From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] 2ND and FINAL SUBMISSION DoD CIO CS :: Comments on NIST SP 800-171r3 final public draft
Date: Friday, January 26, 2024 1:55:28 PM
Attachments: sp800-171r3-fpd-comment_DoDCIOCSv2.xlsx
sp800-171Ar3-ipd-comment-DoDCIOCS.xlsx

Please use this 2nd submission as official submission for DoD CIO CS and disregard initial submission 26 January 2024 at 1146. One line item updated from initial submission.

Please see FPD comments for NIST SP 800-171 draft Rev3 and IPD for NIST SP 800-171A draft Rev3 from DoD CIO CS and advise if you have any questions.

Kindest Regards,
Dana C Mason, GCPM, CDPSE, CISM, CGRC
IT Specialist
Office of the DoD CIO, CMMC Program Office
[redacted]

From: Mason, Dana C CIV OSD DOD CIO (USA)
Sent: Friday, January 26, 2024 11:46 AM
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: DoD CIO CS :: Comments on NIST SP 800-171r3 final public draft

Please see fpd comments for NIST SP 800-171 draft Rev3 from DoD CIO CS.

Thank you,

Kindest Regards,
Dana C Mason, GCPM, CDPSE, CISM, CGRC
IT Specialist
Office of the DoD CIO, CMMC Program Office
[redacted]

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	G.Guissanie/DoD CIO/CS	General	Publication	2	31	As noted in previous comments to the IPD, the 'applicability' statement "The security requirements in this publication are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components" has been (in 800-171r2) purposely misinterpreted to mean that the requirements only apply to components that actually process, store or transmit CUI and the other components (e.g., servers, workstations) that do not process CUI need not meet the requirements. Per earlier suggestion, this problem has been mitigated in the FPD by adding back previous 171r2 guidance (at line36) that "If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain." While this additional clarification is welcome, the original language at line 31 can nevertheless be misinterpreted and should be modified.	Rephrase applicability statement to read "The security requirements in this publication are only applicable to nonfederal systems that process, store or transmit CUI, and the components within that are capable of processing, storing or transmitting CUI or that provide protection for such components."
2	G.Guissanie/DoD CIO/CS	General	Publication	4	88	The statement "Organization-defined parameters (ODPs) are included for some requirements. These ODPs provide flexibility through the use of assignment and selection operations to allow federal agencies and nonfederal organizations to specify values for the designated parameters in the requirements" is problematic. It is noted that the FPD now allows the option for nonfederal organizations to specify the values, but this is still a problem, as it creates confusion as to who is responsible for establishing the requirement. Clearly, the 'organization' should be the non-federal organization (the owner/operator of an information system NOT operated on behalf of the government, but for internal business purposes) and it would be inappropriate for a USG agency to specify what parameters are assigned. Aside from having no knowledge of the nonfederal organization's system, it is especially problematic in that different Agencies (or different elements within an Agency) would almost certainly specify different parameters for the same requirement, creating unnecessary churn and a chaotic security environment if the nonfederal org has to continually accommodate differing or conflicting requirements simultaneously. It also creates unacceptable contract administration issues for the USG, expected to issue some 100K contracts a year requiring compliance with NIST SP 800-171, as it is simply not possible for the USG Requiring Activities/Contracting Officers to complete the many ODPs in rev3 for each contract. Note also that only a few of the many ODPs are simple enough (e.g., frequency of review or update) for the Agency to specify a value – the rest require knowledge of the system operation to complete, which the Agency does not have, and so should be left to the nonfederal organization. Nevertheless, inevitably Agencies will attempt to specify such parameters.	Remove the ODPs from the individual requirements (and the portion of Section 2.2 discussion ODP's) as unnecessary. The NIST SP 800-171r2 requirement statements, without ODPs, established the requirement for the nonfederal organization to specify the necessary parameters to implement the requirement in their SSP or associated documents – a 'fill-in-the-blank' requirement statement is unnecessary. If NIST requires retention of the ODPs to align with 800-53 controls, it should make clear in Section 2.2 that the ODPs are to be assigned by the nonfederal organization. If there is a concern that the nonfederal org may select inappropriate parameters, NIST can provide in 800-171 a suggested range of acceptable values (or point to an appropriate reference). Agencies can, as always, review the SSP and address any concerns with the nonfederal org.
3	G.Guissanie/DoD CIO/CS	General	Publication	15	487	Requirement 3.1.20.c.2 states "Retention of approved system connection or processing agreements with the organizational entity hosting the external system." As noted in the earlier IPD comment to what was then 3.1.22, 'retention' is not the right term, since an agreement must be consummated before it can be 'retained.' In this context, 'Establishment" or Establishment and maintenance' is more appropriate.	Suggest replacing 'Retention' with 'Establishment' or 'Establishment and maintenance.'
4	G.Guissanie/DoD CIO/CS	General	Publication	14	517	Discussion in requirement 3.1.22 (and in 7 other requirements) cites "applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines." This phrase in not meaningful to nonfederal organizations, as 'Executive Orders, directives …' (and most laws directed at the USG) generally do not apply to nonfederal organization's except as separately implemented via the contract or agreement. Inclusion of this phrase will be confusing to most nonfederal organizations or ignored and should be eliminated as unnecessary. If NIST is aware of a specific law or other government policy that applies to the requirement, it should be identified.	Delete the phrase 'applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines' in this and subsequent requirements. In the case of requirement 3.1.22, the Discussion could simply state "in accordance with the contract or agreement, unless cleared for public release, the nonfederal organization is typically not authorized to provide the public access to information provided by or developed for the government."
