From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Cc:	[redacted]
Subject:	[800-171 Comments] Combined AIA & NDIA Comments to SP 800-171 Rev. 3 (Draft)
Date:	Friday, July 14, 2023 5:12:29 PM
Attachments:	AIA-NDIA Comments to NIST SP 800-171r3 ipd.7-14-23.pdf
Importance:	High

Dear NIST:

Please find attached a file containing AIA's and NDIA's combined comments to the SP 800-171 Rev. 3 (Draft).

Please let me know if you have any questions.

V/R

- Jason

Jason Timm | *Director, Defense Policy & Integration*
AIA | [redacted]
aia-aerospace.org

AIA AEROSPACE INDUSTRIES ASSOCIATION NDIA

July 14, 2023

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

RE: Request for Comments NIST Special Publication 800-171 Revision 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Dear NIST:

On behalf of the Aerospace Industries Association of America (AIA) and the National Defense Industrial Association (NDIA), we are pleased to offer comments to the draft NIST Special Publication 800-171 Revision 3.

We are concerned that the 800-171 Rev 3 would represent a step function increase in cost, and impair users' efficiency, without a relevant reduction in risk. We strongly encourage NIST to consider adding additional control scope to the standard. Clarification of existing 800-171 controls and control scope, while using 800-172 for any control additions/enhancements, would help us to better protect Controlled Unclassified Information (CUI). Because many of our members conduct business and operate internationally, we also recommend that NIST consider more closely aligning U.S. and international standards and best practices for any added requirements. The requirements should be achievable by all US Government contractors that store/process CUI on their IT systems. Again, simply adding controls/scope to the 800-171 reduces the likelihood this will be achieved.

Additionally, small businesses would benefit greatly from a defined 'high standard' or 'high water mark' that, if met, would suffice for all Federal agencies and departments. The lack of such clarity, and the dependence on organization-defined parameters (ODP), is problematic and exceptionally prohibitive for small businesses who wish to do business with more than one Federal entity. The persistent fact that CUI is not clearly defined for the Federal space – and that each Federal entity can define CUI differently – is especially onerous for small businesses.

We are committed to initiatives that secure information from cyber threats and we continually work to encourage collaboration between industry and government to improve innovation, agility, and flexibility across all businesses and government entities supporting national and international missions.

Thank you for the opportunity to provide these comments and concerns. Please direct any questions you may have to Jason Timm, AIA's Director for Defense Policy & Integration, at [redacted] or by phone at [redacted]

Sincerely,

Jennifer M. Stewart

John Luddy
Vice President, National Security Policy
Aerospace Industries Association

Jennifer Stewart
Executive Vice President, Strategy & Policy
National Defense Industrial Association

Enclosures:
1. Comment Overview of NIST SP 800-171r3-ipd
2. Comments Matrix to NIST SP 800-171r3-ipd

ENCLOSURE 1

Comment Overview of DRAFT NIST SP 800-171r3

Summary Feedback

The DRAFT NIST 800-171r3 appears to migrate away from and not consider other international standards and best practices and is primarily a derivative of the 800-53 which complicates global enterprise approaches to secure IT systems at scale.

We recommend including international frameworks and best practices as part of control updates and mapping to popular internationally recognized standards and best practices (ISO27000, AUS Essential 8, UK Cyber Essentials Plus).

Organization-Defined Parameters

These need to be consistent across all agencies. A "high water mark – not to exceed" setting should be established in an appendix. Non-federal IT system operators can then choose to hit the high-water mark to meet requirements of all agencies or shoot for a lower set of requirements that is federal agency/organization specific (example: a non-profit that works with only one agency). Recommended approach would have non-federal IT system owners set the ODPs and review during assessment/audit/certification activities with federal customers/partners/etc.

Requirements

Whitelisting requirements in 3.4.8 will have a significant cost impact for medium to large non-federal IT system owners that store/process CUI. There is a significant level of effort to initially deploy and configure whitelisting software as well as continuing operations costs to support the solution. It generally makes the organization 3-5% less efficient across all knowledge workers. This requirement should be part of 800-172, not a baseline requirement for all 13,000 cleared DoD contractors that store/process CUI on their IT systems.

Organization-Defined Parameters

> *For some requirements, organization-defined parameters (ODP) are included. These ODPs provide additional flexibility by allowing federal organizations to specify values for the designated parameters, as needed. Flexibility is achieved using assignment and selection operations. The assignment and selection operations provide the capability to customize the requirements based on organizational protection needs. Determination of organization-defined parameter values can be guided and informed by laws, Executive Orders, directives, regulations, policies, standards, guidance, or mission and business needs. Once specified, the values for the organization-defined parameters become part of the requirement.*

This approach risks creating various requirements between federal agencies which will result in higher operating costs for non-federal IT system operators. Non-federal system operators that support multiple federal organizations/missions will be required to implement different settings and possibly technologies to meet varying ODPs across their enterprise. An example of where this might require deviating technical solutions would be around encryption requirements to protect CUI. Solutions to this issue would include allowing the non-federal IT system owner to select the ODPs. The effectiveness of those settings could be reviewed and accepted or rejected during audit/assessment activities for compliance with requirements. Another approach would be to set a not to exceed high water mark and non-federal system operators could choose to configure/design to that high specification to cover all possible CUI related work conducted on their IT systems.

131 g. Disable accounts of individuals within [Assignment: organization-defined time period] of
132 discovery of [Assignment: organization-defined significant risks].

Organization-defined significant risks cannot be vague parameters. This type of requirement can add significant operational complexity for organizations that serve multiple federal organizations and could be subject to a varying list of "organization-defined significant risks" for each one.

133 h. Notify [Assignment: organization-defined personnel or roles] within [Assignment:
134 organization-defined time period]:

Are the "organization-defined personnel or roles" meant to be non-federal organization persons operating their IT systems and business processes or is the intent to notify the federal entity responsible for the related CUI? This requirement could enable federal entities the ability to force non-federal organizations to operate a certain way. This requirement could also come in conflict with itself if federal entities stipulate different organization-defined personnel or roles.

232 b. Authorize access for [Assignment: organization-defined individuals or roles] to [Assignment:
233 organization-defined security functions and security-relevant information].
234 c. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment:
235 organization-defined roles or classes of users] to validate the need for such privileges.
252 a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or
253 roles].
254 b. Require that users of system accounts (or roles) with access to [Assignment: organization
255 defined security functions or security-relevant information] use non-privileged accounts or
256 roles when accessing non-security functions.

These requirements, as written, are additional examples of ODPs creating the potential to explicitly state how a non-federal entity conducts business operating their IT systems.

<u>Requirement Specific Feedback</u>

895 3.4.8. Authorized Software – Allow by Exception
896 a. Identify software programs authorized to execute on the system.
897 b. Implement a deny-all, allow-by-exception policy to allow the execution of authorized software
898 programs on the system.
899 c. Review and update the list of authorized software programs [Assignment: organization
900 defined frequency].

This "whitelisting" requirement for software will have a significant cost impact on medium to large non-federal system operators. Recommend making this a NIST 800-172 requirement, not a baseline requirement for protecting CUI.

2005 System and Information Integrity
2006 3.14.1. Flaw Remediation
2007 a. Identify, report, and correct system flaws.
2008 b. Test software and firmware updates related to flaw remediation for effectiveness and
2009 potential side effects before installation

This requirement will result in a net-negative security for many businesses, including small businesses. Many businesses typically configure their systems to accept and install vendor security updates automatically. Automatic patching results in much quicker flaw remediation, which is very important.

The vast majority of business IT departments are less qualified than their trusted vendors to test and filter patches. This control means companies cannot accept push updates from their vendor, but instead must configure their systems to reject patches until the internal IT department manually packages them and pushes them to a test group, then to production.

For most businesses, this

1) greatly increases latency before patching from ~12 hours to 15-30 days,
2) requires adding extra infrastructure to manage the process, such as a non-FedRAMP patch management solution, which increases the attack surface of the information system,
3) increases IT burden by at about 10 hours per week for a business with less than 10 users.

For a typical business implementing this requirement, the proposed benefit (testing patches to determine if they are malicious) is negligible. Unless an explicit control is added to this effect, business IT departments will not perform network analysis or behavior analysis during testing to identify malicious behavior. They will simply slow down their patching process dramatically.

This change would result in a net negative for security for most businesses. The risk of a trusted vendor being compromised and pushing a bad patch is less than the unintended consequence of increasing latency in flaw remediation and increasing attack surface.

Recommend eliminating b. This is an operational risk decision that should be left up to IT operations teams to determine what level of testing is required prior to patch deployment and coordinated to meet any timeline specified in line 2010 c.

2165 3.15.3. Rules of Behavior

What rules of behavior should be clearly defined…i.e., what assessment evidence is required to comply with this requirement. For example, is a system owner required to show they have a record of every user that is granted access to CUI acknowledges they must follow the rules of behavior? Are the rules required to be explicitly defined beyond anything in 800-171r3? Which 800-171r3 controls would be required for users to acknowledge or can an organization simply state users with access to CUI must follow all organizational policies required to protect CUI including all that require 800-171r3 compliance?

2277 3.17.2. Acquisition Strategies, Tools, and Methods
2278 Develop and implement acquisition strategies, contract tools, and procurement methods to
2279 protect against, identify, and mitigate supply chain risks.

