From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments on NIST SP 800-171r3 initial public draft
Date: Friday, July 14, 2023 9:16:27 AM
Attachments: sp800-171r3-ipd-comment-SEI.xlsx

Frank Smith, CISSP
Senior Cybersecurity Engineer
CERT Division
[redacted]

Carnegie Mellon University
Software Engineering Institute
www.sei.cmu.edu | www.cert.org

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	SEI/CA	General	publication	0		The use of ODPs will lead to an unreasonable burden on contractors serving the federal government. Each Department/Agency could set different values for the ODPs, putting contractors in the position of having to implement multiple (and possibly mutually exclusive) variants of the same security requirement. In general, use of ODPs is excessive and works against standardization. NFOs seeking compliance with agency requirements will face what amounts to essentially unlimited versions of the "same" standard. During the webinar, NIST indicated that agencies could defer the ODP to the NFO which is entirely counter to good practice and standardization	Eliminate ODPs and provide specific baseline variables in the security requirements. Security enhancements on the baseline can be incorporated into 800-172. At a minimum, NIST should specify default values for most ODPs which are numeric (i.e. frequency based, number of attempts, number of characters, etc.) and give agencies the ability to customize where appropriate. Where appropriate, specific ODPs are addressed in individual comments. In no case should the ODP be entirely up to the NFO. This could lead to periodically (in r2) implementations that greatly exceed sound practice (i.e. do vulnerability scans every 5 years) For ODPs which reference an NFOs policy, procedures, staff roles, risks, personnel, functions, etc., it is unrealistic to assume a Federal agency can specify something that is applicable to NFOs of widely different sizes, maturity, and industries. Where appropriate, specific ODPs are addressed in individual comments but in general these assignment statements should reference the required information to be in compliance with control SSP section 3.15.1. In order to meet the objectives of SSP section 3.15.1, the NFO will need to specify organizational roles, structure, internal processes etc.
2	SEI/CA	General	publication	0		The use of the word *organization* is often confusing and mis-leading especially where ODPs are specified and organization appears in the discussion. While the ODP is clearly a Federal responsibility, subsequent use of organization is unclear as to either Federal or non-federal organization.	In all cases where the word *organization* is used, specify whether the Federal, non-federal, or both organizations are referenced. NFO can be used in place of organization where appropriate
3	SEI/CA	General	publication	0		The FISMA boundary and risk approach built in to 800-53 are evident in the -171r3 descriptions. Throughout, control descriptions refer to a "system" which is not really applicable within the protection of CUI construct. This will lead to NFOs defining a CUI enclave (i.e. a system) and applying -171 controls to that very limited environment. Other organizational assets will be treated as external systems and the approach encourages cheaper (therefore weaker) control application outside the system boundary. The -171 controls need to be applied to an NFO enterprise with specific access controls and restrictions applied to components where CUI is stored, processed, or transmitted.	Delete system references and reword as needed to highlight the need to apply security controls across the organization to include cloud and external vendors (i.e. MSP, MSSPs, data centers etc.)
4	SEI/CA	General	publication	1	footnote 3	Definitions in footnotes are not consistent with glossary definitions and other footnotes	consolidate the definitions into a single definition in the glossary and eliminate the footnote versions
5	SEI/CA	General	publication	1	footnote 4	Definitions in footnotes are not consistent with glossary definitions and other footnotes	consolidate the definitions into a single definition in the glossary and eliminate the footnote versions
6	SEI/CA	General	publication	1	footnote 5	Definitions in footnotes are not consistent with glossary definitions and other footnotes	consolidate the definitions into a single definition in the glossary and eliminate the footnote versions
7	SEI/CA	General	publication	2	footnote 10	Definitions in footnotes are not consistent with glossary definitions and other footnotes	consolidate the definitions into a single definition in the glossary and eliminate the footnote versions
8	SEI/CA	General	publication	2	footnote 9	Definitions in footnotes are not consistent with glossary definitions and other footnotes	consolidate the definitions into a single definition in the glossary and eliminate the footnote versions
9	SEI/CA	Technical	publication	5	118	Inappropriate use of an ODP. This would be difficult for a Federal agency to specify in a way that makes sense to NFOs to all sizes. Additionally, a specification at this level would place undue burden on small and mid-size business . 3.15.1(a) requires the NFO to have written policies and procedures that identify roles and individuals responsible for security functions therefore it would be inpatriate for a Federal organization to specify something potentially different	Delete Assignment Replace with IAW established NFO policy and procedure as documented in SSP section 3.15.1a
10	SEI/CA	Technical	publication	5	125	The ODP organization-defined time period is used throughout 3.1.1 Account Management. This can be problematic as there is no recommendation for a minimum value that is considered acceptable. How does an assessor determine what is acceptable? What is to keep one assessor vs another from being overly prescriptive and organization from trying to be very loose in its approach? I would consider this a general comment to the use of most ODPs through out this standard.	List an acceptable minimum value that all organizations should meet when handling CUI/FCI. Not recommending this be overly prescriptive but having some minimum standard should help clarify this for everyone.