5	G.Guissanie/DoD CIO/CS	General	Publication	50	1825	As noted with the comments to the IPD, the 3.13.11 requirement leaves the type of cryptography open and the Discussion notes only that it should be '… implemented in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines" which is meaningless to the nonfederal and (most) USG organizations. The Discussion then notes that "FIPS-validated cryptography is described in [identified references]" – which is also meaningless since 'FIPS-validated cryptography' is not otherwise mentioned in the requirement or Discussion. However, per the CMVP program, NIST's position is that "Non-validated cryptography is viewed by NIST as providing no protection to the information or data—in effect the data would be considered unprotected plaintext. If the agency specifies that the information or data be cryptographically protected, then FIPS 140-2 or FIPS 140-3 is applicable. In essence, if cryptography is required, then it must be validated. Should the cryptographic module be revoked, use of that module is no longer permitted" [https://csrc.nist.gov/projects/cryptographic-module-validation-program]. So why change the requirement from the current 800-171r2 wording: "Employ FIPS validated cryptography when used to protect the confidentiality of CUI"??	As recommended previously, change wording of requirement to current NIST SP 800-171r2 wording: "Employ FIPS validated cryptography when used to protect the confidentiality of CUI."
6	G.Guissanie/DoD CIO/CS	General	Publication	51	1842	Requirement 3.13.12. Collaborative Computing Devices and Applications. As noted in comments to the IPD, the Discussion for Requirement 3.13.12 notes in the last line that 'Solutions to prevent device usage include webcam covers and buttons to disable microphones" but the requirement does not discuss 'preventing device usage' but rather 'remote activation' and 'explicit indication of use' which are entirely different.	Remove last sentence on solutions to prevent device usage from the 'Discussion' or modify the requirement to make it relevant.
7	G.Guissanie/DoD CIO/CS	General	Publication	56	2039	Requirement 3.15.2. System Security Plan. In the list of the required contents of a System Security Plan, item 4 ('Provides an overview of the security requirements of the system') does not accurately represent the requirement to describe 'how the security requirements are implemented', as described in the SSP definition in the glossary and in NIST SP 800-18 ("A document that describes how an organization meets or plans to meet the security requirements for a system. In particular, the system security plan describes the system boundary, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems.) The requirement to describe HOW security requirements are implemented is extremely important, as it is the simplest way for a reviewer to insure the nonfederal organization actually understands the requirement. The current description to 'provide an overview of the security requirements of the system' in no way meets the SSP definition.	Change item 4 to add 'and how the security requirements are implemented' such that it reads "Provides an overview of the security requirements of the system and how the security requirements are implemented."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
8	Dana Mason/DoD CIO/CS	General	Publication		All	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.	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.
9	Dana Mason/DoD CIO/CS	General	Publication		All	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 feasible.	Make all requirements achievable at the enterprise level.
10	Dana Mason/DoD CIO/CS	General	Publication		All	Recognizing the desire for alignment with 800-53, the varied density of requirements affects the ability to apply a balanced assessment scheme on 800-171 and other related frameworks and models. Security requirement 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 the 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 uniform scoring, assessment, and management.
11	Dana Mason/DoD CIO/CS	Editorial	Publication		All	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").
12	Dana Mason/DoD CIO/CS	General	Publication		All	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.
13	Dana Mason/DoD CIO/CS	Technical	Publication	5	117	The term organization remains ambiguous throughout the document.	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.
14	Dana Mason/DoD CIO/CS	Technical	Publication	6	140	3.1.1 This requirement is too dense and cannot be evaluated the same as a single statement requirement. Recognizing the desire for alignment with 800-53, Account Management has 21 assessment objectives whereas 3.1.2 has a single one. An NFO can have a good account management process and still struggle to implement this control due the structure and organization of the requirement. Some of the requirements are addressed elsewhere as well and although related to account management are better served to be identified elsewhere.	Portions of E, F, and G are covered or can be covered in alternate sections. Section 3.9.2 Personnel Termination and Transfer covers 3.1.1 G and F 4, 5 can be added to 3.9.2. As well as Section 3.10 Physical Protection covers 3.1.1 E in terms of monitoring . This would give reason to delete e, f, and g.
15	Dana Mason/DoD CIO/CS	Technical	Publication	9	252	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. [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] needs to reference back to the NFO policies and procedures in 3.15.1 versus being an ODP. [d] Assign a time period.
16	Dana Mason/DoD CIO/CS	Technical	Publication	9	276	3.1.6[a] Government will not be able to assign this ODP. Reference to 3.15.1 and removed ODP.	change to: a. Restrict privileged accounts on the system to those personnel and/or roles identified in organizational policy as required by requirement 3.15.1
17	Dana Mason/DoD CIO/CS	Technical	Publication	10	313	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.	change to Limit the number of consecutive invalid logon attempts to 3 within a 10 minute time period
18	Dana Mason/DoD CIO/CS	Technical	Publication	15	489	3.1.20 [c][2] BYOD agreements would be between the NFO and an individual, typically an employee of the NFO, and not between two organizational entities. Suggest a change to the language to clarify that a BYOD agreement would also be required	change to: individual owning or organizational entity hosting the external system
19	Dana Mason/DoD CIO/CS	Technical	Publication	15	490	3.1.20 [d] The use of external storage devices should be controlled regardless of ownership and not just for NFO managed devices	change to: Restrict the use of portable storage devices on external systems
20	Dana Mason/DoD CIO/CS	Technical	Publication	18	601	3.3.1 This requirement is dependent on the type of system generating the log. While a list is provided in suggested change, a reference to M-21-31 Basic Logging may be more appropriate.	Also, logging requirements are dictated by industry (ie healthcare, legal, financial etc) remove ODP and Change to a. Specify event types for audit logs using the guidance in M-21-31 Basic Logging and NIST 800-92, and as required by applicable law or regulatory standards

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
21	Dana Mason/DoD CIO/CS	Technical	Publication	20	664	3.3.4 3.3.4[a] Government 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, and 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.	change to: a. Alert organizational personnel in the event of an audit logging process failure. b. Restore the audit logging process. Discussion - remove the last sentence ("Organizations may decide to take no additional actions after alerting designated roles or personnel."), they have to fix it.