This requirement should be removed. Supply chain risk as it pertains to contractor IT systems that could be used for software development that is CUI should be addressed in a separate supply chain set of requirements associated with US Gov or DoD/agency specific requirements. It is unfeasible to have the requirement in 800-171r3 given applicability across all contractor IT systems for US Gov't and current vagueness of requirement with no visibility on assessment criteria for compliance.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	AIA / NDIA	General	NIST SP 800-171r3 ipd	1	22	This states that the intent of the documents is to "provide federal agencies with recommended security requirements". The massive use of ODP throughout the document negates this statement. The document provides an outline, but no real requirements since the requirements are left to the various ODPs to define	Rewite the document to agree with the purpose by removing the ODP and providing actual requirements
2	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	2	30	NIST has consistently said in both writing and via public comments they are not a regulatory entity which does not enforce nor is required to be assessed to the standards they are issuing. However, this creates significant problems within industry where expectations are assumed that all Requirements in 800-171 will be enforced and assessed via the use of the 252.204-7012 clause. This results in a regulated / lawful requirement for non-federal organizations to comply. 30: 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. The requirements are intended for use by federal agencies in contractual vehicles or other agreements that are established between those agencies and nonfederal organizations	Relook at the overall publication to make sure there is consistency across requirements especially related to the assumption that "system" means only those in scope per the previous definition of scope. As a result of the broad use of the NIST series of standards by Federal Agencies and other domestic and foreign entities in contractual obligations it is recommended that more transparency be afforded to the creation/update of the standards and formalize the adjudication of comments. It is also recommended that a group of subject matter experts from both industry and government (non-NIST) be empaneled to discuss and come to concensus on changes to the Standards that affect 100's of thousands of non-federal organizations both domestically and internationally.
3	AIA / NDIA	General	NIST SP 800-171r3 ipd	3	59	Generally true however all contracts need to be more explicit on the exact version referenced. The primary issue is that some DoD entities are expecting additional controls that are above and beyond what is required by regulation.	
4	AIA / NDIA	General	NIST SP 800-171r3 ipd	3	61	This assumption is false as compiance allows for deficiencies/deviations to be listed on a POAM.	
5	AIA / NDIA	General	NIST SP 800-171r3 ipd	3	64	64 Security Requirement Development Methodology 65 Starting with the NIST SP 800-53 security controls in the NIST SP 800-53B [13] moderate 66 control baseline, which satisfy the minimum-security requirements in FIPS 200, the controls are 67 tailored to eliminate selected controls or parts of controls that are: 68 • Primarily the responsibility of the Federal Government 69 • Not directly related to protecting the confidentiality of CUI 70 • Expected to be implemented by nonfederal organizations without specification by the 71 Federal Government **Comment:** As written this assumes, as with previous versions of NIST 800-171 that the Federal Agencies contracting with the non-federal organizations would be allowed to implement security controls relating to each requirement based on their unique information systems technology and Enterprise security control plane.	While ODPs may remain the shift should occur whereby the ODP is defined by the non-federal organizations vs. the federal agencies. Due to the potential for extreme variations related to those ODPs without the benefit or knowledge of how a non-federal organizations network is configured and what technology is being used to support the protection of CUI, intellectual property, information of others, etc., it could cause major disruptions and conflicts between federal agencies.
6	AIA / NDIA	General	NIST SP 800-171r3 ipd	4	79	ODPs are identified as defined by "federal agencies" which are referred to and defined in the document as an "executive department:" An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an independent	NIST needs to take some accountability in the ecosystem in which their guidelines and standards are utilized to help with understanding cost to implement and maintain as well as repercussions of the standards and how they may be tailored to non-Federal agencies.
7	AIA / NDIA	General	NIST SP 800-171r3 ipd	4	80		Change federal to nonfederal as these controls are impossible to implement if every contract can specify a different set of ODPs. I believe the intent was to allow more flexibility within the contractor's environment.
8	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	5	117	Re-word for clarity. It can be difficult to define and document "prohibited" accounts. It is proving a negative. ODPs for inactive accounts as prescribed in DISA STIGS differ (from 72 hours to 30 days) among individual, shared, group, temporary, system, guest, anonymous, emergency, developer, and service accounts.	Why do we need to list the prohibited account types when we can list the approved account types? Recommend rewriting line 117 a. to "Define and document the types of system accounts allowed."
9	AIA / NDIA		NIST SP 800-171r3 ipd	5	118	Managing and meeting the requirements as part of the ODP will be difficult specially for an organization that has multiple contracts with various federal and DoD agencies	Remove the ODP for this control requirement
10	AIA / NDIA		NIST SP 800-171r3 ipd	5	125	3.1.1f-Managing and meeting the requirements as part of the ODP will be difficult specially for an organization that has multiple contracts with various federal and DoD agencies	Remove the ODP for this control requirement
11	AIA / NDIA		NIST SP 800-171r3 ipd	5	131	3.1.1.g-Managing and meeting the requirements as part of the ODP will be difficult specially for an organization that has multiple contracts with various federal and DoD agencies	Remove the ODP for this control requirement
12	AIA / NDIA		NIST SP 800-171r3 ipd	5	133	3.1.1.h-Managing and meeting the requirements as part of the ODP will be difficult specially for an organization that has multiple contracts with various federal and DoD agencies	Remove the ODP for this control requirement

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
13	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	7	229	"Processes" is confusing for as it is used throughout the document as applications/services but also workflows and should be better differentiated such as putting "system processes".	Change "processes" to "system processes" to better delineate from workflow processes as part of procedures to reduce confusion and increase clarity. Please also define and differentiate these terms in the glossary ... process, system process, application, system service.
14	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	8	234	Organization Defined Frequency is not defined in the glossary	Add Organization Defined Frequency to the glossary. Frequency: "the number of times something happens within a particular period, or the fact of something happening often or a large number or times".
15	AIA / NDIA		NIST SP 800-171r3 ipd	8	252	3.1.6-Priviledge accounts should not be governed by the ODP requirements	Remove the ODP for this control requirement
16	AIA / NDIA		NIST SP 800-171r3 ipd	8	254	3.1.6-System accounts and access should not be governed by ODP requirements	Remove the ODP for this control requirement
17	AIA / NDIA		NIST SP 800-171r3 ipd	9	293	3.1.8-How does limiting the unvalid logon attempts and defined period being ODP help with CUI protection	Remove the ODP for this control requirement
18	AIA / NDIA		NIST SP 800-171r3 ipd	10	320	3.1.9-Device lock parameters should not be an ODP	Remove the ODP for this control requirement
19	AIA / NDIA		NIST SP 800-171r3 ipd	10	341	3.1.11-Terminate user session should not be an ODP	Remove the ODP for this control requirement
20	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	10	347	Processes is confusing for as it is used throughout the document as applications/services but also workflows and should be better differentiated such as putting "system processes".	Change "processes" to "system processes" to better delineate from workflow processes as part of procedures to reduce confusion and increase clarity. Please also define and differentiate these terms in the glossary ... process, system process, application
21	AIA / NDIA	General	NIST SP 800-171r3 ipd	11	358	Documenting all usage restriction configurations and connection types would require significant resource allocation from the DIB to support	a. Establish, authorize, and document usage connections and configurations permitted for remote access.
22	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	11	364	Is this crytography required to follow the other crytography requirements? If so, then the discussion should highlight the requirement. Otherwise, identify what is strong cryptography.	Add information relating the cryptography requirement to the ODP cryptography requirement and/or how to validate strong cryptography.
23	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	12	397	Is this crytography required to follow the other crytography/encryption requirements? If so, then the discussion should highlight the requirement. Otherwise, identify what is strong cryptography/encryption.	Add information relating the cryptography/encryption requirement to the ODP cryptography requirement and/or how to validate strong cryptography/encryption.
24	AIA / NDIA	General	NIST SP 800-171r3 ipd	12	398	Disabling wireless on all systems with the determination of intended use would entail significant resources allocation	d. When practical, Disable, when not intended for use, wireless networking capabilities embedded within the system prior to issuance and deployment.
25	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	12	417	3.1.19 was incorporated into 3.1.18 but Mobile Computing Platform is not anywhere in the description or discussion. Is this crytography required to follow the other crytography requirements? If so, then the discussion should highlight the requirement. Otherwise, identify what is strong cryptography. Full device encryption may be difficult with BYOD. The container is encrypted and not accessible from the rest of the phone, but it's not the full device. That's just how InTune works, which is a very common thing for a lot of companies. Disallowing BYOD can hurt SMBs who are not able to provide company owned mobile devices to their employees.	Should add discussion relating to Mobile Computing Platforms or change Mobile Devices to Mobile Computing Platforms for broader usage. Add information relating the cryptography requirement to the ODP cryptography requirement and/or how to validate strong cryptography. Add guidance for BYOD to 3.1.18 Direct to follow: Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2.
26	AIA / NDIA	General	NIST SP 800-171r3 ipd	13	452	Unclear the difference between 3.1.20 and the first part of 3.1.21	Combine them into one requirement and keep the portable storage requirement as its own requirement
27	AIA / NDIA		NIST SP 800-171r3 ipd	13	453	3.1.20-How is this control going to affect the SaaS offering which now needs to meet the ODP requirements which might change over time	Need to provide more details on how to implement this control for cloud based solutions. Also remove the ODP for this control
28	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	13	455	No definition for Trust Relationships.	Need to define trust relationships and put into Glossary.
29	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	13	458	This doesn't make any sense. Does this mean the access of the external system from other external systems? Shouldn't this be both internal and external connections?	Rewrite to better clarify the expectations and if this is connection to/from external systems using approved internal and external systems.
30	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	13	460	Why is b part of 3.1.20 as it seems more in line with 3.1.21 ?	Move b to 3.1.21 for consistency
31	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	13	461	Why is cloud and services are not part of discussion?	Add Cloud Services and other XaaS as those will be some of the first items that people will think about when talking external systems.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
32	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	14	481	Why isn't there an ODP on how often to verify controls such as annually? This is a little confusing and doesn't clarify what is meant by "organization security policy". Does this mean that the external system must align their security policies with the organization they are connecting to, or does it mean that the organization they are connecting to should verify that the external organization is following the security policies that they have been set for their organization?	Add ODP that requires re-assessment to verify security controls such as annually Provide a definition for organization security policy and clarification regarding who, what, when, and where verification should come from.
33	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	14	483	What does retained supposed to mean? Does this mean keep the documentation? Does this mean the connection is kept up?	Reword and better define what is to be retained
34	AIA / NDIA	General	NIST SP 800-171r3 ipd	14	485	External system access to portable storage would be tied to the external system(SaaS) SOW/Contract/MSA. Portable storage devices are already accounted for in 3.8.7	Remove b.
35	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	14	488	The discussion of using org-controlled portable devices on external systems is very lacking.	Add additional discussion regarding org-controlled portable devices and why the limitation and how this is different than Media Protection requirements.
36	AIA / NDIA	General	NIST SP 800-171r3 ipd	14	496	Done through training and would take considerable resources develop a technical implementation	Use of policy and training would be acceptable solution when a technical solution is not available.
37	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	14	500	Why isn't there an additional assessment objective to review content prior to publishing on public domain. Why was Control removed from the requirement as this makes the control weaker?	Add additional objective to Control and Review content for CUI prior to posting on publicly accessible system.
38	AIA / NDIA	General	NIST SP 800-171r3 ipd	14	501	All CUI is dependent on government identified data - Program specific. Scope is not realistic	a. Train authorized individuals to ensure that publicly accessible information does not contain CUI. If discovered report through proper security channels to address accordingly. REMOVE b. Review the content on publicly accessible systems for CUI [Assignment: organization-defined frequency] and remove such information, if discovered.
39	AIA / NDIA		NIST SP 800-171r3 ipd	14	503	3.1.22-Provide guidance on what process and guidance would be required for CUI publicly accessible content	Detailed guidance on how the ODP for this control would be required
40	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	15	512	Increased cost required to implement additional control Inactivity logout requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Because of this, how would a company be able to track an employee's "expected inactivity" and provide proof that people are actually logging off prior to leaving their workstation? Forceably logging off an account after the defined period of inactivity could adversely impact applications and has the potential for loss of data. In addition, some mission or business critical industrial control systems, software, or hardware require a user to be logged in for proper operation and automatically logging them off could leave some connections orphaned which will eventually result in performance issues. This could also have a huge ripple effect on factories and could impact some production lines and systems supporting business infrastructure (i.e., HVAC systems) that cannot be logged off without impacting the operation of the system.	Recommend allowing for exceptions or other risk mitigating controls for mission and business critical systems, software, and/or hardware, Industrial control systems, and systems supporting business infrastructure.
41	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	15	524		Make consistent and define all terms
42	AIA / NDIA		NIST SP 800-171r3 ipd	15	524	3.2.1-Training and Awareness should be a generic requirement rather be defined by ODPs as it will create more problems then solving them Why doesn't a. have awareness in it when b. states training and awareness? Literacy training adds confusion. Why doesn't a. have awareness in it when b. states training and awareness? Why does b. have awareness but a. does not?	Remove the ODP for this control requirement Make consistent and define all terms Define Literacy Training Make consistent and define all terms Add awareness to a.