11	SEI/CA	Technical	publication	5	125	The ODP is somewhat meaningless. The account cannot be disabled until one of the conditions in f1 thru f4 is detected at which time it should be immediately disabled	Delete assignment Replace with: *Upon detection, immediately disable accounts of individuals when the accounts:*
12	SEI/CA	Technical	publication	5	130	ODP is not required. Standard practice is to automatically disable unused accounts within 30 days. If a system does not support automatic disabling, then manual reviews should be required at least every 30d to look at unused accounts	Delete Assignment Replace with: 30 days

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
13	SEI/CA	Technical	publication	5	131	Inappropriate use of an ODP. This would be difficult for a Federal agency to specify in a way that makes sense to NFOs to all sizes. Additionally, a specification at this level would place undue burden on small and mid-size business . 3.15.1(a) requires the NFO to have written policies and procedures that identify roles and individuals responsible for security functions therefore it would be inpatriate for a Federal organization to specify something potentially different	Delete first assignment Replace with IAW established NFO policy and procedure as documented in SSP section 3.15.1a Delete second assignment Replace with IAW established NFO policy and procedure as documented in SSP section 3.15.1a
14	SEI/CA	Technical	publication	5	133	Inappropriate use of ODP. Federal agencies should not be specifying personnel or roles that every NFO is required to have.	Delete first Assignment Replace with IAW established NFO policy and procedure as documented in SSP section 3.15.1a
15	SEI/CA	Technical	publication	5	134	second assignment not required and can lead to weakened access controls	Delete second assignment Replace with *within 24hrs*
16	SEI/CA	General	publication	5	165	"Enforce approved authorizations" is an unclear construct and the description of the requirement does not adequately cover what authorization entails.	Recommend a 2-part requirement: approve authorizations and enforce authorizations.
17	SEI/CA	Technical	publication	6	155	human resource managers listed twice in discussion regarding coordination of various management when disabling system accounts. There is no mention of any business owners.	Add sr. business owners,
18	SEI/CA	Technical	publication	8	232	Assignments are NFO specific and required to be documented in 3.15.1a; inappropriate for Federal agencies to require specific roles within NFOs	Delete assignments Change to Authorize privileged access IAW NFO policy as specified in SSP section 3.15.1a
19	SEI/CA	Technical	publication	8	234	First assignment should be a standard minimum frequency. Second assignments is NFO specific and required to be documented in 3.15.1a; inappropriate for Federal agencies to require specific roles within NFOs	Delete assignments Change to Review privileged access monthly and IAW NFO policy as specified in SSP section 3.15.1a
20	SEI/CA	Technical	publication	8	252	The ODPs listed make this confusing.	Just state "Restrict privileged accounts on the system to personnel that require them to perform their assigned duties or something similar. The same approach can be done for part b. or delete (a)
21	SEI/CA	Technical	publication	8	252	ODPs here add no value and introduce potential for variability between organizations	Alter text to "individuals whose work role requires them to perform privileged and/or security activities"
22	SEI/CA	Technical	publication	8	254	Assignment makes the objective unnecessarily complex.	Change to: Require that privileged users use privileged accounts only when performing privileged functions. A second, non-privileged account is required for all other uses
23	SEI/CA	Technical	publication	8	254	ODPs here add no value and potentially reduce security vs Rev2 depending on the ODP selected.	Alter text to "Require that privileged users (or roles) with access to security functions or security-relevant information use non-privileged accounts or roles when accessing non-security functions."
24	SEI/CA	Technical	publication	9	293	Assignments should be specified as maximum values	Change to 3 in 10 mins
25	SEI/CA	Technical	publication	10	314	Reference to OGC from 800-53 is inappropriate for NFOs.	delete entire sentence requiring OGC review
26	SEI/CA	Technical	publication	10	341	NFO specific and is required to documented in 3.15.1	delete assignment change to: IAW NFO policy as specified in SSP section 3.15.1a
27	SEI/CA	Technical	publication	11	362	Structure of the statement "authorize remote execution of privileged commands" does not clearly articulate the requirement to deny all execution of remote privileged commands by default and to allow only those specifically authorized. This grammatical construction is used elsewhere in Rev 3 and introduces similar issues in those places.	Revise to "deny all execution of remote privileged commands by default and to allow only those specifically authorized"
28	SEI/CA	Technical	publication	12	398	"embedded within the system" is unclear. On first read, it seems to speak to a physical wireless capability on hardware that would be turned off.	Rephrase d. to remove "embedded within the system" as the scope of the requirement is already clear. Remove the sentence that starts on 408 and runs to line 410.
29	SEI/CA	Technical	publication	12	418	Why is "implementation" only guidance rather than "requirements?" Can't implementation subsume the other two items in that series?	Revise to state "implementation requirements"
30	SEI/CA	Technical	publication	12	419	Organization controlled devices is unclear and no all inclusive. Most NFOs allow BYOD of mobile devices, provide a communications allowance, and in return enforce some level of MDM i.e. a work environment on the device	change organization to NFO add *to include BYOD devices*
31	SEI/CA	Technical	publication	12	420	Problematic use of word "authorize" (see 5 above)	Revise to "deny all mobile device connections by default and to allow only those specifically authorized"
32	SEI/CA	Technical	publication	12	421	full device encryption does not fully protect CUI	delete assignment and require container based encryption
33	SEI/CA	Technical	publication	13	453	The list of ODPs for 3.1.20 is long and confusing. One or more of the ODPs can be selected. It would seem that you need both. This focuses on identifying controls to be implemented on external systems while 3.1.21 requires those controls to be in place	Revise to clarify the ODPs and their use. It seems that these security requirements would work better if they were combined as they were in release 2.