22	Dana Mason/DoD CIO/CS	Technical	Publication	23	788	3.4.2[a] It's not obvious what would go into the ODP besides the STIGS or perhaps the CIS Baseline for cloud systems. 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.
23	Dana Mason/DoD CIO/CS	Technical	Publication	25	868	3.4.6 [b] While there are port and service conventions that are typically used and deviation from convention could be restricted, each environment is different and different ports, protocols., services, etc. are required to support business functions. A blanket allow/prohibit is unrealistic. Likewise, an IoT device may require mail relay over port 25 because it does not support TLS. While not secure, it may be necessary from a business perspective and the organization would need to take appropriate actions to prevent the exploit of the unsecured mail relay.	delete ODP change to: b. Prohibit or restrict the use of functions, ports, protocols, connections, and services except for those required to support essential mission or business functions.
24	Dana Mason/DoD CIO/CS	Technical	Publication	27	960	3.4.12 Ideally, travel to high risk areas would not include taking devices containing CUI and any devices would have limited utility and not be reattached to the NFO network upon return. The NFO needs to make a business decision on what can go to high risk areas and then continue to be used as not every organization can afford "burner" devices which are scrapped upon return. The decision and approach would likely involve the person traveling, the purpose of the travel, and the opportunities for a threat actor to access a device. While the basic tenants of the requirement are sound, it cannot be pre-determined and is circumstantial	Delete the requirement or require that NFOs have a documented policy and process regarding use of devices in high risk areas in 3.15.1
25	Dana Mason/DoD CIO/CS	Technical	Publication	30	1048	3.5.5[c] ODP is unnecessary, could just end after identifiers. Reuse of identifiers is technically impractical in most cases and there is virtually no business case for doing so. Reuse should always be prohibited. The case of an employee who left and returned to an organization could have an identifier restored but since this is the same identifier for the same person it would not be a reuse.	change to: c. Prevent the reuse of identifiers. Or Apply a NIST defined upper limit to eliminate the implication of maintaining the same identifiers indefinitely
26	Dana Mason/DoD CIO/CS	Technical	Publication	33	1170	3.6.2[b] Government cannot establish a single time and even within a department the type of compromise may dictate the notification time. Likewise, the appropriate authorities to notify are dependent on the nature of the incident. This requirement is essentially to have and execute an Incident Response Plan and the execution of the IRP needs to happen as soon as the incident is suspected. The IRP will contain the necessary information regarding notifications and timelines	change to: a. Execute the Incident Response Plan immediately upon detection of events which may indicate an incident b. Report the initiation of the IRP to organizational managers, law enforcement, and sponsoring agencies IAW the severity of the incident, contractual requirements, and the plans notification procedures.
27	Dana Mason/DoD CIO/CS	Technical	Publication	34	1209	3.6.4a.1 Training should be provided before assuming the role.	delete ODP change to: Prior to obtaining system access in an incident response role
28	Dana Mason/DoD CIO/CS	Technical	Publication	35	1237	3.7.5 Ignores cloud and hybrid solutions. While non-local maintenance can be observed and monitored on some aspects of a cloud solution, actions taken by the CSP are transparent to the NFO. Likewise, maintenance of a PaaS system can be performed by a third party or NFA staff via a CSO dashboard which would typically not have the ability to be seen by more than the party performing the action unless a second individual was physically present to observe. If using a MSP to administer systems or applications, the MSP would typically perform actions as dictated by contractual terms and the NFO would most likely lack the personnel with skills need to effectively monitor. Clearly defined roles and separation of duties along with adequate logging, correlation, and audit practices are designed to prevent and detect any discrepancies introduced during maintenance. This requirement implicitly is focused on on-premises solutions where nonlocal access is used to administer the system.	Add to discussion section Requirements for cloud maintenance should be implemented
29	Dana Mason/DoD CIO/CS	Technical	Publication	36	1283	3.7.6 As written, this requirement ignores cloud implementations. If an organization is subscribing to a SAAS environment, all of these are difficult if not impossible to do. Implementation in other than the on-premises architectures are far more common and this control (along with 3.10 requirements) need to be directed at organizational facilities and systems. For other implementations, contractual requirements, other certifications (i.e. FedRAMP) will dictate how these requirements are implemented. In those cases, the NFO will never maintain lists of individuals.	add to requirement before a thru d list: **Where the organization has direct physical or logical control to systems which process, store, or transmit CUI, the organization must:** a .... b ... c ... d ...
30	Dana Mason/DoD CIO/CS	Technical	Publication	38	1364	3.8.5 Cryptographic mechanisms deleted as a requirement but remains as an assessment objective in -171a IPD. Also discussion refers to 3.13.11 as a related requirement and discusses cryptographic protections. This requirement is greatly improved with the restoration of the cryptographic protection.	add: c. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI stored on digital media during transport.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
31	Dana Mason/DoD CIO/CS	Technical	Publication	39	1388	3.8.7 The ODP is too broad and difficult to define. Only organizationally owned devices under active management should be permitted	[a] Change to Allow the use of only organizationally-managed media.
