comma - there are systems which don't allow for spaces or some printable characters so this unnecessarily increases cost. Instead set to 4 character types as specified in 3.5.7a. [e] Remove. Note that we don't believe Microsoft complies. It appears that you can save passwords as salted but they would also be saved not salted that defeats the purpose of the requirement. If Microsoft can't comply this is a huge cost and changeover for almost all organizations. If kept strike "preferably " preferably belongs in discussion not a requirement. [f] Immediately isn't possible. Change to "force a new password selection upon next logon." [g] Needs to be a "unique" temporary password that meets the requirements of 3.5.7[a]	Simplify by splitting into multiple requirements. Add in restricting password reuse. [a] Set minimum of 12 characters with all 4 character types. [b] End requirement after "passphrases." [e] Remove requirement. [f] Change to "Force a new password selection upon next logon." [g] Add in that temp password need to be "unique" and meet the requirements of 3.5.7[a].
44	JHU/APL	Technical	800-171r3 ipd	30	1117	3.5.12 Again this is too complex - need more uniform requirements. [a] Confusing as written consider rewording for clarity or deleting. Do not believe it adds value. [b] You can verify the identity of someone who is not the person to whom the authenticator belongs and still meet this requirement. Need to ensure they only distribute authenticator to the correct person or thing to whom it belongs validate the appropriateness of that individual/thing to have that authenticator. [d] Doesn't add value from the other requirements listed in the discussion creates assessment issues with trying to defend what "more" one has done to protect to meet this requirement. Remove. [e] It's impossible to change a password "prior to" first use. Change to "at first use". Seems like a superset of 3.5.7[g] which can then be deleted. Also only half makes sense - can't change fingerprints for example. [f] Implies mandatory password change policy many companies have moved away from this by using very long and complex passwords which are more secure. Reword to allow for this case.	Simplify by splitting into multiple requirements. [a] Remove or rewrite for clarity. [b] Rewrite to ensure they only distribute authenticator to the correct person or thing to whom it belongs va idate the appropriateness of that individual/thing to have that authenticator [d] Remove requirement. [e] Change "prior" to "at first use" and remove 3.5.7[g] which is duplicative as a subset of this requirement. [f] Reword to allow for long complex passwords that are not changed.
45	JHU/APL	Technical	800-171r3 ipd	30	1151	3.6.1[c] Should have a periodicity to it that the DIB is required to follow since incident response plans are very important and they should be checked every so often in order to make updates or see where they could be improved.	Add a minimum timeline that Incident response plans needs to be updated or checked for updates.
46	JHU/APL	Technical	800-171r3 ipd	31	1173	3.6.2[b] govt will not be able to assign this ODP. Reference to 3.15.1 and remove ODP.	[b] Reference to 3.15.1 and remove ODP.
47	JHU/APL	Technical	800-171r3 ipd	32	1194	3.6.3 Just make it annual and remove ODP. Requirement is a little too vague - suggest pul ing "identify potential weaknesses or deficiencies" into the requirement itself.	Just make it annual and remove ODP. Pull "identify potential weaknesses or deficiencies" from the discussion into the requirement itself.
48	JHU/APL	Technical	800-171r3 ipd	32	1206	3.6.4 Belongs in Training family. [b] Assign as annually and following any significant event.	Move to Training family. Assign as "annually and following any significant event" and remove ODP.
49	JHU/APL	Technical	800-171r3 ipd	33	1231	3.7.4 is a big departure from 3.7.4 in R2 should really be a new requirement number - better aligns to old R2 3.7.3 if you want to reuse a number. [c][2] Need to define minimum standards for sanitizing equipment. [c][3] Remove. No one at an NFO has the power to provide a CUI exemption.	Give a new number or assign as 3.7.3 not 3.7.4. [c][2] Define minimum standards for sanitizing equipment. [c][3] Remove.