34	SEI/CA	Technical	publication	13	453	Requirement is unclear; first assignment requires Federal agencies to specify Ts&Cs that NFOs must use in external system agreements. This would require that those Ts&Cs are in the NFOs agreement with the government and that the agreement contains flowdown requirements. In the case of a vendor to the NFO, specifying vendor requirements where the vendor d/n directly support a federal contract is probably outside of allowed practice	At a minimum, delete first ODP Second assignment is probably required IAW SSP section 3.15.1a
35	SEI/CA	Technical	publication	13	453	Use of ODP in a is so extensive as to make the sub-requirement indecipherable.	Revise to eliminate ODPs or break them up into separate sub-requirements

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
36	SEI/CA	Technical	publication	13	460	The blocklisting of external systems is not as secure as an allowlist approach.	Revise b to: "Prohibit the use of external systems that are not specifically authorized."
37	SEI/CA	Technical	publication	13	462	Discussion focuses on a Federal system and ignores cloud and other subscribed services widely used by NFOs	revise to be more appropriate for NFOs
38	SEI/CA	Technical	publication	14	485	Assignment is not required; each NFO should have a general portable storage device policy. In the case of CUI, the use is largely contract specific and is based on the type of work, the need to move large data sets etc.	change to Restrict…on external systems IAW NFO policy as specified in 3.5.1a.
39	SEI/CA	Technical	publication	14	500	The security requirement listed in release 3 for 3.1.22 is not as clear as the original in release 2. R3 indicates individuals should be trained and that there should be a periodic review. No process to review to review before it is posted.	r2 stated "Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included" something like this should be added back to the r3 requirement in addition to what is there.
40	SEI/CA	Technical	publication	14	500	3.1.22 has always struck me as an odd requirement. The other requirements about protecting the confidentiality of CUI would prevent CUI from being displayed publicly. Calling out this particular vehicle for public disclosure of CUI is like calling out email as a particular vehicle for disclosure of CUI.	Remove this requirement
41	SEI/CA	Technical	publication	15	512	3.1.23 inactivity logout requirement needs clarified. The discussion indicates that automatic enforcement of the inactivity logout is addressed in 3.1.10. 3.1.10 - Device Lock states "Device locks are not an acceptable substitute 332 for logging out of the system, such as when organizations require users to log out at the end of 333 workdays" They are not the same.	Clarify the write up for security control 3.1.23. Also, if this is related to 3.1.10 why place this as 3.1.23? Why not place it right after 3/1/10 so the distinction being made is more obvious. Placing it in the group with 3.1.10 (device lock) and 3.1.11 (session termination) would make a better flow.
42	SEI/CA	Technical	publication	15	512	requirement should be combined with the similar requirement in 3.1.10a; second assignment is unclear and not required	combine w 3.1.10a and use the same period of inactivity
43	SEI/CA	Technical	publication	15	512	Requiring users to log out of a system when they expect inactivity is a far less robust control than that provided by 3.1.10. Requirement to log out after a time period or defined condition should be automatically enforced. 3.1.10 (see line 319) only requires a device lock and doesn't not require an automated method for implementing that requirement, resulting in weakened security.	Require automation to implement device locks and user logouts after defined periods of inactivity. Allow alternative controls for systems that lack the technical capability for device locks and user logouts. Automated logouts would be a suitable substitute for automated locks.
44	SEI/CA	Technical	publication	15	524	The org-defined frequency would allow organizations to hold training just once, during onboarding process, which provides inadequate security.	The org-defined frequency should stipulate not less than once per year to provide a baseline of coverage.
45	SEI/CA	Technical	publication	15	526	assignment not required	delete assignment replace with at least annually
46	SEI/CA	Technical	publication	15	528	assignment not required	replace with or following a significant system or security event
47	SEI/CA	Technical	publication	15	530	assignment not required	replace with annually and following any significant system or security change
48	SEI/CA	Technical	publication	16	552	The org-defined frequency would allow organizations to hold training just once, during onboarding process, which provides inadequate security.	The org-defined frequency should stipulate not less than once per year to provide a baseline of coverage.
49	SEI/CA	Technical	publication	16	555	assignment not required	replace with annually and following any significant system or security change
50	SEI/CA	Technical	publication	16	557	assignment not required	replace with or following a significant system or security event
51	SEI/CA	Technical	publication	16	557	The lack of a frequency statement undermines the potential security benefits of this control, as it allows this training to occur just once in a user's tenure with an organization.	The requirement should stipulate not less than once per year to provide a baseline of coverage.