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
43	AIA / NDIA	General	NIST SP 800-171r3 ipd	15	526	3.2.1 and 3.2.2 Leaving training frequency up to an ODP outside the contractor organization is a significant financial risk to the contractors. Traing of a workforce is a significant and costly undertaking considering the time each user spends in training is time they cannot be productive on the work tasks.	Either state the required frequency or leave it to the contractor
44	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	16	552	Why doesn't this have Literacy as part of the training discussion?	Make consistent and define all terms
45	AIA / NDIA		NIST SP 800-171r3 ipd	16	553	3.2.2-Similar to above the role based training should be generic and not an ODP	Remove the ODP for this control requirement
46	AIA / NDIA	General	NIST SP 800-171r3 ipd	16	556	2. is redudant if training is provided before authorized access, regardless of the system.	Remove
47	AIA / NDIA	General	NIST SP 800-171r3 ipd	16	557	Frequency for specifc role based training would require additional resouces ($) to orgainzations that currently deliver a more informal training manner	Role-Based Training a. Provide role-based security training to organizational personnel: 1. Before authorizing access to the system, CUI, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes. REMOVE b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
48	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	16	577	Why does 3.2.3 exist when Advanced Literacy training is discussed in 3.2.1?	Combine, remove, and/or provide additional clarity on the differences without repeating and possibly add an ODP for how frequently the training should be taken.
49	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	16	592	Adding social engineering and social mining to the insider threat control is good. Before this, no mention of phishing.	No Change
50	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	17	597	Social engineering and social mining defined in previous sentence, data mining not defined.	Replace "data mining" with "social mining" on line 597.
51	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	17	603	Dictating all the possible event types by an organziation can be very cumbersome with different intepretations between organizations. 3.3.1-Allowing external ODPs to redefine logging requirements can be extremely disruptive to the organizational operation and security. Log storage systems are designed based on defined requirements and the log analysis systems are programmed based on the logs determined to be presented to it. To allow ODPs to arbitrarily change predefined procedures and processes can be quite expensive for the contractor and could negatively impact the contractor's operation	Recommend removing the ODP from part a. Also, change "remains necessary and sufficient" to "remains relevant and sufficient."
52	AIA / NDIA		NIST SP 800-171r3 ipd	17	604	3.3.1-If event logging is to be changed per the ODP requirements it could have huge cost implications so ODP should be taken out for this control	Remove the ODP for this control requirement
53	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	17	625	The wording is confusing	Change "necessary" to "relevant"
54	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	18	643	What happens if the software or hardware being used cannot provide or generate audit records? This requirement is written like the contractor creates the software rather than using/configuring to generate logs and records.	Rewrite to "configure for audit record generation and identify what record types can and cannot be generated on the system"
55	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	18	664	3.3.4.b-"Take the following additional actions: [ODP defined]." This is a wide open invitation for the ODP to insert any action regardless of the complexity of the action or the cost to the contractor	Remove this statement
56	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	19	680	What defines inappropriate or unusual activity?	Add an ODP for inappropriate and unusual activity.
57	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	19	683	3.3.5.b-"Report findings to [ODP}". This leaves the reporting wide open and could require reporting outside of the contractor organization which may be completely out of line as the contractor systems generally include data no related to any one specific contract	Remove this statement
58	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	19	705	What is definition of on-demand and why does it have to be on-demand?	Remove "on-demand".
59	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	20	722	Why was an "authoritative time source" removed from the requirement for ease of log evaluation. Otherwise, the point of log reviews is lost with inconsistent time sources.	Add "authorative time source" back into the requirement.
60	AIA / NDIA		NIST SP 800-171r3 ipd	20	724	3.3.7-Since the time stamps have already been defined to follow UTC or fixed local time why this control should be defined by ODP. Also it could create conflicts on which guidance to follow	Remove the ODP for this control requirement

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
61	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	21	754	For consistency, why isn't an ODP defined here for the subset of users?	Rewrite and replace "subset of priv users or roles" to ODP with users and roles.
62	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	21	766	Why was the requirement for the organization to maintain a full inventory of devices, software, etc? There is some parts in discussion of 3.4.10 but that requirement is for System Components and not the actual inventory.	Add inventory back in as a requirement
63	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	21	769	3.4.1.b-This allows the ODP to redefine the update frequency of the baseline configuration. Development of a proper baseline is a costly process and to leave it to the whim of and ODP is a significant risk to the contractor	Either state the required frequency or leave it to the contractor
64	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	21	783	Why identified as "most restrictive mode" and what is the point of this statement?	Remove "most restrictive mode" and leave as part of the ODP
65	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	21	783	Why isn't "review" with ODP frequency listed for configuration settings as well as deviations?	Add ODP requiring review for a, b, and c
66	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	21	784	3.4.2.a-This allows the ODP to redefine what a secure configuration is. In addition the statement "OD common secure configuration" makes no sense. If it's a "common" configuration then how can it be ODP defined?	State the configuration requirements or leave them to the contractor.
67	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	22	814	Why is there no requirement or ODP that requires an org to define who could/should approve changes? There could be little or no separation of duties Rewrite a. as an ODP for consistency	Rewrite a. as an ODP for consistency Modify ODP to require org-defined approvers
68	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	23	840	Appreciate and support the criticality of the new requirement for reviewing impact of changes on supply chain partners, who may be less knowledgeable of the details of changing regulatory requirements and how they can meet with those requirements. However, it is not clear if this review applies to both internal and external stakeholders, such as service providers, hardware/software suppliers, vendors, etc.	Please clarify if "stakeholders" is intended to mean internal and external stakeholders. Please include a definition of "supply chain partner" and "stakeholder" (including examples), in this context of reviewing impact of changes.
69	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	23	862	Why isn't this an ODP such as Org-defined capabilities? 3.4.6-Entire control leaves items up to the ODP. How can an ODP that is unfamiliar with the software and systems used by a contractor redefine the ports and protocoles used, the program exexution parameters, or the systme review requirements	Change to ODP for defining missing-essential capabilities or leave this to the contractor
70	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	24	895	By deny all applications from executing, except those you authorize, it can cause a massive burden increase if organizations have been relying blocklist. This is a huge paradigm shift from a NASL to an ASL. Most large companies are struggling to do this across their enterprises	Change this control to match 800-53r5 CM-7(4).
71	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	25	924	3.4.9.b-How can the software installation process be left to an external ODP who has no view of the details of the contractor network?	Leave this to the contractor
72	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	25	940	Why only system components and not a full inventory list? System component is confusing as it seems to be what is in the systems and not the systems themselves.	Add/modify previous requirements to identify the need to have a complete inventory. Change the requirement to be "System and System Component Inventory"
73	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	26	958	Increased resources required to implement additional control Having to document all existing CUI processed within a large organization and it's location is possible, but it will take considerable time to verify the location of any existing CUI currently stored on a contractor network. It may be more feasible to begin tracking document locations as those documents are received instead of trying to locate all CUI currently existing in a company's possession. What is the level of granularity required to meet this requirement? Will simply documenting the information systems that contain CUI be sufficient or will it require an organization to identify the file location within the system?	Recommend that we simply track new CUI from this point forward, based on new contracts after the date that R3 is approved and effective.
74	AIA / NDIA		NIST SP 800-171r3 ipd	26	959	3.4.11-Is this control defining the restriction for data sovereignity and nationality requirement for accessing the CUI data	Provide more guidance on what details are required for this control