50	JHU/APL	Technical	800-171r3 ipd	34	1258	3.7.5 Ignores cloud solutions. This is written as if everyone is old school sitting down with a monitor and keyboard. Cannot monitor or approve maintenance being done by the CSP. How does someone using a cloud solution achieve this requirement? An assessor cannot evaluate this for a cloud solution.	Scope to operating system level maintenance only. Update definition of nonlocal for the many d fferent ways in which systems are designed in 2023.
51	JHU/APL	Technical	800-171r3 ipd	34	1272	3.7.6 Cloud is a problem - If an organization is subscribing to a SAAS environment all of these are difficult if not impossible to do. Would a shared responsibility matrix indicating that the CSP is performing this work be accepted? If so this should go into the discussion. If not needs to be rewritten to be achievable in cloud solution.	Rewrite or use discussion to describe how to achieve this with a cloud solution.
52	JHU/APL	Technical	800-171r3 ipd	35	1310	3.8.2 govt will not be able to assign this ODP. Reference to 3.15.1 and remove ODP.	Reference to 3.15.1 and remove ODP.
53	JHU/APL	Technical	800-171r3 ipd	35	1323	3.8.3 Provide specific ink to where NARA provides this guidance.	Provide specific link to where NARA provides this guidance.
54	JHU/APL	Technical	800-171r3 ipd	36	1337	3.8.4[a] The reqt is okay for anything "known" to be CUI. But the company cannot be held accountable for CUI not marked by the govt. The reqt needs to provide companies with an out for this case - when the govt fails to mark CUI - because that is out of the NFO's control. [b] Remove not applicable to NFOs. CUI needs to be marked - there are no exemptions.	[a] Provide an out for NFO's when the govt fails to mark CUI. [b] Remove requirement.
55	JHU/APL	Technical	800-171r3 ipd	36	1352	3.8.5[b] Transport is not clear. Elevate this to require cryptographic mechanisms on all removable media which will encompass during transport. This is an expansion from R2. What happens when the govt provides unencrypted media to an NFO for use on a contract? Has the organization automatically failed when they accept that media? How does the NFO get out of that with an assessor?	Elevate this to require cryptographic mechanisms on all removable media which will encompass during transport. Provide explanation of how NFO achieves requirement is govt gives them unmarked CUI to transport.
56	JHU/APL	Technical	800-171r3 ipd	37	1375	3.8.7[a] Too open ended and not poss ble for the govt to define. Reqts are easier to meet and assess when phrased in the positive.	[a] Change to "Allow the use of only organizationa ly-managed media."
57	JHU/APL	Technical	800-171r3 ipd	37	1400	3.8.9 Cloud issue - small companies primary use cloud for backups. How do they achieve this? Link to 3.13.11 so NFOs don't accidentally fa l by choosing one type of encryption here that differs from the 3.13.11 requirement. Remove alternative physical controls from the discussion - conflicts with the requirement.	Explain how this works with cloud backups. Link to 3.13.11 for selection of the encryption type. Remove alternative physical controls from the discussion.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
58	JHU/APL	Technical	800-171r3 ipd	38	1413	3.9.1[a] Add authorizing or "elevating " access to the system. [b] Remove. This is too close to requirements for classified. HR is going to have an issue with this for unclassified personnel and classified personnel are held to different standards automatically anyway. At the 800-172 level you get into adverse information which will require this for specialized CUI.	[a] Add when "elevating" access. [b] Remove.
59	JHU/APL	Technical	800-171r3 ipd	38	1426	3.9.2 duplicative of 3.1.1f&h - should be combined. Too much risk in the ODPs need maximums set. Different govt orgs will have different standards this is not scalable to manage for companies that work across agencies with many contracts.	Combine with 3.1.1[f]and[h]. Assign ODPs to reduce risk and make scalable.