52	SEI/CA	Technical	publication	16	578	as written, allows for a once and done approach. This should be a recurring requirement. Ideally all users would receive a monthly phishing prevention test with associated micro-training (less than 15mins) which would increase awareness across the board and give information about the latest threats to the entire organization	change to Provie MONTHLY literacy….
53	SEI/CA	Technical	publication	17	604	Assignment is not appropriate. A minimum list of event types to be captured is needed for standardization and an adequate detection and response capability	Replace ODP with a list of event types and events to be captured, subject to device specific limitations.
54	SEI/CA	Technical	publication	17	632	assignment not required; additional information to be captured is dependent on the capability of the system to generate the event detail and not a specified requirement	delete Assignment statement
55	SEI/CA	Technical	publication	18	647	this is NFO specific and cannot be dictated by a Federal agency with universal application. While the agency can say what requirements it wishes to impose, that is likely one of many that the NFO needs to address in its record retention policy. The NFOs policy must dictate but it must be informed by multiple contract, agency, and other requirements	change to: Retain audit records retention policy which must be informed by applicable, contract requirements, laws, and regulations.
56	SEI/CA	Technical	publication	18	662	Alerting of personnel should be IAW the NFOs organization and policy which is specified in the 3.15.1 requirements. Personnel should be immediately notified when a process fails. The requirement as written requires only an alert. No action (i.e. fix it) is required	a. Alert personnel IAW NFO policy as described SSP section 3.15.1 when an audit logging process fails. b. Restore audit logging capability within 4 hours
57	SEI/CA	Technical	publication	19	675	Alerting only with no corrective action is unacceptable. Audit logging needs to be restored ASAP or the overall system integrity is potentially compromised.	delete: Organizations may decide… personnel.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
58	SEI/CA	Technical	publication	19	683	This is NFO specific and it is unrealistic for a federal agency to dictate specific roles or personnel requirements. This is required to be documented within 3.15.1	delete assignment replace with: Report findings IAW established NFO policy as documented in SSP section 3.15.1
59	SEI/CA	Technical	publication	20	724	Not an ODP	delete assignment specify time granularity to at least the second HH MM SS
60	SEI/CA	Technical	publication	21	769	Not an ODP	remove assignment replace with annually, in response to a vulnerability being discovered, anytime changes occur…..
61	SEI/CA	Technical	publication	21	784	3.4.2a refers to the system. This is more appropriate for a government defined FISMA boundary and for NFOs. The specification of configuration settings at this level is not appropriate for NFOs who have commercial as well as multiple Federal agency customers. NFOs may choose a bassline configuration standard or create their own to meet their business needs as opposed to adapting the business infrastructure to comply with a single agency or contract.	change a. to Establish, document and implement configuration settings for the system
62	SEI/CA	Technical	publication	21	785	ODP is too difficult to implement for NFOs with multiple Federal customers. While DoD may specify their STIGs and SRGs, many FEB agencies have their own "standards" or rely on publicly accessible standards. This would encourage isolated enclaves of CUI, each specific to a different customer and would result in an overall lower level of cyber hygiene. Most NFOs would prefer to implement this on their environment and a specific system. federal agencies have the luxury of using different standards within each FIMA boundary	delete assignment Require that baseline configuration (and associated configurations) settings be documented in the SSP section 3.15.1
63	SEI/CA	Technical	publication	23	833	The verification requirement is difficult and expensive to do especially for SMBs. In an assessment scheme, this would be difficult for a 3rd party to evaluate	change to assess impacted controls
64	SEI/CA	Technical	publication	23	864	The choice of ports/protocols etc. in use is determined by the NFOs business needs and cannot be determined by a federal agency. In fact, requirements imposed by one agency could impact an NFOs ability to serve a different agency or commercial client	3.4.6b is NFO specific and should be documented as to which ports/protocols/etc. are required for them to do business. After documenting a need, the specific port/protocol/etc. should be implemented
65	SEI/CA	Technical	publication	23	867	This requirement is superseded by and better implemented under 3.4.8	delete 3.4.6c
66	SEI/CA	Technical	publication	24	899	ODP is not appropriate	Delete Assignment Change to: at least annually
67	SEI/CA	Technical	publication	25	923	3.1.5 Least Privilege and 3.4.8 Authorized Software negate the need for this control. Organizations can grant limited admin functionality to users when needed (i.e. for developers to install libraries etc.) for a limited time period. "Normal" users can install authorized software from software center, play stores etc.	delete 3.4.9
68	SEI/CA	Technical	publication	25	943	ODP not needed. The inventory should be continually maintained for both licensing and vulnerability/patching reasons. That said, the inventory should be validated at least annually.	Delete assignment and replace with at least annually
69	SEI/CA	Technical	publication	26	971	As written, this control is difficult to understand, the ODPs are inappropriate for a Federal agency to define, and the applicability of the control is extremely limited and will not apply to most NFOs. When this situation occurs, the only option is to issue burner devices which then can never connect to NFO assets again because they are to be assumed compromised. Organizations subject to travel to high risk areas already do this	change to: Issues special purpose devices to users needing to travel to high risk areas. Prohibit the connection of these devices toother NFO assets
70	SEI/CA	editorial	publication	27	993	user should be users	…and authenticate system users…
71	SEI/CA	Technical	publication	27	995	Assignment Statement is inappropriate, cannot be adequately defined for an NFO by a Federal agency, and is very NFO specific. Additionally, this could lead to conflicting contractual requirements for an NFO. Situations requiring reauthentication should be detailed in the NFO policies and procedures which are required under 3.15.1	delete Assignment Statement replace with IAW NFO policies and procedures
72	SEI/CA	Technical	publication	27	1011	ODP is not required. All devices should be identified and authorized before connecting and all devices capable of authenticating should authenticate	change to: Uniquely identify, authorize and where possible authenticate devices before establishing a system or network connection.