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
75	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	26	971	Why isn't there an ODP that defines areas/locations of significant risk? If C3PAO or ODP does not agree with the list the Organizations deems to be “significant risk, who determines what is “high risk”. Who is the “organization”? Destroying laptops and/or removing from circulation for enhanced checks is unaffordable by SMBs. They do not have the resources or knowledge to identify false chips or added chips to devices. Who determines what is an "Organization Defined System"? 1 - Is maintaining a list of authorized software, and denying installation of any other software, sufficient? Or must the software be validated each time before it executes? 2 - Is the intent that an organization can decide that monitoring authorized software at the application level is sufficient? Or, must the organization have a plan that protects "against attacks that bypass application-level authorized software" as the discussion suggests?	Modify/add ODP that defines the areas/locations of significant risk Re-word line 972 a. "The contractor defines countries that are 'high risk areas' and implements controls to limit the amount of CUI and propietary data on the computers or mobile devices prior to travel.". Re-word line 975 b. "The contractor will re-image the laptop prior to being allowed on the network. The mobile device will be re-imaged prior to being allowed on the contractor network." Re-word discussion "The computer and mobile device will be examined by the contractor to ensure any devices have been tampered with during travel." "This can be accomplished by photographing the motherboard of the computer and mobile device, prior to travel and photographing upon return."
76	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	26	972	"Organization Defined System" is not listed in the glossary.	Define "Organization Defined System" in the glossary
77	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	26	972	3.4.12.a and b. These are open blank checks for the ODP and it is unclear what "organization" means in the parts of the requirement outside of the reference to ODP	Leave this to the contractor
78	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	27	993	The use of processes is confusing to many users.	Rewrite as "system processes" to differentiate from "workflow processes"
79	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	27	993	Tense of nouns should be consistent as it says authenticate system user but then says acting on behalf of users.	Change "system user" to "system users" for consistency with the rest of the requirement objectives or change "users" to "user" in all instances.
80	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	27	993	3.5.1.b-Allowing ODPs to redefine the requreiments for re-authentication can be very disruptive to the operations of the contractor	Either state the required frequency or leave it to the contractor
81	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	27	1010	This discusses "before establishing a system or network connection" but the discussion only talks about network connections. What about system connections. How and what is supposed to be used for authenticating system connections such as plugging in a USB or adding a device via external ports as these would both be classified as system connections. If you meant only network connections, then drop the system requirement.	Drop system connection from the requirement if only meaning network connections or provide additional examples and discussion relating to direct system connections and how authentication and identification would occur.
82	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	27	1011	3.5.2-This is really unclear what the ODP is intended to define	Leave this to the contractor
83	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	27	1025	Do we need to do MFA within our boundary? End points can be logged into with single factor.	Specify if a contractor needs to implement MFA for non-privileged accounts within their boundary.
84	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	27	1025	Per this updated requirement and per 3.1.1 discussion, system account types include individual, shared, group, temporary, system, guest, anonymous, emergency, developer, and service. This seems overly broad and unobtainable to require MFA for all of these account types when accessing the system.	This should be scoped down from what is defined as system accounts per 3.1.1 (individual, shared, group, temporary, system, guest, anonymous, emergency, developer, and service). Change back to NIST SP 800-53 IA-3 as the rewording is overly broad and changes the scope of the requirement to be overly broad and hard to meet.
85	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	27	1026	Unclear if Multi-factor authentication is needed for any type of account on the network - privileged/non-privileged user accounts, service accounts, local accounts? 3.5.3 specifies a blanket requirement for MFA to all system accounts, which is technically impossible to implement in a number of conditions, including but not limited to: 1. OS-local administration accounts such as Windows “Administrator” or Linux “Root”. 2. Application-specific service accounts. 3. All user accounts on standalone (non-networked) systems.	Define what a "System Account" is in the control and the glossary. Permit the ability for a Non-Federal Organization to specify by policy the conditions under which single factor authentication is permitted.

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
86	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	28	1049	Why is this limited to specific accounts when system accounts is overly broad per 3.1.1 discussion? Why not have every identifier that could be assigned/created be unique? Why is unique not listed anywhere in this requirement? What "status" means is highlighted in the discussion but by just reading the requirement in d, it is hard to identify what you are looking for and status is contractor, foreign national, etc. does not seem to be a good fit and really should be called something other than status such as identifying specific characteristics based upon the needs, regulations, and requirements of the org. Why are only users, processes, and devices listed as identifiers when other items are listed in the requirements. This should be consistent with requirement verbiage to reduce confusion.	Change "to assign an individual, group, role, service, or device identifier" to "to assign system account, role, or device identifier" for all instances in this requirement. Add "to assign a unique identifier" to the different requirement. B. should be "select and assign a unique identifier …" Change d back to original from NIST SP 800-53 IA-4(4). Add the other types of identifiers as listed in a and b.
87	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	28	1050	3.5.5-ODP authorizations in this control can be very disruptive to the operation of the contractor systems	Leave this to the contractor
88	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	28	1054	What "status" means is highlighted in the discussion but by just reading the requirement in d, it is hard to identify what you are looking for and status is contractor, foreign national, etc. does not seem to be a good fit and really should be called something other than status such as identifying specific characteristics based upon the needs, regulations, and requirements of the org.	Change d back to original from NIST SP 800-53 IA-4(4).
89	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	28	1057	why are only users, processes, and devices listed as identifiers when other items are listed in the requirements. This should be consistent with requirement verbiage to reduce confusion.	Add the other types of identifiers as listed in a and b.
90	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	29	1069	What does "allow user selection" mean? Does it mean allow them to choose them from a list or to create them?	Change "allow user selection of" to "allow user to create"
91	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	29	1069	Does the cryptographically protected channels fall into the crytography requirements in this document? If so, that should be reiterated. b. has some options such as including spaces and all printable characters that could immediately make some instances other than satisfied due to technology limitations and challenges	Reiterate that the cryptographically-protected channels have to meet the cryptography requirements in the requirements. Remove "including spaces and all printable characters" from the requirement
92	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	29	1070	3.5.7(a) gives federal organizations the ability to specify to NFO s a set of password complexity rules. This violates NIST SP 800-63b 5.1.1.1 which says that besides a minimum length, “No other complexity requirements for memorized secrets SHOULD be imposed.”	Withdraw
93	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	29	1072	Not every system still supported and in use can accept long passwords and all printable characters	Leave this to the contractor
94	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	29	1074	Increase in resources required to select/purchase/install password checker Part C may be challenging, depending on which password provider being utilized by the company. This can be challenging for SMBs if they need to purchase a different password management system. Would this be an investment? How does this impact the future implementation of Zero Trust passwordless authentication?	Please explain how this impacts passwordless authentication with Zero Trust Architecture.
95	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	29	1077	e should not have "preferably" in the requirement as that will become mandatory and thus should be in discussion instead on how to meet or best practices.	Remove "preferably" from the requirement
96	AIA / NDIA	General	NIST SP 800-171r3 ipd	30	1116		

* indicate required fields

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
97	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	30	1116	Increased resources required to implement additional control Are these authentication requirements being required for accessing government data and company proprietary information? Does this require authentication to access data, applications, or network components? Will there need to be an additional layer put into place for accessing CUI? Why aren't "shared" accounts not discussed and only "group" or "role" accounts? The change from 800-53 changes the content and context of the requirement and should be modified to remove "content" as that adds confusion. The word "content" also add no value. Does e really mean "change the defaults of the authenticators prior to first use"	Recommend providing more information on where/when authenticators will need to be used. Add "shared" to the types of accounts for consistency with other requirements. Reword d to "Protect authenticator from unauthorized disclosure or modification" Reword to "Change the defaults of authenticators prior to first use."
98	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	30	1122	The change from 800-53 changes the content and context of the requirement and should be modified to remove "content" as that adds confusion. The word "content" also add no value.	Reword d to "Protect authenticator from unauthorized disclosure or modification"
99	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	30	1123	Does e really mean "change the defaults of the authenticators prior to first use"	Reword to "Change the defaults of authenticators prior to first use."
100	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	30	1124	Allowing ODP to define the refresh period or circumstances under which an authenticator refresh is required will be disruptive to the operation of the contractor systems	Leave this to the contractor
101	AIA / NDIA	General	NIST SP 800-171r3 ipd	31	1173	(Including 3.6.2): DFAR 7012 and the NISPOM already define the reporting requirements.	Remove this statement
102	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	31	1174	What evidence will the C3PAO be looking for this control?	Make sure to include evidence types that will satisfy this control in the NIST.SP.800-171Ar2 IPD for 3.6.2
103	AIA / NDIA	General	NIST SP 800-171r3 ipd	32	1194	3.6.3-Incident response testing-Allowing any ODP to redefine the test frequency would be very disruptive to the operation of the contractors systems	Leave this to the contractor
104	AIA / NDIA	General	NIST SP 800-171r3 ipd	32	1206	Increased resources required to implement additional control	
105	AIA / NDIA	General	NIST SP 800-171r3 ipd	32	1210	3.6.4-Allowing each ODP to redefine the incident response training requirements is unnecessary.	Leave this to the contractor
106	AIA / NDIA	General	NIST SP 800-171r3 ipd	33	1237	3.7.4-Maintenance Tools-Item c.3. is unnecessary and can allow any ODP to significantly alter the operational procedures of the KR	Leave this to the contractor
107	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	34	1272	This requirement seems to be overly broad especially with the additional "technical competence" required for supervising maintenance activities. This could result in issues with all of the non-CUI related maintenance activities within an organization. For example, if there needs to be HVAC work performed in an area with CUI, having an HVAC knowledgable person available to escort the technician may be unrealistic and unachievable.	Update the requirement to specify maintenance work on the systems in scope per the scoping guidance (i.e., CUI systems or security for those systems) instead of leaving open ended.
108	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	35	1309	3.8.2-KRs already have processes for managing access to CUI and there are several other controls that already define restrictions. To allow each ODP to define who within the KR org can have access is unnecessary	Leave this to the contractor
109	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	36	1339	3.8.4-Allowing each ODP to redefine the exemption process would be disruptive to the KR operations	Leave this to the contractor
110	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	36	1351	3.8.4 has ODP for controlled areas. Why doesn't 3.8.5 have the same for a. or is there an assumption that it is defined in 3.8.4? However, no part of the discussion identifies the controlled areas as those from 3.8.4. This requirement calls out cryptography but the description does not call out 3.13.11 for approved ODP cryptography and encryption similar to what other discussion provide for other, related requirements	add "as defined in requirement 3.8.4" to the end of a. Add call out to 3.13.11 in the discussion regarding approved cryptography within the discussion to identify that it is related.
111	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	36	1354	3.8.5-There are ocasions when encryption is not practical or possible on media being transported. An option for other security requirements in these cases should be included	Include an option for other security requirements in lieu of encryption
112	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	37	1374	if Prohibit is selected for a., what is the relevance of b? B. should contain some type of verbiage such as "if applicable per a." otherwise, b is N/A which may not be accepted.	Change b. to be consisten to the new wording in a.
113	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	37	1374	Why doesn't b. have the same "Selection: Restrict; Prohibit" as a. since they are interrelated?	Add "Selection: Restrict; Prohibit" to b
114	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	37	1374	Change "portable storage devices" on b to "ODP removable system media" for consistency	Change "portable storage devices" on b to "ODP removable system media" for consistency