32	Dana Mason/DoD CIO/CS	Technical	Publication	40	1434	3.9.1[a] Add authorizing or "elevating " access to the system. [b] Remove. Periodic rescreening imposes an excessive cost across the NFO for limited benefit. At the 800-172 level you get into adverse information which will require this for specialized CUI ,	[a] Add when "elevating" access. [b] Remove.
33	Dana Mason/DoD CIO/CS	Technical	Publication	41	1482	3.10.1 Add organizational facilities to the requirement as the NFO has direct responsibility for this requirement only in the facilities where it controls physical access i.e. leased or owned facilities. Cloud/datacenter/etc. locations would not be under the control of the NFO. Contractual terms or other authorizations (i.e. FedRAMP) would dictate the physical access authorizations to facilities where CUI is hosted.	change to: For organizational facilities where CUI is processed, stored, or transmitted: a. Develop, approve, and maintain a list of individuals with authorized access to the physical location where the system resides. b. Issue authorization credentials for physical access. c. Review the physical access list periodically. d. Remove individuals from the physical access list when access is no longer required.
34	Dana Mason/DoD CIO/CS	Technical	Publication	42	1501	3.10.2 Add organizational facilities to the requirement as the NFO has direct responsibility for this requirement only in the facilities where it controls physical access i.e. leased or owned facilities. Cloud/datacenter/etc. locations would not be under the control of the NFO. Contractual terms or other authorizations (i.e. FedRAMP) would dictate the physical access authorizations to facilities where CUI is hosted.	change to: For organizational facilities where CUI is processed, stored, or transmitted: a. Monitor physical access to the location where the system resides to detect and respond to physical security incidents. b. Review physical access logs periodically.
35	Dana Mason/DoD CIO/CS	Technical	Publication	42	1530	3.10.6[b] The requirement as written is too broad and relies almost entirely on the ODP for specification and enforcement. Alternate work sites span the range from hot spots in coffee shops, employee home offices, and hotel rooms when on travel.	change to: Define and implement privacy and physical security requirements to ensure compliance with CUI handling and storage requirements when employees use alternate work sites. Add to discussion section Alternate work sites should ensure that CUI cannot be viewed by unauthorized personnel and is properly secured when not in use. These general alternate work location requirements are circumstantial; performing work with CUI in a dedicated home office is different than working from home in a communal space. Additionally, working from a hotel while on travel is a different environment than working in a corner coffee shop. Travel to certain areas may necessitate additional requirements and behaviors. See security requirement 03.04.12
36	Dana Mason/DoD CIO/CS	Technical	Publication	43	1548	3.10.7[c]. Visitors should always be escorted. Non-employees who regularly access the facility are not considered visitors if the NFO has granted them permanent physical access and would therefore not require escort.	change to: [c] Escort visitors and control visitor activity.
37	Dana Mason/DoD CIO/CS	Technical	Publication	45	1686	3.12.5 The Selection statement is not required. The NFO need not use one method to document interconnection agreements and in fact the choice of agreement is dependent on the circumstances and the type of parties involved. Further, a combination of these items is the most likely to be used, will likely be the most effective, differ for any scenario and may rely on something not specified in the Selection. Individual regulated industries may impose additional artifacts not covered in the Selection which are equally effective. For example: When exchanging CUI with a subcontractor, a Federal contractor will likely 1) incorporate the basic contract terms regarding CUI into the subcontract agreement 2) specify any technical requirements in an ISA 3) require corporate and personal NDAs regarding control and disclosure of CUI 4) require the sub complete SCRM questionnaire which is typically cloud based	Change to: Document, approve and manage the exchange of CUI between the system and other systems.
38	Dana Mason/DoD CIO/CS	Technical	Publication	50	1822	3.13.11 FIPS-validated or NSA-approved are really the only options so the ODP is not really needed. Regardless, need to tie this requirement back to all the other requirements 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.	change to: Implement FIPS validated or NSA approved cryptography whenever cryptographic protections are required.
39	Dana Mason/DoD CIO/CS	Technical	Publication	52	1882	3.14.1 Requirement to test software has been deleted. This weakens the control unnecessarily.	add: c. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
40	Dana Mason/DoD CIO/CS	Technical	Publication	53	1909	3.14.2c.1 Routine, periodic scans are not required nor are they an option with advanced detection programs. Once installed and a full scan run, continuous scans preclude the need for periodic scans. 3.14.2.c.2 - take other actions as written allows the option of doing nothing. Specify that other actins need to be directed towards mitigation	delete requirement for periodic scans and the ODP. Change 3.14.2c.1 to read: Perform real time scans of files from external sources at endpoints or network entry and exit points as the files are downloaded, opened, or executed. Perform periodic (or ODP frequency) scans of systems where continuous monitoring and scanning is not implemented Change 3.14.2c.2 to read: Block malicious code, quarantine malicious code, or take other MITIGATING actions in response to malicious code detection.
41	Dana Mason/DoD CIO/CS	Technical	Publication	53	1943	3.14.3.[c] Established timeframes and security directives is vague. Within the 800-53/FISMA structure, the concept of both is much clearer. CISA for example issues BODs which have implementation timelines required by Federal agencies. There is no analogous system or requirement that applies to NFOs.	Delete the requirement. Compliance in this context would be voluntary on the part of the NFO
42	Dana Mason/DoD CIO/CS	Technical	Publication	55	1999	3.14.7 was deleted from the IPD. While spam detection does not directly impact CUI confidentiality or integrity, email remains an active attack vector for the compromise of systems. Recommend restoring the requirement with addition for phishing prevention and detection added	3.14.8. Email Protection Implement email protection mechanisms at designated locations within the system to detect and mitigate the effects of phishing attacks. DISCUSSION System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Malicious code can be transported by different means, including email, email attachments, and web accesses. Phishing and spear phishing attacks attempt to harvest credentials and/or data through the use of deceptive emails. Protection mechanisms include signature definitions. REFERENCES Source Controls: SI-8 Supporting Publications: SP 800-45 [81], SP 800-177 [74]
43	Dana Mason/DoD CIO/CS	Technical	Publication	55	2001	3.14.8 Requirement applies to Federal systems and does not have direct applicability to NFOs. Contractual terms as well as agency regulations already specify retention requirements for contractors	Delete the FPD version of 3.14.8
44	Dana Mason/DoD CIO/CS	Technical	Publication	57	2075	3.16.1 Unsure what the focus of the requirement is. As written it appears to be more focused on Federal acquisition requirements.	change to: Include security requirements in subcontract and vendor agreements commensurate with requirements in the NFO's contract with the Federal agency.