73	SEI/CA	Technical	publication	28	1039	The -171r2 wording was better; system accounts is subject to mis-interpretation, includes local access, and would be difficult to assess	change to Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.
74	SEI/CA	Technical	publication	28	1050	ODP cannot be specified by a Federal agency; this is very NFO specific and is required to be specified in the NFOs policies and procedure in 3.15.1	delete assignment change to Receive authorization IAW NFO policies and procedures to assign…..
75	SEI/CA	Technical	publication	28	1052	requirement in b is unclear	
76	SEI/CA	Technical	publication	28	1053	There is little id any need to reuse identifier. ODP is not required; identifier re-use is prohibited and most NFOs already do that	change to Prevent reuse of identifiers
77	SEI/CA	Technical	publication	28	1054	Requirement is unclear but it seems like something that would apply to a government scenario where contractor or civilian is part of a users name in their email address. There is not an analogous scenario in the private sector	delete requirement d
78	SEI/CA	Technical	publication	29	1069	the combined 3.5.7 requirement is overly complex as is and was better as separate requirements	restore 3.5.8, 3.5.9 and 3.5.10

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
79	SEI/CA	Technical	publication	29	1070	ODP can lead to chaos for NFOs with the potential for vastly different requirements. Specify a minimum and allow NFOs to implement stricter policies as they can. Policy is required to be defined in 3.15.1	delete assignment Passwords must be AT LEAST 12 characters and draw from the four character types (upper, lower, numeric, special character)
80	SEI/CA	Technical	publication	29	1072	Spaces and all printable characters are not allowed in some systems. Requiring them to be allowed would force an NFO into non-compliance	change to: Allow user selection of long passwords and passphrases.
81	SEI/CA	Technical	publication	29	1077	Remove. Note that we don't believe Microsoft based systems can comply. It appears that you can save passwords as salted but they would also be saved not salted, which defeats the purpose of the requirement. If Microsoft can't comply this is a huge cost and changeover for almost all organizations.	delete requirement
82	SEI/CA	Technical	publication	29	1079	immediately is problematic	change to: immediately upon first use
83	SEI/CA	Technical	publication	29	1080	The use of temporary passwords is fine but they must be unique. Think Colonial Pipeline welcome2020. Accounts that get setup and not used with a standard initial password are easy targets for attack	change to Allow the use of a **unique** temporary…..
84	SEI/CA	Technical	publication	29	1099	Requirement to prevent password reuse has value and should not be withdrawn	restore 3.5.8 from r2 and set a value Prohibit password reuse for 24 generations.
85	SEI/CA	Technical	publication	30	1117	Requirement is unclear and appears to be of limited value.	delete requirement
86	SEI/CA	Technical	publication	30	1118	As worded seems overly complex for a relatively simple concept.	Verify identity prior to issuing credentials to an individual, group, role, service or device
87	SEI/CA	Technical	publication	30	1123	Credentials cannot be changed prior to first use.	Change prior to immediately after first use
88	SEI/CA	Technical	publication	30	1124	both assignment statements are inappropriate and indicate a mandatory password change policy when best practice says that may not be the best password management solution. Complex passwords, MFA, authentication tokes etc. when used in combination provide a greater level of security than frequent password changes	change to: Change or refresh authenticators IAW NFO policy
89	SEI/CA	Technical	publication	30	1126	Correct implementation of privileged access management and password vaults negate the need for this requirement and provide a more secure method of maintaining "shared" account access with a better audit trail and easier access management.	Make requirement contingent on no system in place to manage access
90	SEI/CA	Technical	publication	31	1173	ODP is not appropriate as this is NFO specific and required to be defined in 3.15.1	change to: Report incident information IAW NFO policies and procedures
91	SEI/CA	Technical	publication	32	1194	assignment not required	delete assignment replace with at least annually
92	SEI/CA	Technical	publication	32	1206	assignments not required	delete assignment replace with at least annually and following any significant incident or change
93	SEI/CA	Technical	publication	33	1234	Maintenance equipment would not typically be used to process, store, or transmit CUI and the likelihood that CUI ended up on it is low. C1 requires that the absence of CUI is verified but under 2 the equipment must still be sanitized or destroyed. They should be either or requirements. c3 requires an exemption be granted; no one at the NFO (or the Federal agency most likely) can suspend handling requirements and grant the exception	change to: c1 - Verify there is no CUI on the equipment c2 - If CUI is found on the equipment, sanitize IAW SP800-88 c3 - delete
94	SEI/CA	Technical	publication	34	1258	The control ignores cloud solutions. These requirements are focused on a traditional on premise solution where maintenance is performed over the internal network or by a third party connecting from outside the premise. While an NFO can monitor some of the non-local maintenance of the cloud, they cannot monitor all of it and in fact will often pay third parties to perform maintenance because they lack the capability to do it and hence cannot effectively monitor it	clarify that control apples to a local , on-premise