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
115	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	37	1374	if Prohibit is selected for a., what is the relevance of b? B. should contain some type of verbiage such as "if applicable per a." otherwise, b is N/A which may not be accepted. Why doesn't b. have the same "Selection: Restrict; Prohibit" as a. since they are interrelated? Change "portable storage devices" on b to "ODP removable system media" for consistency	Change b. to be consistent to the new wording in a. Add "Selection: Restrict; Prohibit" to b Change "portable storage devices" on b to "ODP removable system media" for consistency
116	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	37	1375	3.8.7-Allowing each ODP to define what media can be uses may be disruptive to the KR operations	Leave this to the contractor
117	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	37	1399	This requirement calls out cryptography but the description does not call out 3.13.11 for approved ODP cryptography and encryption similar to what other discussion provide for other, related requirements The discussion identifies that "alternate physical controls" is acceptable but that is not what the requirement states.	Add call out to 3.13.11 in the discussion regarding approved cryptography within the discussion to identify that it is related. Change the requirement to "implement cryptographic mechanisms or alternate controls .." in the requirement to be consistent with the discussion.
118	AIA / NDIA	General	NIST SP 800-171r3 ipd	38	1412	Increased resources required to implement additional control	REMOVE b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].
119	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	38	1414	3.9.1-To allow each ODP to redefine the personnel screening refresh requirements may be quite costly to the KR	Either state the required frequency or leave it to the contractor
120	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	38	1425	Why doesn't b have a ODP time period for reviewing and confirming the need for access? If the assumption is that other requirements provide guidance on ODP time periods for reviews, etc., then the discussion should be updated to reflect that with the appropriate requirement numbers.	Add ODP for b. 1. for time period review. If the assumption is that other requirements provide guidance on ODP time periods for reviews, etc., then the discussion should be updated to reflect that with the appropriate requirement numbers.
121	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	38	1427	3.9.2-System access disablement and action initation are driven by the standing KR systems and processes. To allow each ODP to redefine these time periods may require sigificant changes to the KR systems and processes for each ODP	Either state the required frequency or leave it to the contractor
122	AIA / NDIA	General	NIST SP 800-171r3 ipd	39	1457	Increased resources required to implement additional control	
123	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	39	1457	Is the expectation that external providers would have to follow various customer security policy and procedures? This would mean that we would need to share our internal policies with external companies and that is sharing our intellectual property.	Clarify exactly what type of external provider oversight is needed to meet the requirement
124	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	39	1457	How many Tiers (1, 2, 3) of external personnel employed by subs or suppliers must comply with personnel security requirements?	Define Tier Levels: Tier 1 Suppliers: Direct suppliers Tier 2 Suppliers: Suppliers suppliers or companies that subcontract to direct suppliers Tier 3 Suppliers: Suppliers or subcontractors of tier 2 suppliers
125	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	39	1457	Requiring external personnel, especially cloud services per discussion, to comply with an organization's security policies and procedures as well as monitoring that compliance is unrealistic. Why are there no ODP for time periods or reviewing compliance?	Redefine this requirement to differentiate the types of roles that would be required for these vs just stating all external providers. Add ODPs for timeframes for reviews and monitoring of compliance. Due to no ODPs for reviews or compliance and if assuming met by other requirements, then the discussion needs updated to reference those other requirements for their ODPs
126	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	39	1474	The assumption is made that an information system is only in a single facility. This is not true in many cases even before cloud and remote data centers.	a. should change "facility" to "physical locations" b should state "Require authorization credentials for physical location access" c. should change "facility" to "physical location(s)" d. should change "facility" to "physical location(s)" Need to define "facility" and "physical location(s)"
127	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	40	1492	The assumption is made that an information system is only in a single facility. This is not true in many cases even before cloud and remote data centers.	a. should change "facility" to "physical locations"
128	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	40	1515	Why is there no review timeline or process for alternate work sites as there are many other requirements?	Add ODP that has a requirement and timeline for reviewing alternate work sites allowed by employess
129	AIA / NDIA	General	NIST SP 800-171r3 ipd	40	1516	It is not clear what data elements need to be tracked to meet this requirement (e.g. are we to keep track of people's home addresses as alternate work sites?)	Clarify the data elements that need to be tracked to meet this requirement
130	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	41	1517	3.10.6-Allowing each ODP to redefine the controls required at alternate work sites would be disruptive to the KR operation.	Leave this to the contractor

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
131	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	41	1530	The assumption is made that an information system is only in a single facility. This is not true in many cases even before cloud and remote data centers.	Change "facility" to "physical location(s)" or "physically secured location(s)" and add definitions to the glossary
132	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	41	1530	There doesn't anything that requires documentation of how visitors are to be controlled and/or escorted.	Update ODP to "[Assignment: organization-defined circumstances requiring visitor escorts and control and organization-defined controls of visitor activity]"
133	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	41	1534	3.10.7-Seems to allow each ODP to define what access control system is to be used. KRs cannot change their access control sysetms to satisfy the desires of each ODP	Leave this to the contractor
134	AIA / NDIA	General	NIST SP 800-171r3 ipd	42	1555	Increased resources required to implement additional control	
135	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	42	1555	The two items do not seem directly connected and could cause confusion by combining them. They are likely different personnel that would perform each of these as well.	Split into separate requirements.
136	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	42	1576	This requirement seems to have lost the overall objective and original context of reviewing risk in the information systems and now only assess risk of unauthorized disclosure. With the new wording of a, b seems to only affect assessments of unauthorized disclosure so limited in scope and applicability. Based on the update to be risk assessments of unauthorized disclosure, the Discussion seems to not have been updated to discuss the limited scope but rather still discusses an overall risk management program that would assess risk of organizational assets	Revert back to the original requiring risk assessments to flow with many of the other requirements. Otherwise, the overall intent is lost If this is the intent of the new requirement, update the Discussion to highlight the limited scope
137	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	43	1599	c. seems to be redundant to a. unless referring to vulnerability feeds and databases.	Reword to reduce confusion since a already identifies that new scans should occur when new vulnerabilities are identified which imply updating the feeds.
138	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	43	1599	Discussion is overly complicated for this requirement that doesn't necessarily make the requirement objectives relatable.	Clean up the discussion to be more relatable to the new requirements.
139	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	43	1600	3.11.2.a-Scanning frequency is cannot be easily modified to satisfy each ODP. Large KRs must schedule scanning frequency to meet the size of the orgainzation and the ability to digest the scan results	Leave this to the contractor
140	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	43	1602	3.11.2.b-Remediation time is generally covered in contract terms if the KR has outsourced systems support. Allowing ODPs to redefine this may cause contractural problems or operational problmes for the KR	Leave this to the contractor
141	AIA / NDIA	General	NIST SP 800-171r3 ipd	44	1638	Increased resources required to implement additional control	
142	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	44	1638	There is no direct relationship to risk in the requirement. The discussion provides information on risk strategy and tolerance but none of the requirements are directly related to risk management since 3.11.1 was scoped down to only unauthorized disclosure of CUI.	Update the discussion to be more relevant to the updates to this domain and requirement Add "risk" into the requirement such as with "Respond to findings from risk and security assessments, monitoring, and audits"
143	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	44	1654	The control changes completely change the context of all organizational systems to only the system that has CUI and its environment of operation. Does environment of operation mean the security systems in place to support or something else?	The "environment of operation" needs to be better defined to add clarity of definition. With the descoping of all organizational systems down to only the one with CUI, this could make the entire organization ecosystem less secure since only requirement is to assess the CUI components and, maybe, the security systems
144	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	45	1681	the Plans of actions now require creation for known vulnerabilities so does this mean that every time a new vulnerability comes out, we have to update the SSP and create POAMs for remediation or can the normal processes, as defined in 3.11, be used? The way this is now worded, most systems will constantly have POAMs which would make Other Than Satisfied by many assessors/auditors.	Better clarity and/or association with other requirements, especially for vulnerability remediation, should be in the discussion.
145	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	45	1681	The definition of POAMs in the description is different in context of what is inferred/described in the requirement. The requirement describes POAMs due to continous monitoring (i.e., vulnerabilities) vs unimplemented security controls (missing requirements) and thus are inconsistenty and partially incompatible.	Better clarity and/or association with other requirements, especially for vulnerability remediation, should be in the discussion. Update the discussion to be consistent with the updated requirement.
146	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	45	1681	Use of the word "vulnerability" in paragraph 2 is too general.	Update the discussion to better clarify and/or associate with other requirements, especially for vulnerability remediation.
147	AIA / NDIA	General	NIST SP 800-171r3 ipd	45	1686	3.12.1 and 3.12.2.b-POAM update requirements will be coverd based on assessment. CMMC may have defined POAM update requirements. To allow ODPs to redfine this may disrupt other certification processes	Remove this statement