45	Dana Mason/DoD CIO/CS	Technical	Publication	58	2121	3.16.3[a] 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).	change to: a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with requirements as set forth in the contract between the Federal agency and the NFO
46	Dana Mason/DoD CIO/CS	Technical	Publication	59	2148	3.17.1 [a] For consistency with 3.17.2 which clearly requires implementation, require implementation of the SCRM plan as well	change to: a. Develop **AND IMPLEMENT** a plan for managing supply chain risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.
47	Dana Mason/DoD CIO/CS	General	Overlay		All	There isn't a way for ogranizations that use the overlay to know what controls or portions of controls that they are compliant with. It would be helpful for organizations to be able to visually see what controls on the overlay that they are compliant or partially compliant to be able to make adjustments as an organization. Doesn't aid NFOs to measure their compliance. Add XXXX to make it useful in assessments.	Include the ability to change entire control groups to green to show that an organization is compliant with that control. Also allow for an entire control to be made red when not compliant with a control group. There should also be functionality for control groups to be marked yellow to show partially compliant, while also having red and green markers within the sub categories of a control to show what sub categories that an organization is and is not compliant with.
48	Dana Mason/DoD CIO/CS	General	Overlay		All	To provide ease of use for organizations, the ability to collapse controls and expanding them should be implemented to better navigate the CUI overlay. In combination with the first suggestion, you could easily navigate to controls that are partial or not compliant , while skipping those that the organization is already compliant with.	Add expand and collapse buttons for each control for better overlay navigation.
49	Dana Mason/DoD CIO/CS	General	Overlay		All	Currently Column E has numbering before the requirement statement which duplicates the information in Column D and makes it difficult to filter, sort and search.	Remove the numbering in Column E and just have the security requirement similar to how the numbering in 800-53 is done.
50	Dana Mason/DoD CIO/CS	General	Overlay		AC-02-00-02	NFO tailoring criteria has been removed from -171r3. Recommend tailoring criteria reflect that the control is not important to the protection of CUI.	Change to NCO.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
51	Dana Mason/DoD CIO/CS	General	Overlay		AC-02-00-03	NFO tailoring criteria has been removed from -171r3. Recommend tailoring criteria reflect that the control is not important to the protection of CUI.	Change to NCO.
52	Dana Mason/DoD CIO/CS	General	Overlay		AC-02-00-18	NFO tailoring criteria has been removed from -171r3. Recommend tailoring criteria reflect that the control is not important to the protection of CUI.	Change to NCO.
53	Dana Mason/DoD CIO/CS	General	Overlay		AC-07-00-02	NFO tailoring criteria has been removed from -171r3. Recommend tailoring criteria reflect that the control is not important to the protection of CUI.	Change to NCO.
54	Dana Mason/DoD CIO/CS	General	Overlay		AU-02-00-01	NFO tailoring criteria has been removed from -171r3. Recommend tailoring criteria reflect that the control is not important to the protection of CUI.	Change to NCO.
55	Dana Mason/DoD CIO/CS	General	Overlay		CA-07-00-03	NFO tailoring criteria has been removed from -171r3. Recommend tailoring criteria reflect that the control is not important to the protection of CUI.	Change to NCO.
56	Dana Mason/DoD CIO/CS	General	Overlay		MA-03-00-02	NFO tailoring criteria has been removed from -171r3. Recommend tailoring criteria reflect that the control is not important to the protection of CUI.	Change to NCO
57	Dana Mason/DoD CIO/CS	General	Overlay		PE-17-00-03	NFO tailoring criteria has been removed from -171r3. Recommend tailoring criteria reflect that the control is not important to the protection of CUI.	Change to NCO.
58	Dana Mason/DoD CIO/CS	General	Overlay		All	The current overlay shows the one to many relationship from the perspective of 800-53. A second tab in the overlay which shows the same information from the perspective of 800-171r3 resolves the repeated references to standards from 800-171 r3. Bi-directional mapping (Allowing 800-53 to be mapped to 800-171 r3 and vice versa) will allow NFOs to see which 800-53 controls (subject to tailoring) are relavent for their implementation of a specific 800-171 requirement. This would significantly enhance usability from the NFO's perspective, while preserving machine readability aspects of the CUI overlay.	Add an additional tab for organizations to see 800-53 mapped to 800-171 r3 in addition to the current overlay that maps 800-171 r3 to 800-53. For a suggested change, see attached screenshot below.