95	SEI/CA	Technical	publication	34	1258	Both 3.7.5 and 3.7.6 are difficult to implement and assess for cloud environments. While contractual arrangements can address some of these intents, a separate control for cloud solutions is needed. This control should address a customer responsibility matrix, any certifications the CSP has (i.e. FedRAMP, ISO 27001, SOC2 etc.), and contractual controls that should be specified	
96	SEI/CA	Technical	publication	34	1272	The control ignores cloud solutions. These requirements are focused on a traditional on premise solution and is impossible in a cloud environment.	clarify that control apples to a local , on-premise
97	SEI/CA	Technical	publication	35	1310	ODP not needed. Required to be documented in 3.15.1	delete Assignment change to IAW NFO policies and procedures
98	SEI/CA	Technical	publication	36	1339	NARA dictates the marking of CUI and NFOs and Federal agencies lack the authority to exempt items from those requirements, therefore b is not relevant	delete 3.8.4b
99	SEI/CA	Technical	publication	36	1354	The option for alternative physical controls was deleted but the discussion includes locked containers.	change to: Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
100	SEI/CA	Technical	publication	37	1375	Delete selection; restrict includes prohibit and is an NFO decision and should be defined for certain classes of users. Additionally, only NFO managed devices should be allowed. The ability to specify a particular portable storage devices and block all others is a relatively simple task. The devices can be centrally tracked, encrypted and controlled	change to: a. Restrict the use of portable storage devices to only those devices managed and issued by the NFO IAW established policies and procedures
101	SEI/CA	Technical	publication	37	1403	The requirement deleted the option for alternative physical controls but the option is described in the discussion	delete: or alternative physical controls

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
102	SEI/CA	Technical	publication	38	1414	3.9.1b seems to be a uniquely government issue related to SF85 and SF86 screenings; this is not a typical process within NFOs and is of limited benefit	delete 3.9.1b
103	SEI/CA	Technical	publication	38	1426	3.9.2a is duplicative of 3.1.1f and h	delete 3.9.2a
104	SEI/CA	Technical	publication	38	1433	3.9.2b2 is almost entirely assignment statements and is not clear as to intent. Documentation in 3.15.1 would cover this	delete or clarify intent
105	SEI/CA	Technical	publication	39	1460	This may be appropriate for NFOs that have an ESP perform work on site but is difficult to implement and validate. Including it in contract terms would provide a false sense of accomplishment if it couldn t be verified especially if the ESP is a CSP.	
106	SEI/CA	Technical	publication	39	1474	Control is traditional on-premise focused and is impossible to address if the system resides in the cloud	Clarify intent for applicability to on-premise
107	SEI/CA	Technical	publication	40	1492	Control is traditional on-premise focused and is impossible to address if the system resides in the cloud	Clarify intent for applicability to on-premise
108	SEI/CA	Technical	publication	40	1515	If CUI access is allowed at alternate work sites then there does not appear to be any option to apply a limited set of controls. Regardless of the approach, it is largely unenforceable and impossible to assess. If CUI is only accessible thru a VDI then an NFO can require that only NFO devices access the VDI. The only additional control to specify might be that the device used be oriented to prevent unauthorized viewing. If CUI access is prohibited at alternate work sites, then the NFOs policy and procedures apply. In many ways, the R2 wording was better	restore R2 wording
109	SEI/CA	Technical	publication	41	1530	The assignment statements throughout this control are not appropriate. Physical access requirements vary greatly across NFOs and it is unrealistic to expect a Federal agency could define a universal set of requirements.	
110	SEI/CA	Technical	publication	41	1531	Assignment would be impossible for a federal agency to define. As written, it also implies an on-premise system within space the NFO controls and ignores cloud. Simpler language would allow more implementations and not degrade security	change to: a. Enforce physical access authorizations
111	SEI/CA	Technical	publication	41	1534	Selection and assignment not appropriate. Suffices to say that access must be controlled IAW the NFOs policy	change to: 2. Control ingress and egress to the facility
112	SEI/CA	Technical	publication	41	1537	Assignment statement not required. NFOs should maintain access logs	change to: b. Maintain physical access audit logs
113	SEI/CA	Technical	publication	42	1558	Assignment not required. Simpler language will achieve the same result	change to: Control physical access to output devices to prevent unauthorized individuals from obtaining the output
114	SEI/CA	Technical	publication	42	1577	3.11.1 requires an organization to assess the risk of unauthorized disclosure of CUI and to update risk assessments at an organization defined frequency. There is no discussion of risk mitigation. Why assess the risk if nothing is to be done to address it.	Add risk mitigation plan requirement and add risk mitigation to the discussion. I would expect that tracking risks to their resolution would also be part of this and should be added.