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
148	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	45	1701	The Discussion states that "ongoing" and "continuous" imply that an organization assesses and monitors at a frequency sufficient to support decisions. By changing the wording from "monitoring on an ongoing basis" to "continuous monitoring", the scope, complexity, and cost of this requirement jumped exponentially.	Change to an ODP to define the frequency for monitoring for the ODP types of controls to identify how different controls require different frequencies.
149	AIA / NDIA	General	NIST SP 800-171r3 ipd	46	1716	Increased resources required to implement additional control	
150	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	46	1716	There is no frequency defined for these independing assessments so it is left to interpretation instead of defining	Add ODP for frequency of assessments
151	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	46	1716	More clarity and detailed requirements should be provided for independent assessments. Are independent assessments required anytime controls are assessed? Should this be done annually? Do independent assessors count if they are part of the same organization but are not the ones implementing the controls? Will a self-assessment from a dedicated assessment team that is not typically involved with development and implementation but still part of the same company suffice? For example, can a company "internal audit" function be considered an "Independent Assessment"? This could cause a huge increase in cost to the government if this will be required on a contract to contract basis. The wording in the discussion suggests that small organizations or organizations without any independent assessment org must use a 3rd party to perform assessments which then significantly raises the costs of doing business with the government which will add additional cost to implement, so how will this be funded?	Recommend providing more clarity to contractors on: Who is allowed to perform the assessment. The judgment of an internal auditor, an employee may be influenced by any commitment, relationship, obligation, or involvement, direct or indirect. What type(s) of assessment will require independent assessment. Whether the ability to provide attestations/assessments by internal groups for an organization is allowed. What can be done if a company doesn't have the resources to complete an independent assessment.
152	AIA / NDIA		NIST SP 800-171r3 ipd	46	1717	3.12.15-Need more information on use of independent assessors or assessments. It s the understanding that CUI audit will be conducted by independent accessors. Does this control require a pre-assessment by independent assesors before Audit?	Having an additional assessment prior to audit will be a huge burden on the control owners plus will have monatary implications
153	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	46	1730	Is this requirement basically supposed to be about flow-down requirements between an org and vendors, suppliers, and sub-contractors? If so, why isn't this under SCRM or discussed relating to the new SCRM requirements?	Provide additional discussion and guidance for clarity relating to the intent of this requirement including possibly providing template documents for what these agreements would/should look like.
154	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	46	1730	This requirement seems to be addressing many of the same elements in 3.1.20. What is the difference and why doesn't the discussion relate to the previous requirements plus anything in the other areas.	Clarify the intent of this requirement with relationship to others such as 3.1.20 and the other requirements that levy requirements on external entities.
155	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	46	1731	3.12.6-CUI exchage criteria are often included in agreements between organizations. To allow each ODP to redefine the criteria for exchange may require all of these agreements to be re-negotiated	Remove this statement
156	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	46	1750	The discussion bringing up Intra-system connections seems very arbitrary and adds confusion to what is in scope for this requirement. What is the intent of this compared to other requirements such as 3.1.3, 3.5.2, 3.13.6? There seems to be overlap and there is no part of the discussion that relates them?	Remove and/or update the discussion to provide additional clarity of what is considered in scope for this requirement. Put any exceptions such as Intra-system connections, at the end to call them out and relate them to different requirements in the SP. Change to "Approve and manage internal system connections .. "
157	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	46	1750	Should this say "authorize and manage"?	Change to "Authorize and manage internal system connections .. "
158	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	46	1750	Why is 3.12.7 Internal System Connections under 3.12 and not under 3.13?	Move to the Systems and Communications Protection domain (3.13)
159	AIA / NDIA	General	NIST SP 800-171r3 ipd	46	1751	Duplicate effort/requirement as internal connections should be documented within 3.4.1	
160	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	46	1751	3.12.7-KRs already have processes for approving internal sysetms connections. To allow each ODP to redefine those requirements may require KR process changes and the ODP will not be familiar enough with the KR systems to make a rational judgement	Remove this statement
161	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	46	1751	3.12.7-What does authorize mean here for system connections. Does it require a documentation to see if interconnections were approved or there needs to be any formal process documented for approval and authorization of these connections	Provide more guidance on what details are required for this control
162	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	47	1769	Why put "managed" for external interfaces? Does this mean that any unmanaged interfaces are not in scope?	Provide clarity and reference to other requirements discussing the differences and/or assumptions on managed vs unmanaged.
163	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	47	1769	The order of the sub-requirements should be re-ordered.	Swap c. and a. to be a better flow of how the lifecycle is for systems.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
164	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	47	1769	Why was "protect" removed?	Identify why "protect" was removed from the old requirement.
165	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	47	1769	The entire discussion paragraph on shared commercial telecomm services is interesting but outside the scope of the boundaries being discussed in the requirement.	Rewrite this portion of the discussion to add clarity and that it is out of scope for the requirement.
166	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	47	1769	The discussion should identify the interrelationship between this requirement and the IA/AC requirements.	Update the discussion to highlight the interrelationships between the different requirements and how they are also in differing contexts.
167	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	47	1769	When discussing managed interfaces, why are guards lumped into the middle when the rest are technologies? Are "guards" personnel or something else? This needs to be explained or additional clarity added.	Rewrite the discussion to better reflect how technologies vs physical elements protect the system as "guards" are not "managed interfaces" in most people's minds.
168	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	48	1815	In most/many cases, this requirement has no meaning to most people and/or organizations without additional context and/or if they are using standard COTS software/hardware. Additional discussion regarding this should be included.	Add clarity to the discussion by citing some examples, such as using a temp file for storing paramters, etc. to help in understanding as well as to identify how COTS software/OS/HW may not allow for typical changes by an organization.
169	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	49	1845	The prohibition against “Split Tunneling” in 3.13.7, including the references to VPN and “external” systems propagates a legacy implicit trust mindset and is contrary to Zero Trust tenets and principles. 3.13.7 is in contradiction to NIST SP 800-207 which specifies on page 22: “Remote enterprise assets should be able to access enterprise resources without needing to traverse enterprise network infrastructure first. For example, a remote subject should not be required to use a link back to the enterprise network (i.e., virtual private network [VPN]) to access services utilized by the enterprise and hosted by a public cloud provider (e.g., email).” The definitions of External System and External Network starting on line 2792 refer to “direct control” of security controls and their effectiveness, continuing the pre-ZT idea that non-remote connections to a network that is under “direct control” should be granted a degree of implicit trust, whereas cloud service provider systems under contract are where threats lie and they are as untrustworthy as any random system on the Internet. As written, 3.13.7 is technology specific to VPN technology and should eventually be withdrawn. Until then, non-VPN text needs to be added to the discussion.	At the end of the Discussion on line 1863, add additional text that accounts for post-VPN zero trust thinking. Add additional Discussion text such as: “Where VPN is not used to implement these controls, such as Zero Trust architecture with distributed policy enforcement, the concept of split tunneling does not exist, so data exfiltration is controlled through other means. Preventing data exfiltration to unauthorized network resources could be established through web browser access controls, or through software allow/block-listing and EDR for monitoring and response to unauthorized software activity.”
170	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	49	1845	In lines 79-81 in rev3, states “For some requirements, ODP are included. These ODPs provide additional flexibility by allowing federal organizations to specify values for the designated parameters, as needed.”. Will a DoD or Federal org specify the criteria to use split tunneling, or allow companies to select the values?	Specify on line 1847 if the contractor or the government customer is able to define safeguards.
171	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	49	1845	The discussion highlights that VPNs can be used to perform approved split tunneling but 3.13.17 identifies that the proxy requirement can cause problems and possible "MITM" attacks.	Highlight the inconsistencies between requirements and how they interrelate.
172	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	49	1846	3.13.7-Once a KR has established a secure split tunnelling approach to allow each ODP to redefine the requirements would not only be disruptive but could reduce the security of the connections	Remove this statement
173	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	49	1866	How do the cryptographic mechanisms relate to the cryptography requirement (3.13.11). The discussion should relate this requirement to the others.	Update the discussion to relate to the other cryptographic requirements.
174	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	49	1866	Why was the "unless otherwise protected by alternative physical safeguards" removed?	The context of this drastically changed and now requires cryptography at all times during transmission and storage and undermines the requirement of physical transmission.
175	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	49	1866	What happened to physical transmission?	The context of this drastically changed and now requires cryptography at all times during transmission and storage and undermines the requirement of physical transmission.
176	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	49	1866	Why is encryption at rest now required for all CUI? This drastically changes the scope and requirements for storage, even in internal locations.	Add back the "unless otherwise protected" or add additional caveats to not require all CUI to be encrypted at rest.

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
177	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	49	1867	The updated requirement removes wording that allows for alternate physical safeguards. Many companies may use alternative measures and implementing this new requirement as stated could have significant impacts to large data center systems that may not encrypt. Removing the capability of implementing physical safeguards as a mitigation strategy would increase cost on contractors. The way the requirement reads now, all transmissions of CUI, even internally, must be encrypted which can be very problematic and is different from previous requirements.	Recommend including the wording that allows for alternative physical safeguards as an alternative mitigating security measure. Add an ODP to define boundaries and/or restate for external transmissions instead of requiring cryptography for all transmissions and at rest, regardless of location (i.e., internal or external)
178	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	49	1868	3.13.8-This control adds a requirment for encryption at rest regardless of where the data is stored. Many current file and database storage systems cannot support encryption at rest. This may make sense in cloud services, but does not make sense in on prem systems that have physical security controls that are KR managed	Remove this statement
179	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	50	1890	KRs will have established network session termination criteria established based on the needs of the KR. To allow each ODP to redefine these criteria will not only be disruptive to the KR but may make some KR required processes impossible to support	Remove this statement
180	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	50	1902	The discussion does not relate this cryptography requirement to the other ones and even states "when" used where most of them are "must" use.	Update discussion with relationships with other requirements.
181	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	50	1903	3.13.10-KRs will have established key management and regeneration criteria estabilished based on KR systems and requirements. To allow each ODP to redefine this will be impossible for the KR to manage	Remove this statement
182	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	51	1915	FIPS validated ODP leaves the usage of multiple of algorithms.	Suggest using NSA and FIPS validated algorithims.
183	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	51	1915	Requirement 3.13.11 removes direct wording for FIPS validated requirement and allows org defined encryption standard. However still references FIPS validation. Unclear if an assessor would still require FIPS. ODP should have baseline configuration and/or additional parts that define strong cryptography such as how 3.1.1 is identifying required areas to review. This is already complex enough with most services, applications, and technologies providing some type of cryptography options. This would allow for organizations to vet and validate vendor solution crypto rather than guessing and/or remaining non-compliant due to costs to change. The discussion doesn't identify the relationship with the other cryptographic requirements and doesn't discuss what would be considered strong crypto. It doesn't even list examples except FIPS-validated which is very limited in applicability and is the single most cause of most organizations having Other Than Satisfied, per DCMA, due to lack of technologies in the industry. In the previous version, there were discussions that identified that always encryption was not part of the intent but now this seems to be the intent which will cause serious cost and challenges with industry for requiring encryption at rest and transmission at all times. FIPS validated is problematic and NSA approved is even harder to obtain. When patches come out, any validation is typically invalidated. The requirement should describe strong encryption and/or identify the user of FIPS validated algorythms or FIPS compliant modules with strong key management. ITAR is only requiring FIPS compliant.	Remove the reference to FIPS validation to alleviate confusion as to whether FIPS is required of not. Modify the requirement to provide a list of minimum requirements for proving strong cryptography instead of just stating ODP to allow flexibility in meeting the requirement while being secure and provable. Update discussion with relationships with other requirements. Update the discussion to provide guidance on identifying strong cryptography. Modify requirements and discussions with ODPs that identify and highlight the boundaries and requirements as well as relationships with the other requirements in their associated discussions. Change the encryption requirements to identify FIPS compliant with strong key management is considered strong encryption and cryptography rather than FIPS validated.
184	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	51	1916	3.13.11-To allow each ODP to redefine the types of encruyption to be used will be impossible for the KR to manage, particularly in enterprise sysetms. Allow flexibility based on the data's specific risk situation, types of assets and business needs or other compensating controls. There is a high risk involved causing inconsistency in control implementation as not all assets e.g. third party, COTS applications etc. will adhere to ODP as they build their own ODP.	Remove this statement
185	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	51	1926	The discussion uses the example of "Indication of use includes signals to users.." What are signals? A better example would be useful here such as a pop-up on screen that says recording in progress or that your microphone has been turned on rather just the generically stated "signals".	Update the discussion with better examples of "provide explicit indication of use" rather than "signals to users".