60	JHU/APL	Technical	800-171r3 ipd	39	1457	3.9.3 - Cloud providers are external providers this is extraordinarily hard to implement for them especially [b]. This is written for brick and mortar in person external providers - it's fine from that perspective. Either exclude external providers who are offsite or rewrite to be inclusive of cloud. [b] Need to be clear which "organization" is being referred to here believe it's the NFO not the govt. Discussions has a typo we think: External providers may have personnel who work at organizational facilities with credentials badges or system privileges issued by organizations. At the end should be "the organization" not "organizations." Still has a major clarity issue throughout the document with the misuse of the term organization.	Explain how this works with cloud. [b] Clarify which "organization" is intended. Fix typo in discussion from "organizations" to "the organization" or clarify sentence if this is not a typo.
61	JHU/APL	Technical	800-171r3 ipd	39	1475	3.10.1 Doesn't extend to cloud. Restrict it to the on-premise facilities that the NFO controls. They can't control access at the cloud provider's "fac lity where the system resides" - needs to be deliberately excluded. In a cloud environment the system can move from a west coast facility to two different east coast facilities at the flip of a switch way faster than one can keep up with a requirement like this.	Explain how this works with cloud. Exclude systems that the NFO does not directly control.
62	JHU/APL	Technical	800-171r3 ipd	40	1493	3.10.2 same issue as 3.10.1 with application to cloud environments - they need to be excluded.	Explain how this works with cloud. Exclude systems that the NFO does not directly control.
63	JHU/APL	Technical	800-171r3 ipd	40	1516	3.10.6[a]Alternate work sites (home office) needs to be defined to exclude temporary work sites (work travel and work from vacation). [b] Is not a requirement as written you have to define something. It's so vague we have no idea what is intended. The old R2 3.10.6 was written much more clearly that CUI has to be protected based on all the CUI protection rules. Implies that some reqts can be excluded and they can't be. Can delete the entire requirement the other requirements all stand and cover this.	[a] Define alternate work sites (home office) versus temporary work sites (work travel and work from vacation). [b] Remove requirement or revert to R2 wording.
64	JHU/APL	Technical	800-171r3 ipd	41	1530	3.10.7[a] ODP cannot be defined by the govt. Needs to just say all access points to CUI and incorporate. [a][1] into the primary requirement. [a][2] Needs to be deleted - small businesses are going to have a receptionist at best. [b] Just say all access points to CUI. [c] End before the ODP. The combination of so many requirements into one just makes them more complex - the additional complexity just makes them harder to understand assess and pass. It was more straightforward with the R2 wording in separate requirements.	[a] Define ODP as all access points to CUI. [a][1] Fold into [a]. [a][2] Remove requirement. [b] Define ODP as a l access points to CUI. [c] Remove ODP and end after "activity."
65	JHU/APL	Technical	800-171r3 ipd	42	1558	3.10.8[b] ODP doesn't add value and should be e iminated.	[b] Change to "Control physical access to output devices to prevent unauthorized individuals from obtaining the output."
66	JHU/APL	Technical	800-171r3 ipd	42	1577	3.11.1[a] Impossible for an NFO as written. The govt has to assess the risk of CUI disclosure it's their data. The NFO can't assess this it's not their risk. In R2 the risk assessment was tied to "organizational operations" meaning the NFO operations that's something they can assess. Can change back to that (with proper definition of organization). [b] Just make it at least annually.	[a] Revert to R2 wording or put back in the concept of "organizational operations." [b] Define as at least annually.
67	JHU/APL	Technical	800-171r3 ipd	43	1599	3.11.2 ODPs make this not scalable for companies with hundreds of contracts. Need to set limits or use periodically. which also allows the organization to define it but they can make a consistent definition across their system.	Remove ODPs set limits or set to periodically.
68	JHU/APL	Technical	800-171r3 ipd	44	1655	3.12.1 What does "control" mean? Is it different from "security controls?" Are the (security) controls just all the 171 requirements? Why switch terms? What does "environment of operation" mean? This is the only place that phrase appears in the document - please define or remove it. This requirement is really unclear as written due to inconsistent terminology used. Assign ODP to annually and remove.	Use consistent terms - either requirement or control or security control. Remove or define "environment of operational." Assign ODP to annually.