115	SEI/CA	Technical	publication	42	1577	Not an NFO responsibility. Only the Federal agency can assess the risk of a CUI disclosure. If reworded to address general business risk, then the requirement makes sense. All NFOs should be performing a periodic risk assessment	delete requirement or update to remove specific CUI risk requirement
116	SEI/CA	Technical	publication	42	1579	As written should be deleted unless (a) is modified to address risk in general and not just CUI risk. ODP should be deleted	delete assignment and replace with at least annually IAW NFO policies and procedures
117	SEI/CA	Technical	publication	43	1599	3.11.2 vulnerability monitoring and scanning there is no discussion of tracking to closure vulnerabilities that cannot be immediately addressed or of verifying vulnerability remediations actually took hold or fully address the vulnerability.	Add verification of vulnerability remediations and tracking unresolved vulnerabilities to the requirements/discussion.
118	SEI/CA	Technical	publication	43	1600	ODP is not required. To be effective, vulnerability scanning should be performed at least monthly and whenever new vulnerabilities are detected in the wild	delete assignment statement replace with at least monthly
119	SEI/CA	Technical	publication	43	1602	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: Remediate vulnerabilities in accordance with the timelines established in the CISA Known Exploited Vulnerabilities Catalog
120	SEI/CA	Technical	publication	43	1604	This requirement really has no meaning. Vulnerability scanners typically do not have a definitions file like legacy AV software and access the latest set when a scan is initiated	delete requirement
121	SEI/CA	editorial	publication	44	1638	Section 3.11.4 Risk Response seems out of place. Why not have it follow section 3.11.1. It is also mainly about when to generate a POAM.	Move to after section 3.11.1.
122	SEI/CA	Technical	publication	44	1642	Discussion allows for risk acceptance/transfer etc. with justification. While accepted for Federal agencies under the RMF, it is not within the purview of NFOs which are required to implement the controls in 800-171	Update discussion around risk acceptance/transfer to make it appropriate to NFOs
123	SEI/CA	Technical	publication	44	1655	Assignment is not required. This should be done at least annually or in response to a significant change or event. This would be in alignment with the Federal authorization process	delete assignment statement replace with at least annually and when significant incidents or changes occur

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
124	SEI/CA	Technical	publication	45	1686	Assignment statement is not appropriate. POA&Ms should be updated as required to ensure currency as opposed to a predefined timeframe. They should be reviewed at least monthly to ensure progress is occurring	change to: Review at least monthly and update as needed the existing plan of action and milestones based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.
125	SEI/CA	Technical	publication	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."
126	SEI/CA	editorial	publication	46	1716	Section 3.12.5 Independent Assessment discusses the requirement for independent assessors. This would be better if it followed section 3.12.1 (control assessments) directly.	Move directly after section 3.12.1.
127	SEI/CA	Technical	publication	46	1716	Understanding that this is performed as part of the RMF ATO process, it is not appropriate for all NFOs to always have third party assessments and is prohibitively expensive. And given the lack of standardization that the ODPs introduce, NFOs would require independent control assessments for every agency they contract with. Recognizing the value of third party assessments, agencies can set individual requirements for self-assessment and independent assessment	delete requirement
128	SEI/CA	Technical	publication	46	1731	Within the construct of systems within a FISMA boundary, the concept of an ISA/MOU/etc. makes sense but its unclear what the requirement intends for an NFO without the same system definitions.	clarify the applicability of the requirement outside the construct of exchange between FISMA boundaries or in/out of a FISMA boundary. Alternatively delete the requirement
129	SEI/CA	Technical	publication	46	1733	ODP is not required	if 3.12.6 is maintained, delete assignment statement and changed to at least annually IAW NFO policies and procedures
130	SEI/CA	Technical	publication	46	1750	Purpose of the requirement is unclear. All connected components within the "system" are subject to the CUI controls and are internal so what additional benefit is achieved is unclear. Additionally, this is overreach by Federal agencies to specify that level of detail within an NFO environment	delete the requirement
131	SEI/CA	Technical	publication	47	1788	Second paragraph of the discussion is confusing and its unclear if it is relevant to NFOs	delete paragraph
132	SEI/CA	Technical	publication	49	1845	Although allowed within 800-53, this is difficult to implement correctly and virtually impossible to specify safeguards through the ODP. The many products and configurations available would effectively prevent the specification required. Newer tools being deployed within government and the private sector (i.e. Z-Scaler which is cloud based and FedRAMP High) implement the concept of a split tunnel with actually employing traditional split tunnels. This control would be better served to prevent the use of traditional split tunnels	change to: Prevent split tunneling for remote devices.
133	SEI/CA	Technical	publication	49	1867	3.13.11 is expected to require either FIPS or NSA validated algorithms therefor implying that any form of encryption is acceptable is counter productive.	Either specify FIPS and NSA algorithms or reference compliance with 3.13.11
134	SEI/CA	Technical	publication	50	1903	Assignment statement is overly complex and requires multiple parts. A standard approach (i.e. eliminate ODP and make part of the requirement) would be preferable but the actual specification can be quite complex.	Replace ODP with select guidance from 800-57
135	SEI/CA	Technical	publication	51	1915	Section 3.13.11 cryptographic protection needs more discussion	Update cryptographic protection discussion.