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
186	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	51	1927	3.13.12-To allow each ODP to define the requirements for remote activiation of collaborative systems could easily make it impossible for a KR to initiate a collaborative call session as these frequently require remote activitation	Leave this to the contractor
187	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	51	1940	Documenting unacceptable mobile code leaves risk that something will be missed. Defining only acceptable mobile code and indicating all other code is unacceptable would suffice The discussion should provide more clarity on how mobile code is defined and examples of monitoring code.	Update the discussion with better every day examples of mobile code and how to monitor along with examples such as PDFs and Macros. a. Define acceptable mobile code and mobile code technologies.
188	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	52	1959	The discussion highlighting the possibility of allowing MITM attacks is directly conflicting with 3.13.15 which is required to protect against MITM attacks.	Reassess the need for 3.13.17 especially with the conflicts with other requirements such as 3.13.15.
189	AIA / NDIA	General	NIST SP 800-171r3 ipd	52	1972	Not sure how internal traffic is routed or if we have an authenticated proxy server	
190	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	52	1972	Internal Network Communications Traffic. Route internal network communications traffic to external networks through an authenticated proxy server. Comment: requiring “an authenticated proxy server” for “internal network communications traffic to external networks” is a significant financial, administration, and operations burden for small and some large companies. NIST should not be prescribing a solution; this functionality can be performed by other mechanisms, that SMBs will already have, and having a separate Proxy server is an extra cost they cannot afford.	Remove this control because this is difficult for SMBs.
191	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	52	1972	Why is this called "internal network communications traffic" when there are other requirements that discuss internal network traffic but this specific requirement is for internal to external?	Remove "Internal" from the title or rename to "Internal to External Network Communications Traffic" or "Routing Network Communications Traffic Externally"
192	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	52	1972	The discussion highlights that this requirement can cause problems with VPNs and be more insecure while conflicting with other requirements in this same SP. Does this requirement need to be here or technology/architecture specific? Why is a requirement added that is technology/solution specific "authenticated proxy server" when 3.13.14 was removed due to being technology specific? The original requirement in the R2 provided more flexibility for implemntation.	Remove the requirement or remove the technology specific requirement. Highlight the inconsistencies between requirements and how they interrelate. Modify the requirement to not be solution specific but rather meet the intent of the requirement such as "Require internal communications traffic to be authenticated prior to allowing an external connection".
193	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	53	1993	The discussion creates confusion and needs to be rewritten. What is the number that this should be limited to? What if the point of the mission is external facing such as for collaboration purposes where access is limited but not the number of network connections? This seems to undermine the ability to perform.	Separate the first sentence into what limiting is about and the example of transitioning from older to new technologies. The example should then be combined with the second sentence to form a single sentence that discusses why needed and the risks created. This would add clarity around the example. Provide guidance of recommendations for baseline configurations for when it is not part of the scope of the mission vs when it is the scope of the mission.
194	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	53	1993	Why wouldn't this be one that has an ODP as it seems to be variable based upon the mission.	Add ODP to the requirement and provide baseline recommendations based on the mission.
195	AIA / NDIA		NIST SP 800-171r3 ipd	53	1994	3.13.18-There is no defined limit for this control which has been defiend. Is the number of connections left to organizations to define and manage	Provide more guidance on what details are required for this control

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
196	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	53	2006	The additional requirement from NIST 800-53 Rev 5 was missing - Incorporate flaw remediation into the organizational configuration management process. subobjective b. is problematic for many small businesses as most use the "automatic updates" as that is what is suggested by all security training sessions. Requiring testing of patches. This should be be scoped down to just critical systems. This also requires every company to have an additional system for testing the patches before deploying which also adds significant cost. Flaw Remediation “b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation” - This requirement will result in a net-negative security for many businesses, including small businesses. Many businesses typically configure their systems to accept and install vendor security updates automatically. Automatic patching results in much quicker flaw remediation, which is very important. - The vast majority of business IT departments are less qualified than their trusted vendors to test and filter patches. This control means companies cannot accept push updates from their vendor, but instead must configure their systems to reject patches until the internal IT department manually packages them and pushes them to a test group, then to production. - For most businesses, this 1) greatly increases latency before patching from ~12 hours to 15-30 days, 2) requires adding extra infrastructure to manage the process, such as a non-FedRAMP patch management solution, which increases the attack surface of the information system, 3) increases IT burden by at about 10 hours per week for a business with less than 10 users. -- For a typical business implementing this requirement, the proposed benefit (testing patches to determine if they are malicious) is negligible. Unless an explicit control is added to this effect, business IT departments will not perform network analysis or behavior analysis during testing to identify malicious behavior. They will simply slow down their patching process dramatically. -- This change would result in a net negative for security for most businesses. The risk of a trusted vendor being compromised and pushing a bad patch is less than the unintended consequence of increasing latency in flaw remediation and increasing attack surface.	Include as part of the requirement to ensure change management processes are followed when implementing flaw remediation processes since it involves changes within the environment. Modify b. with and ODP that is requiring the testing for Critical and Key systems.
197	AIA / NDIA	General	NIST SP 800-171r3 ipd	53	2008	not sure if we verify testing of patches?	
198	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	53	2010	3.14.1-Installation of softwar and firmware updates are frequently covered in contract requirements when the KR has outsourced support. In addition, KR requires sufficient time to test updates before they are installed. To allow each ODP to redefine this when the ODP has no understanding of the KR systems will be quite disruptive	Leave this to the contractor
199	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	54	2028	Why didn't this get updated with an ODP as it is prime candidate relating to frequency and designated locations. This should mirror what is in 3.11.2	Add an ODP to b. for frequency of updates. Add an ODP to a. for designated locations/boundaries.
200	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	54	2028	The second paragraph is good information but extraneous to the requirement and should be removed.	Remove the second paragraph under Discussion.
201	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	54	2057	The example in the Discussion implies that response activities should include notifying external organizations which is not part of the requirement, recommend removing this from the discussion.	Recommend removing the example in Discussion that implies that response activities should include notifying external organizations
202	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	55	2077	The discussion should relate to the other requirements that do very similar actions (i.e., detecting unautorized use, logging, etc.)	Update the discussion to identify the relationship between relevant requirements such as in the AC, IA, and AU domains.
203	AIA / NDIA	General	NIST SP 800-171r3 ipd	56	2114	Not sure how/if spam protection mechanism is updated	
204	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	56	2114	What is the definition of Spam?	This needs defined to help understand how to meet the requirement

* indicate required fields

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
205	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	56	2114	What are considered messages? Email only or does this also include voicemail, text, SMS, etc.? "Spam" needs to be clearly defined. Discussion identifies parts of emails but also could include other technologies per examples for entry/exit points.	Messages needs to be clearly defined as well as all the technologies that this is meant to address.
206	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	56	2114	Why wouldn't this be one that has an ODP as it seems to be variable based upon the mission and/or technologies?	Add ODP to the requirement to define the technologies or services that would be affected by this and provide baseline recommendations based on the mission.
207	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	56	2114	Modify the discussion to better define what "messages" and the intent of the requirement.	Update the discussion to be similar to: "Spam filtering is used to prevent unwanted, unsolicited, and often harmful emails from reaching end user mailboxes. Spam filters are applied on inbound and outbound emails to help protect your network from phishing messages and emails containing viruses and other malicious content"
208	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	56	2117	3.14.8-To allow each ODP to redefine spame protection updates will be disruptive to KR operations	Leave this to the contractor
209	AIA / NDIA	General	NIST SP 800-171r3 ipd	56	2127	Increased resources required to implement additional control	
210	AIA / NDIA	General	NIST SP 800-171r3 ipd	57	2148	3.15.2-SSP update frequency will likely be covered by CMMC or other certification criteria. To allow ODPs to redefine these requriements is duplicative and unnecessary	Remove this statement
211	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	57	2165	How is this different from 3.1.9, 3.2.1, 3.2.2, 3.9.1, and 3.9.3? The discussion should identify and relate all of the relevant requirements.	Update the discussion with how this requirement relates to the others in the document and how it is different in intent. Update the discussion to relate to 3.1.9
212	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	57	2165	Since CUI is "owned" by the federal government, it is the agency's responsibility to provide handling instructions to the contract prime, who is then responsible for flowing those requirements down to their vendors and suppliers. Because of this, contractor would not only be required to maintain different Rules of Behavior forms based on role; there will be a need to maintain unique forms for each agency supported.	It would be much easier for agencies to maintain these types of forms for their organization. Recommend that this requirement be recategorized to FED.
213	AIA / NDIA	General	NIST SP 800-171r3 ipd	57	2168	3.15.3-KRs will already have established processes for updating any requried rules of behaviour so to allow each ODP to redefine this is unnecessary	Remove this statement
214	AIA / NDIA	General	NIST SP 800-171r3 ipd	58	2199	Increased resources required to implement additional control	
215	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	58	2199	Mitigation/hardening/compensating controls are refenced in the subsequent discussion but not an option How does this relate to identifying and maintaining a list? The discussion should relate to the other requirements for inventory and component management.This needs to be rewritten to identify how risk is managed and unsupported components are managed.	b. Provide options for alternative sources for continued support for unsupported components; or c. Restrict/isolate/harden unsupported components per an approved ODP Modify the requirement to be similar to: Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk. Determine if: [a] the organization maintains a list of products the organization is using that are no longer supported by their vendors or do not have any type of vendor support; [b] the organization documents how it manages the risk of each such product within the organization; and [c] the organization tracks the risks of using non-vendor-supported products. Update the discussion to relate to managing the list of components 3.4.10.
216	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	59	2224	Requiring external personnel, especially cloud services per discussion, to comply with an organization's security policies and procedures as well as monitoring that compliance is unrealistic.	Redefine this requirement to differentiate the types of roles that would be required for these vs just stating all external providers.
217	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	59	2224	The discussion should relate this requirement to the organizational agreements requirements (3.1.20)	Update the discussion to identify the relationship between this and 3.1.20
218	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	59	2225	3.16.3-KRs will have established relationships with external system service providers that define the security requirements. To allow each ODP to redefine these requirements will be disruptive to KR operations and may result in contractural issues with the external suppliers, and the scope of suppliers is unclear	Remove this statement
219	AIA / NDIA	General	NIST SP 800-171r3 ipd	59	2251	Increased resources required to implement additional control	
220	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	59	2251	This is useful in NIST SP 800-53 for the program level but very difficult to implement at the enterprise level because the plan varies for each individual program.	This is useful in NIST SP 800-53 for the program level but very difficult to implement at the enterprise level because the plan varies for each individual program.