69	JHU/APL	Technical	800-171r3 ipd	45	1681	3.12.2[a] Implies that an NFO always has a POAM that should not be required. Needs to be rewritten to allow for an org not to have a POAM and to only make one when needed - could add "as applicable". [b] Implication is a long-term perpetual POAM which some govt orgs are not going to accept. Old R2 wording worked better. A good POAM always has an expected end date otherwise it's just a paper drill to pass an assessment without any real action. Should include a max plan length for each POAM entry of 180 days.	[a] Rewrite to allow for an org not to have a POAM. [b] Revert to R2 wording. Or reword so as not to imply a perpetual POAM. Also set POAM limit of 180 days.
70	JHU/APL	Technical	800-171r3 ipd	45	1701	3.12.3 Second half is duplicative of 3.12.1 could just end after "strategy."	Change to "Develop and implement a system-level continuous monitoring strategy."
71	JHU/APL	Technical	800-171r3 ipd	46	1717	3.12.5 What does "control" mean? Is it different from "security controls?" Are the (security) controls just all the 171 requirements? Why switch terms? Please be consistent. Does this mean to assess every requirement? If they bring in someone to assess one requirement have they met this? Need to be much more specific. The argument for ODPs is that NIST wants to provide flexibility - this one requirement removes a HUGE part of flexibility for the govt. CMMC level 2 self-assessment would fail this that's a huge piece of flexibility the govt wants to utilize. This requirement needs to be removed. It's not right to impose this on every company nor is there an ecosystem to support it. We believe this excludes anyone internal to the NFO from being the "independent" accessor because they always have some level of COI when a failure could mean loss of contracts which means potentially loss of job for anyone who works in the company on the enterprise network - please be explicit regarding whether that's true or not. Minimally you have doubled the cost of a CMMC Level 2 assessment because you have to do an independent assessment first at $$$ to pass this requirement and then have a C3PAO come in and do the "real" assessment for another $$$.	Use consistent terms - either requirement or control or security control. Either reword to better explain the scope (e.g. assessment of one requirement by an independent party would meet this) and define independent (e.g. can someone inside the NFO ever meet the definition of independent) OR REMOVE.
72	JHU/APL	Technical	800-171r3 ipd	46	1730	3.12.6 What does "other systems" mean? This makes sense for govt systems it doesn't make sense in the world of NFOs. We shouldn't be telling NFOs how to conduct business in this way. All CUI protection requirements apply and cover this. Not applicable- should be removed.	Remove requirement.
73	JHU/APL	Technical	800-171r3 ipd	46	1750	3.12.7 All system connections have to occur within the system boundary so all requirements already apply. This should be removed from an NFO perspective. Only applies in govt environment.	Remove requirement.
74	JHU/APL	Technical	800-171r3 ipd	48	1800	3.13.3 Requirement is fine but duplicative of 3.1.4 3.1.5 3.1.6 3.1.7 put together. Really could be deleted.	Remove requirement.
75	JHU/APL	Technical	800-171r3 ipd	48	1816	3.13.4 Short of requiring log off and system reboot before someone else uses it don't know how you can protect the previous session. Covert channel discussion is confusing. Expand on what is meant and be sure it meets the goal.	Clarify.
76	JHU/APL	Technical	800-171r3 ipd	49	1845	3.13.7 This is a tough requirement to protect correctly even when you know what you're doing - huge risk to use an ODP here and allow NFOs who already don't do cyber security we l to try to guess how to fill it in. Really need to define it if we want to improve security. Or end the requirements at Prevent split tunneling for remote devices (no exceptions).	Define the ODP or change to "Prevent split tunneling for remote devices." and do not allow any exceptions.