Unique Sort ID (FPD 800-171r	SP 800-171 Rev 3 Security Requirement	Tailoring Decision	Unique Sort ID (800-53r5)	SP 800-53 Rev 5 Control & Control Enhancement
03-15-01:	3.15.1 Policy and Procedures	CUI		Policy and Procedures
			AC-01-00-01	
			AC-01-00-02	
			AC-01-00-05	
			AC-01-00-06	
			AT-01-00-06	
			AT-01-00-07	a. Develop, document, and disseminate to [Assignment: organization-
			AT-01-00-10	defined personnel or roles]:
			AU-01-00-04	1. [Selection (one or more): organization-level; mission/business process-
			AU-01-00-05	level; system-level] access control policy that:
	Develop, document, and disseminate to organizational personnel or roles, policies and		AU-01-00-08	2. Procedures to facilitate the implementation of the awareness and
03-15-01a.	procedures needed to implement security requirements.	CUI	... SR-01-00-05	training policy and the associated awareness and training controls;
			AC-01-00-07	
			AC-01-00-08	
			AC-01-00-09	
			AT-01-00-12	
			AT-01-00-13	
			AT-01-00-14	c. Review and update the current access control
			AU-01-00-10	1. Policy [Assignment: organization-defined frequency] and following
			AU-01-00-11	[Assignment: organization-defined events]; and
			AU-01-00-12	2. Procedures [Assignment: organization-defined frequency] and following
03-15-01b.	Review and update policies and procedures periodically.	CUI	... SR-01-00-09	[Assignment: organization-defined events].

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Dana Mason/DoD CIO/CS	Technical	4	342	Examine targets assessment objects and specifications. Activities are used in test, as stated in line 344. It doesn't make sense to meaningfully observe a specification or object and the other verbs adequately cover Examine.	Remove "observing"
2	Dana Mason/DoD CIO/CS	Technical	4	345	"Assessment methods include attributes of depth and coverage, which define the rigor, scope, and level of effort for the assessment as well as the degree of assurance that the security requirements have been satisfied." This sentence appears to be taken from 800-53A.Text states that methods include attributes of "depth and coverage" without providing in-line explanation of what those terms mean or how they are relevant for an assessor. Recommend define depth and coverage in-line with the text and state how they are related to whether an objective is determined as met.	Add "The appropriate depth and coverage attribute values for a particular assessment method are based on the assurance requirements specified by the organization and are an important component of protecting information commensurate with risk (i.e., risk management). As assurance requirements increase with regard to the development, implementation, and operation of controls within or inherited by the system, the rigor and scope of the assessment activities (as reflected in the selection of assessment methods and objects and the assignment of depth and coverage attribute values) tend to increase as well." and provide a reference to 800-53A because there is additional guidance.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
3	Dana Mason/DoD CIO/CS	Technical	5	381	The concepts of satisfied and other than satisfied are introduced and is based on assessment objectives being met. Met and not met is a clearer way a representing the evacuation of an assessment objective and compliance with a control. Satisfied implies a spectrum of options as opposed to a single yes/no.	change to: The findings are compiled and used as evidence to determine whether the security requirement has been met or not met. A finding of met indicates a fully acceptable result. A finding of not met indicates that there are potential anomalies that need to be addressed by the organization. A finding of not met may also indicate that the assessor was unable to obtain sufficient information to make the determination called for in the determination statement. For assessment findings that are not met, organizations may define subcategories of findings to indicate the severity or criticality of the weaknesses or deficiencies discovered and the potential adverse effects of those weaknesses or deficiencies on the missions and/or business functions of the organization. Defining such subcategories can help to establish priorities for risk mitigation actions.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
4	Dana Mason/DoD CIO/CS	Technical	5	388	Understand why "other than satisfied" is being used. However, absence of sufficient information needs to be resolved. If an assessment can be performed over a period of time, then the availability of information, personnel, or test results should not be a factor. The absence of information indicates an open item in the assessment and the assessment is not complete. Other than satisfied should be limited to practices that do not comply with the requirement.	Create third category that would be "not assessed or not rated"
5	Dana Mason/DoD CIO/CS	Technical	5	388	Subcategories are out of scope of the assessment and may be done as part of improvement planning/risk management activities. An assessment is a snap shot of where the organization is in relationship to requirements at a particular moment in time. The findings are evidence based. Determining severity, criticality, impact and priorities are activities that normal happen outside of the scope of the assessment. Since this document focuses on assessment, this information should be removed.	Remove paragraph and place in supplemental documentation

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
6	Dana Mason/DoD CIO/CS	Technical	5	399	Need to better explain the two roles and the differences. From the description, assessors compile evidence, conduct different types of activities, and build an assurance case. However, not clear as to what happens to requirements that are not met. Since many of the requirements have multiple parts, an organization may be addressing some, but not all of the requirements. There is no mention where this information is documented. Also, from the description, hard to tell whether an assessor can also be the designated official. Since the assessors are building the assurance case, they are determining compliance. Therefore, the role of the designated official is to provide an objective approval of the assurance cases. Where internal personnel are designated officials, there should be appropriate checks and balances to insure objectivity.	Add sentence(s) to clarify the two roles.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
7	Dana Mason/DoD CIO/CS	Technical	5	413	First sentence of this paragraph is not really true. The evidence is what is assessed to determine compliance and comes from the organization being assessed. Assessors review the evidence and determine if an assessment objective is met.	change to: The evidence which demonstrates the implementation of the safeguards and countermeasures selected to satisfy the security requirements is assessed and a determination is made if that evidence adequately demonstrates that an assessment objective is fully met and therefore compliant.
8	Dana Mason/DoD CIO/CS	Editorial	6	417	Who is conducting assessments and assurance cases are combined together into one paragraph. Break into two paragraphs since who is a different concept from the what (assurance case).	Start a new paragraph on line 418 on page 5.