136	SEI/CA	Technical	publication	51	1915	There is a lack of clarity regarding the requirement to use FIPS-validated encryption suites. More accurately, it no longer seems required, but is rather just mentioned as a potential option (see, for example, 3.13.11). This represents a significant reduction in the security provided by cryptography as many vendors have implemented sound cryptographic algorithms such as AES-256 in unsound ways, reducing the value provided by the crypto. This comment applies to all requirements where cryptography is specified.	Cryptography is a complex field that is poorly understood by lay people and even most IT teams. Contractors will be poorly equipped to make appropriate choices regarding the implementation of cryptography without clear direction on specific allowed crypto suites. I strongly recommend returning to a requirement for FIPS-validated crypto, perhaps supplemented by another validation authority.
137	SEI/CA	Technical	publication	51	1917	Ultimately, this would be expected to be either a FIPS or NSA validated algorithm. NFOs will typically have an easier implementation path for FIPS validated so it should be the default with a provision for NSA validated algorithms in NSSS applications.	Implement FIPS 140-2/3 validated cryptography when used to protect the confidentiality of CUI unless NSA validated is otherwise required
138	SEI/CA	Technical	publication	51	1926	The ODP and exemption are not needed. It is better to simply prevent the remote activation of these deices	change to: Prohibit remote activation of collaborative computing devices and applications
139	SEI/CA	Technical	publication	52	1972	Requiring all outbound traffic to route through a proxy is of limited value. If the objective is to shield user web activity from tracking then that limited use case would be appropriate if the NFO could have trusted sites (i.e. web based HR, accounting, NFO email and collaboration etc. services). Note that a proxy server is not the only option for implementing web content filters and other options should be allowed if that is the objective.	Clarify the objective of the control and reword as appropriate. Allow other options beyond proxy servers
140	SEI/CA	Technical	publication	53	1994	This requirement is vague and kind of meaningless. NFOs typically do this simply because there is no need to add telecom service and associated on-prem devices which are not needed	Delete or clarify intent

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
141	SEI/CA	Technical	publication	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. NFOs are encouraged to patch sooner but this would align NFOs with FCEB agencies	Change to "Install security relevant software and firmware updates in accordance with the timelines established in the CISA Known Exploited Vulnerabilities Catalog."
142	SEI/CA	Technical	publication	54	2032	Organizational implies the NFO but clearer use of terms throughout would be helpful. IAW organizational (NFO) policy and procedure, which are documented under 3.15.1, would help reduce the number of ODPs and increase standardization	Clarify that organization in the context refers to other NFO
143	SEI/CA	Technical	publication	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"
144	SEI/CA	Technical	publication	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
145	SEI/CA	Technical	publication	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 mobile 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 if 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."
146	SEI/CA	Technical	publication	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
147	SEI/CA	Technical	publication	56	2130	Assignment Statement is not applicable	Delete Assignment Statement Change to "at least annual and following significant change or event."
148	SEI/CA	Technical	publication	57	2148	Assignment Statement is not applicable	Delete Assignment Statement Change to "at least annual and following significant change or event."
149	SEI/CA	Technical	publication	57	2168	Assignment Statement is not applicable	Delete Assignment Statement Change to "at least annual and following significant change or event."
150	SEI/CA	Technical	publication	57	2322	This control is redundant of 3.8.3 since the item must contain CUI. However, in the front matter :"The requirements apply to components of nonfederal systems that process, store, or transmit CUI **or that provide protection for such components.**"	Change to: Dispose of system components, documentation, or tools containing CUI or that provide protection for such components using the techniques and methods described in NISP SP 800-30
151	SEI/CA	Technical	publication	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."
152	SEI/CA	Technical	publication	58	2224	As written, 3.16.3 applies to all external service providers when it 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 that provide protection for such components
153	SEI/CA	Technical	publication	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
154	SEI/CA	Technical	publication	59	2225	The requirement as written is too open ended and the ODP is not applicable. 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."
155	SEI/CA	Technical	publication	59	2230	The requirement as written is too open ended and the ODP is not applicable. 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
156	SEI/CA	Technical	publication	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"
157	SEI/CA	Technical	publication	59	2255	Assignment Statement is not applicable	Delete Assignment Statement Change to "at least annual and following significant change or event"
158	SEI/CA	Technical	publication	60	2277	This requirement is included under 3.17.1 and is redundant. Add "implement" to 3.17.1	Delete requirement

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
159	SEI/CA	Technical	publication	60	2305	The requirement as written is too open ended and the ODP is not applicable. 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
160	SEI/CA	Technical	publication	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.
161	SEI/CA	Technical	publication	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
162	SEI/CA	editorial	publication	74	2811	references NSA approved cryptography which d/n exists in glossary. While the 800-53 definition may be more appropriate for -171 purposes, The definition from CNSSI 4009-2015 may be better to incorporate in both documents	add definition: Cryptography that consists of an approved algorithm, an implementation that has been approved for the protection of classified information and/or controlled unclassified information in a specific environment, and a supporting key management infrastructure. (NIST SP 800-53r5)