77	JHU/APL	Technical	800-171r3 ipd	49	1867	3.13.8 Since 3.13.11 is going to specify a certain cryptography this and the others requiring cryptography should be linked to 3.13.11 so people don't choose something else and accidentally fail their assessments. Remove all suggestions from the discussions and point to 3.13.11.	Remove all suggestions from the discussions and point to 3.13.11.
78	JHU/APL	Technical	800-171r3 ipd	50	1890	3.13.9 If you assign a time period there will be a valid case where someone needs to break that to complete their work (e.g. download) - needs an exception clause. For the common case needs a defined time period to be scalable for companies across govt sponsors and contracts.	Add exception clause. Define time period outside of exception and remove ODP.
79	JHU/APL	Technical	800-171r3 ipd	50	1903	3.13.10 It's unclear how the govt would complete this ODP.	Define the ODP for clarity.
80	JHU/APL	Technical	800-171r3 ipd	51	1915	3.13.11 Believe the govt will just say "FIPS-validated or NSA-approved" so why have the ODP? Regardless need to tie this requirement back to all the other reqts involving cryptography and remove from their discussions any other options so it's clear to NFOs that they need to meet this requirement everywhere it applies.	Assign ODP as "FIPS-validated or NSA-approved" and tie all other requirements for cryptography back to this one so when they are implemented people know one of those two solutions are required.
81	JHU/APL	Technical	800-171r3 ipd	51	1926	3.13.12 R2 wording was more clear. [a] Delete the exceptions end after "applications."	Revert to R2 wording. [a] Change to "Prohibit remote activation of collaborative computing devices and applications."
82	JHU/APL	Technical	800-171r3 ipd	52	1972	3.13.17 Requires everything to go through a proxy server this has limited benefit and companies are likely to do it wrong. Reduce what traffic is required to something more manageable.	Reduce what traffic is required to something more manageable.
83	JHU/APL	Technical	800-171r3 ipd	53	1994	3.13.18 Too arbitrary no added value. Limit to what? Needs more definition or to be removed.	Remove or define better.
84	JHU/APL	Technical	800-171r3 ipd	53	2010	A single value across hundreds of thousands of organizations is not practical. In the interest of standardization (between Federal and NFOs) use the requirements specified in the CISA Known Exploited Vulnerability Catalog. This provides the added benefit that NFOs would use this as a source of vulnerability information in addition to establishing timeframes for applying patches.	Change to "Install security relevant software and firmware updates in accordance with the timelines established in the CISA Known Exploited Vulnerabilities Catalog."
85	JHU/APL	Technical	800-171r3 ipd	54	2032	Although the NFO is implied organizational policy is a good way to do it. 3.15.1 requires those policies/metrics be documented. This approach can help eliminate many of the ODPs in R3.	
86	JHU/APL	Technical	800-171r3 ipd	54	2058	Alerts and advisories should be from trusted sources The discussion makes general comments on sources and provides examples but is not binding. Make discussion more directive in nature or incorporate into the requirement. Also as written there is no requirement to act on any received alerts other than passing it on.	Change [a] from "Receive" to "Receive and respond to"
87	JHU/APL	Technical	800-171r3 ipd	54	2028	The requirement for periodic and real-time scans in not explicitly incorporated from R2 3.14.5. While it appears in the discussion it is not called out in the requirement statement.	Revert to R2 3.14.5 or add: [c] Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded opened or executed.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
88	JHU/APL	Technical	800-171r3 ipd	55	2076	Although periodic and real time scans ae in the discussion they are no longer part of the requirement in 3.14.2 as was previously required in R2 3.14.5	Revert to R2 3.14.5 or add requirement to 3.14.2
89	JHU/APL	Technical	800-171r3 ipd	56	2115	The phrase at "designated locations" is not applicable to spam protection and will vary based on the tools techniques and email service. Spam protection mechanisms must be incorporated. Delete at designated locations. 3.14.8 implies that spam protection is required on NFO mail systems. Because of the use of BYOD mob le devices which can connect to the network and non-NFO mail systems which can be accessed through web browsers spam protection should also be required f non-NFO mail can be accessed from the NFO environment. Individual users would be required to ensure spam protection is enabled on personal accounts and devices accessed within an NFO's environment through the NFOs usage policy	Change to "Implement spam protection mechanisms to detect and act on unsolicited messages."