9	Dana Mason/DoD CIO/CS		7	452	Each user should have which systems they have access to, what are their memberships, and the authorizations given them. This should be tracked per user. Tracking that authorizations are specified does not make much sense unless it is checked per user. Breaking each objective up in this manner appears to allows one to say authorizations have been specified so therefore it is complete -- when it should be verified that authorizations have been specified for each specific user. Aligns closer to requirement as written -171	delete: A.03.01.01.c [1,2,3] add: A.03.01.01.c Each user has system authorizations, group and role memberships, and access authorizations defined.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
10	Dana Mason/DoD CIO/CS		7	455	Authorization is co-dependent. Valid access authorization and intended system usage must be true before access is granted. Tracking them separately could lead to access being granted when not warranted. Aligns closer to requirement as written in -171	delete A.03.01.01.d [1,2] change to: A.03.01.01.d access to the system is authorized based on having valid access authorization and valid intended system usage.
11	Dana Mason/DoD CIO/CS		11	584	This amounts to circular logic. "Privileged accounts are restricted to those that have Privileged accounts"	A.03.01.06.ODP[01]: personnel or roles to which privileged activities are required to be restricted are defined.
12	Dana Mason/DoD CIO/CS	Editorial	13	671	Since there are only two options listed it really should be "one or both" instead of "one or more". Yes I know it says this in 800-171 3.1.10 but it should be fixed there too.	change to:]: one or both of the parameter values
13	Dana Mason/DoD CIO/CS	Editorial	19	902	Social mining is not defined in the NIST glossary. Recommend adding a definition.	add definition of social mining to the NIST glossary or delete references to social mining
14	Dana Mason/DoD CIO/CS	Technical	23	1032	3.3.4b sub-category is expanded and uses language not included in FDP. FDP ends "b" with "Take the following additional actions [ODP]" while Ar3 adds "in the event if an audit logging process failure" to the sub-category	Add "in the event if an audit logging process failure" to the end of 3.3.4b. This iteration of the requirement is better than the FDP version.
15	Dana Mason/DoD CIO/CS	Technical	23	1044	Test for 3.3.4 only mentions mechanisms for system response to audit processing failures while this section is referring to organizational personnel response to audit processing failure.	Add "mechanisms for implementing policies and procedures for personnel response to audit processing failures."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
16	Dana Mason/DoD CIO/CS	Editorial	24	1074	The requirement is referred to as A.03.03.05.a instead of A.03.03.06.a	Change A.03.03.05.a to A.03.03.06.a
17	Dana Mason/DoD CIO/CS	Editorial	24	1077	The requirement is referred to as A.03.03.05.b instead of A.03.03.06.b	Change A.03.03.05.b to A.03.03.06.b
18	Dana Mason/DoD CIO/CS	General	25	1098	The requirement is missing the action word "Record" that was used in the -171 FDP in the assessment objective.	Change A.03.03.07.b to "time stamps **recorded** for audit records meet [ODP]"
19	Dana Mason/DoD CIO/CS	Editorial	25	1100	The naming mechanism is not consistent with what was previously used. The sub-category of 3.3.7b is not split into the three different sub categories, but splits the main 3.3.7b and its sub-categories (3.3.7b1-3) into only two categories.	Break out the b requirement to be consistent with the rest of the document. A.03.03.07.b[01] to "time stamps recorded for audit records use Coordinated Universal Time (UTC) A.03.03.07.b[02] to "time stamps recorded for audit records have a fixed local time offset from UTC A.03.03.07.b[03] to "time stamps recorded for audit records include the local time offset as part of the time stamp are recorded.
20	Dana Mason/DoD CIO/CS	Editorial	27	1172	The assessment objective in 800-171R3 fpd has a single ODP establish, document, and implement organization defined configuration settings (that are most restrictive and consistent with operational requirements), but in 800-171A ipd this is spilt into separate (2) ODPs. Need consistency across documents.	Mirror 800-171R3 fpd and list one ODP that reads "Establish, document, and implement the following configuration settings for the system that 790 reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings]."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
21	Dana Mason/DoD CIO/CS	Editorial	30	1281	The assessment objective in 800-171R3 fpd has a single ODP to prohibit or restrict use of organization defined functions, ports, protocols, connections, and services, but in 800-171AR3 ipd this is spilt into separate (10) ODPs. Need consistency across documents.	Mirror 800-171R3 fpd and list one ODP that reads "Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services]."
22	Dana Mason/DoD CIO/CS	Editorial	37	1539	In 3.5.5, there should only be one ODP: a time period for preventing the reuse of identifiers.	Delete ODP[1] and rename ODP[2] to ODP[1]; remove the ODP from A.03.05.05.a; fix the ODP reference in A.03.05.05.c
23	Dana Mason/DoD CIO/CS	Technical	44	1784	3.7.4 Examine should include equipment labeling as 3.07.04d specifies equipment containing CUI.	add within Examine "labeling for maintenance tools that contain CUI"
24	Dana Mason/DoD CIO/CS	Technical	44	1808	3.7.5 Implementing MFA and replay resistance should be separate objectives to align with structure of other sub-requirements that have multiple requirements	Break A.03.07.05b into A.03.07.05b[01] and [02]
25	Dana Mason/DoD CIO/CS	Technical	45	1839	3.7.6 Assessment methods and objects does not include documentation to indicate the "technical competence" of the organizational personnel observing the maintenance.	Examine should include documents that indicate the "technical competence" of the individuals responsible for monitoring maintenance activities. Suggestions include position descriptions or KSA descriptions.
26	Dana Mason/DoD CIO/CS	Technical	48	1945	A.03.08.05.c. Assessment objective requires cryptographic protections during transport but the requirement was deleted from 800-171r3 FPD	Keep the AO and add the cryptographic requirement to 800-171r3. Alternatively, delete the AO if the requirement is dropped from 800-171r3
27	Dana Mason/DoD CIO/CS	Editorial	50	2021	Add rescreening to statement to explicitly show that this isn't a one and done activity	Change to "procedures for personnel screening and rescreening"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
28	Dana Mason/DoD CIO/CS	Technical	51	2027	Need to cover rescreening too	Change to "processes for personnel screening and rescreening"
29	Dana Mason/DoD CIO/CS	Editorial	51	2049	The ODPs are swapped from how they are presented in 171. Transfer or reassignment actions come first followed by time period.	Change A.03.09.02.ODP[03]: transfer or reassignment actions> to ODP 2 and <A.03.09.02.ODP[02]: time 2049 period>: to ODP 3
30	Dana Mason/DoD CIO/CS	Technical	51	2063	Since this talks about system and organizational property, human resources and supervisors should be in the list since they typically play a role in termination activities.	Add human resource personnel; supervisors
31	Dana Mason/DoD CIO/CS	Editorial	55	2191	It would make more sense to use parallel construction in these two requirements statements.	add to line 2192: "to prevent unauthorized individuals from obtaining access to CUI."
32	Dana Mason/DoD CIO/CS	Editorial	57	2251	"Within" is was not included in the requirement that helps describe what the time period in which remediation is required. "Within" that was used in the FDP gives better understanding to the requirement and ODP.	Change to "system vulnerabilities are remediated within:"
33	Dana Mason/DoD CIO/CS	Technical	57	2268	Test' vulnerability scanning, analysis, and remediation, but fails to mention the process for vulnerability monitoring.	Add vulnerability monitoring to Test. Change to "processes for vulnerability scanning, analysis, monitoring, and remediation; mechanisms for supporting and/or implementing vulnerability scanning, analysis, monitoring, and remediation."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
34	Dana Mason/DoD CIO/CS	Editorial	67 81 pdf	2619	The assessment objective in 800-171R3 fpd has a single ODP for both software and firmware, but in 800-171A ipd this is spilt into separate ODPs, one for software and one for firmware. ODP consistency among documents is important	Update 171 ODPs to match 171a assuming different parameters are allowed for firmware and software
35	Dana Mason/DoD CIO/CS	General	70 84 pdf	2738	System or network administrators and personnel with information security responsibilities were removed from the 'Interview' assessment method. They may have relevant knowledge concerning system monitoring	Consider adding "System or network administrators and personnel with information security responsibilities" back into the Interview assessment method
36	Dana Mason/DoD CIO/CS	Editorial	72	2788	3.15.1 Here as in other places, NIST is inconsistent as to what it breaks up into separate sub-objectives. In this case develop and document are sufficiently close that it doesn't make sense to separate them out. One might also argue in that case that there's no point in writing "develop" as you can't document something that isn't developed.	Minor quibble. Remove "develop and"
37	Dana Mason/DoD CIO/CS	Editorial	76	2959	Research and development were combined in 171A but defined as separate items in 171	Separate into two statements. MODIFIED: A.03.17.01.a[02]: the SCRM plan addresses risks associated with the research of the system, system components, or system services. NEW: A.03.17.01.a[03]: the SCRM plan addresses risks associated with the development of the system, system components, or system services.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
38	Dana Mason/DoD CIO/CS	Editorial	76	2971	Operations and maintenance were combined in 171A but defined as separate items in 171	Separate into two statements. MODIFIED: A.03.17.01.a[08]: the SCRM plan addresses risks associated with the operations of the system, system components, or system services. NEW: A.03.17.01.a[09]: the SCRM plan addresses risks associated with the maintenance of the system, system components, or system services.
39	Dana Mason/DoD CIO/CS	Editorial	77	2987	List of documents under examine do not address all of the objectives. Add documents to cover research, design, manufacturing, delivery, operations, maintenance and disposal. Also, 171 discusses monitoring performance against the plans and monitoring SCRM controls. Organizations should have documentation that reflects these activities.	Add SCRM performance reports; SCRM controls monitoring records Revise "system life cycle documentation" (line 2986) to "system life cycle documentation including manufacturing, delivery, operations, maintenance and disposal"
40	Dana Mason/DoD CIO/CS	Technical	77	3011	The objectives talk about the identification of supply chain risks. There should be documentation for the identified risks	Add "risk register with identified supply chain risks"
41	Dana Mason/DoD CIO/CS	Technical	77	3016	The objectives talk about the mitigation of supply chain risks. There should be mitigation plans for the identified risks	Add "risk mitigation plans for supply chain risks"
42	Dana Mason/DoD CIO/CS	Technical	78	3022	Missing the identification, protection, and mitigation of risks	In both statements add to the end of the statement, "to manage supply chain risks"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
43	Dana Mason/DoD CIO/CS	Technical	78	3046	171 describes shipping and handling procedures, configuration management tools, techniques, and measures to maintain provenance and are not addressed in 171A	Add "shipping and handling procedures; configuration management documentation and records"
44	Dana Mason/DoD CIO/CS	Technical	78	3048	Objective A.03.17.03.b focuses on the enforcement of the requirements. However, this is not addressed.	Add "personnel ensuring security requirements are enforced"
45	Dana Mason/DoD CIO/CS	Technical	78	3052	Enforcement of requirements is not addressed.	Add "processes for ensuring security requirements are enforced"
46	Dana Mason/DoD CIO/CS	General	All	All	The handling of compound requirements is inconsistent and can cause a lot of confusion.	Choose a consistent mechanism for handling compound requirements in 800-171Ar3
47	Dana Mason/DoD CIO/CS	General	All	All	Overall formatting is difficult to read and understand--lines and numbers tend to merge together.	Employ the table format used in 171A R2 for 171A R3. A version of 171A R3 that is more "machine readable" also could be published as a secondary source.