90	JHU/APL	Technical	800-171r3 ipd	56	2117	Commercially available spam protection tools and services are generally continuously updated and do not require the update of a tool or data source.	Delete Assignment Statement Replace with in real-time
91	JHU/APL	Technical	800-171r3 ipd	56	2130	Assignment Statement is not applicable	Delete Assignment Statement Change to "at least annual and following significant change or event."
92	JHU/APL	Technical	800-171r3 ipd	57	2148	Assignment Statement is not applicable	Delete Assignment Statement Change to "at least annual and following significant change or event."
93	JHU/APL	Technical	800-171r3 ipd	57	2168	Assignment Statement is not applicable	Delete Assignment Statement Change to "at least annual and following significant change or event."
94	JHU/APL	Technical	800-171r3 ipd	58	2202	The discussion of alternative sources appears to allow for in-house solutions as well as contractual external providers. Open-source community based sources -- subject to a risk determination -- also serve as valuable sources of on-going support.	Add "The use open-source patches which are not controlled through a contractual relationship is subject to the NFOs open-source policy."
95	JHU/APL	Technical	800-171r3 ipd	58	2224	As written 3.16.3 applies to all external service providers when it is only applicable "to components of nonfederal systems that process store or transmit CUI or that provide protection for such components"	Clarify that the ESP must be used to process store or transmit CUI or provide protection for such components
96	JHU/APL	Technical	800-171r3 ipd	59	2225	The requirement as written is too open ended and the ODP is not app icable. The government lacks the blanket authority to impose requirements on NFOs that are applicable to the NFO's vendors. (The government can impose flow down requirements to sub-contractors).	Delete "the following" and assignment statement. Replace with "same security controls as the NFO."
97	JHU/APL	Technical	800-171r3 ipd	59	2230	The requirement as written is too open ended and the ODP is not app icable. The government lacks the blanket authority to impose requirements on NFOs that are applicable to the NFO's vendors. (The government can impose flow down requirements to sub-contractors).	Delete 3.16.3c
98	JHU/APL	Technical	800-171r3 ipd	59	2252	This requirement includes 3.17.2 with the exception that 3.17.2 clearly requires implementation which is otherwise assumed.	Change 3.17.1a Develop to "Develop and implement"
99	JHU/APL	Technical	800-171r3 ipd	59	2255	Assignment Statement is not applicable	Delete Assignment Statement Change to "at least annual and following significant change or event"
100	JHU/APL	Technical	800-171r3 ipd	60	2277	This requirement is included under 3.17.1 and is redundant. Add "implement" to 3.17.1	Delete requirement
101	JHU/APL	Technical	800-171r3 ipd	60	2305	The requirement as written is too open ended and the ODP is not app icable. The government lacks the blanket authority to impose requirements on NFOs that are applicable to the NFO's vendors. (The government can impose flow down requirements to sub-contractors). There is no single accepted definition of supply chain controls and the term is undefined in the NIST Glossary.	Delete 3.17.3
102	JHU/APL	Technical	800-171r3 ipd	61	2322	This control is redundant of 3.8.3 since the item must contain CUI.	Either delete as redundant or add security protection components to requirement.
103	JHU/APL	Technical	800-171r3 ipd	74	2809	Definition requires FIPS 140-2 and excludes FIPS 140-3 validation.	Adjust definition to verified by CNVP to meet requirements of FIPS140-2 or FIPS140-3.
104	JHU/APL	Editorial	800-171r3 ipd	74	2811	References NSA approved cryptography which does not exists in Glossary.	Add definition.