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
221	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	59	2251	The term "plan" is typically used at the program level and in many cases companies would want to show persistent compliance artifacts at the enterprise or division level, and this requirement would be very difficult to implement at the enterprise level because plans will vary for each individual program. Additionally, the second paragraph is extraneous and adds confusion and should be removed from this document.	Consider using “system” or “process” terminology instead of “plan” to connote persistence. Remove the ODP for reviews as it doesn't add any real value. Create an example template for a Supply Chain Plan that organizations can use. Remove "the development, manufacturing, acquisition, delivery, operations, maintenance, and disposal of" Remove the second paragraph under Discussion.
222	AIA / NDIA		NIST SP 800-171r3 ipd	59	2252	3.17.1-All the sub contractors and suppliers already require to be Level 1 or 2 compliant as per the flow down requirements. Does this control require additonal tracking of supply chain risk in a more formal way other than the flow down requirements	Provide more guidance on what details are required for this control
223	AIA / NDIA	General	NIST SP 800-171r3 ipd	59	2255	3.17.1-It is unnecessary to allow each ODP to redefine the update frequency of the supplier risk management plan	Remove this statement
224	AIA / NDIA	General	NIST SP 800-171r3 ipd	60	2277	Increased resources required to implement additional control	
225	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	60	2277	Using “avoid” instead of “protect against” may be clearer for the reader. Or “protect against in advance”	Using “avoid” instead of “protect against” may be clearer for the reader. Or “protect against in advance”
226	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	60	2283	Please clarify what is meant by a "filtered buys". Discussion paragraph: 1. NIST has consistently referred financial questions to DOD and DOD has consistently refused to provide financial reimbursements, other than via overhead, so why would NIST include the statement ""Organizations also consider [did they mean ""should consider""?] providing incentives for suppliers to implement controls, promote transparency in their processes and security practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. 2. The last sentence of the first paragraph is confusing and can be worded. 3. Any detailed information on supplier processes and security practices should be limited to critical suppliers, as contractors and their supply chain are not staffed to address this with every supplier, nor should contractors have the liability for protecting such information. Again, a financial issue NIST shouldn't be implicating by such a requirement.	Delete the reference to "filtered buys", or if it is retained, please define this term in the glossary. Delete incentives reference and reword the transparency reference, so it would read "Organizations should require transparency in critical suppliers' processes and security practices, flow down contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Reword the last sentance to: "Tools and techniques may provide protections against unauthorized production, theft, tampering, poor development practices, and the insertion of counterfeits, malicious software, and backdoors throughout the system life cycle."
227	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	60	2289	Discussion: **1**. NIST has consistently referred financial questions to DOD and DOD has consistently refused to provide financial reimbursements, other than via overhead, so why would NIST include the statement "Organizations also consider [*did they mean should consider* ?] providing incentives for suppliers to implement controls, promote transparency in their processes and security practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. **2**. The last sentence of the first paragraph is confusing. **3**. Any detailed information on supplier processes and security practices should be limited to critical suppliers, as contractors and their supply chain are not staffed to address this with every supplier, nor should contractors have the liability for protecting such information. Again, a financial issue NIST shouldn't be implicating by such a requirement.	Delete incentives reference and reword the transparency reference, so it would read "Organizations should require transparency in critical suppliers' processes and security practices, flow down contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers.
228	AIA / NDIA	General	NIST SP 800-171r3 ipd	60	2300	Increased resources required to implement additional control	
229	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	60	2300	3.17.3. Supply Chain Controls and Processes a. Establish a process or processes for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes. b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain�related events: [Assignment: organization-defined supply chain controls] **Comment:** This ODP is wide open. What if one agency demands the use of its standard solution, and that contradicts the choice of another agency?	The intent of adding ODP s is a step in the right direction, but defining the Federal Agency as the definition of the “Organization” was a fundamental mistake. DIB companies don t work for just one “Federal Organization” at a time, unlike the assumption made for the audience of 800-53r5, so copying that text over as-is was a mistake. The definition of “Organization” has to be the non-federal organization (company) itself, and the DoD CIO s office should correct that mistake on line 80 of 800-171r3. C3PAO / DCMA DIBCAC assessors can hold the DIB companies accountable to reasonable and fair interpretations of their defined ODPs.

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
230	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	60	2300	It is very difficult to maintain compliance at the enterprise level when the controls contain organization-defined parameters that change based on the customers preferences or have differing levels of compliance based on system/information criticality similar to how NIST SP 800-171 and 172. The NIST SP 800-53 source controls for Supply Chain Risk (SR Family) talk about using a diverse supply base as a control to protect against supply chain risk, however this can be difficult for some product lines or instances where supplier parts are locked into a specific product for many years (e.g., complex sub systems where sources can't be changed before going through the lengthy and costly process to qualify). As a result, contractors will have trouble meeting the source requirements, and many customers may disagree with swapping out parts.	It would be better for NIST to define a minimum set of techniques and methods. Also recommend adding language in that would caveat it to say something to the effect of "when contractually requested by the customer".
231	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	60	2303	3.17.3-to allow each ODP to define the controls to be used for the supply chain will be quite disruptive not only to the KR but also to the KR supply chain	Remove this statement
232	AIA / NDIA	General	NIST SP 800-171r3 ipd	61	2322	Duplicate effort/requirement of 3.8.3 as non-digital media is also covered/discussed	Remove
233	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	61	2322	It would be better for NIST to define a minimum set of techniques and methods. It is very difficult to maintain compliance at the enterprise level when the controls are organization-defined, i.e., change per customer set.	It would be better for NIST to define a minimum set of techniques and methods. It is very difficult to maintain compliance at the enterprise level when the controls are organization-defined, i.e., change per customer set.
234	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	61	2322	The discussion should relate to the media protection sanitization requirements as this seems to say many of the same things so the context should be clarified.	Update the discussion to identify the relationship with this requirement and 3.7.4 and 3.8.3.
235	AIA / NDIA	Editorial	NIST SP 800-171r3 ipd	61	2322	How does this requirement differentiate from 3.8.3 Media Sanitization?	Recommend including "in the supply chain" or "on components" to 3.8.3 and removing this requirement or provide clarification as to how these two requirements are dofferent.
236	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	61	2323	3.17.4-Component disposal requirments should not be ODP assigned. If the USGOV wants particular disposal requirement to be implemented then those requirements should be directly stated in this document	Define the requirement and remove the ODP
237	AIA / NDIA	General	NIST SP 800-171r3 ipd	61	2338	Noticed the NIST standard for disposal was not included in references	Reference NIST 800-88
238	AIA / NDIA	Editorial/Technical	NIST SP 800-171r3 ipd	79	3011	NCO is a new tailoring criteria and some previous requirements were recategorized as NCO. Is there expectation that all NCO are also to be met by an organization similar to NFO?	More clarity regarding NCO is needed to understand the point of the new tailoring criteria and how it affects contractors/DIB.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
239	AIA / NDIA	General	NIST SP 800-171r3 ipd	2	N/A	"Why did NIST introduce organization-defined parameters (ODP) in selected security requirements? Organization-defined parameters are used in the NIST SP 800-53 controls to provide flexibility to federal agencies in tailoring controls to support specific organizational missions or business functions and to manage risk. To provide that same flexibility to federal agencies in working with nonfederal organizations to protect CUI, ODPs have been selectively employed in the requirements in NIST SP 800-171, Revision 3, consistent with their use in NIST SP 800-53, Revision 5. Once ODPs have been defined, they become part of the security requirement and can be assessed as such. ODPs also help simplify assessments by providing greater specificity to the requirements being assessed and reducing ambiguity and inconsistent interpretation by assessors. Federal agencies can elect to specify ODPs, provide guidance on selecting ODPs for nonfederal agencies, or allow nonfederal agencies to self-select ODP values." **Comment:** Due to the nature of enterprise, and now cloud computing, information systems have been built based on specific technologies that make up the non-federal information system(s) which are not common across industry. These systems have been tuned to a companies risk tolerance and any changes mandated by a potentially wide variety of federal agencies would cause significant changes to these systems and others (Cloud, SaaS, IaaS, PaaS, etc.,) that are being used to support federal agencies missions and purpose. These information systems are also used to support other entities to include Commercial entities via appropriate segregation that are subjected to other regualtions and requirements beyond 800-171 and in some instances could conflict with 800-171 ODP's defined by federal agencies. It also negates and significantly complicates assessments due to the variability of ODP's from a variety of non-coordinated stakeholders. As such, each contract could require the re-write of process, policy and procedures within a information system that conflicts with another contract by a separate federal agency.	Allow the non-federal organizations the ability to identify ODP's within their own information system(s). Allow these non-federal organizations to define and explain how their information system protects CUI data via the System Security Plan and via interview with non-federal organization SMEs. The significant variabilty introduced by "federal agencies" choosing ODP's without benefit of knowing how an Enterprise network is configured would cause significant delays to apply changes. Additionally, companies with 1,000's of federal contracts would be innundated with changes. The statement in the FAQ that it would: "simplify and reduce ambiguity in assessments" is erroneous since any federal agency could define their own ODP thereby increasing complexity and variability. The current DCMA DIBCAC Assessment methdology allows for proper Basic, Medium and High assurance assessments of non-federal organizations and should be used as a model/guide for future assessments where the non-federal organization defines ODPs and then supports their use via, evidence, interview and demonstration.

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
240	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	We remain concerned with agencies having the option to set differing Organization-Defined Parameters (ODPs). The stated objective of Executive Order (EO) 13556 is to establish a governmentwide program to standardize the handling of Controlled Unclassified Information (CUI). Allowing federal agencies to use ODPs to define unique requirements is contrary to the objective, as it promotes inconsistent and potentially competing standards across the federal government. Agency baseline expectations will diverge resulting in a patchwork approach to cybersecurity, rather than allowing a single baseline standard as intended. Companies supporting multiple agencies may determine that some requirements are too costly to implement based on financial/risk analysis. Having these contradictory ODP requirements across agencies will make it difficult for companies to fully comply and will create operational challenges as noted below: • Differing ODPs being specified in RFI/RFPs will result in no single baseline security configuration. • Companies will be burdened with coordinating different ODP assignments across multiple agencies. • As ODP assignments may be incompatible, companies will find it difficult to have one 'enterprise' level SSP that complies with all ODPs. • Companies being forced to implement varying agency mandated ODPs will result in significant impact on government programs due to additional unnecessary costs and compliance challenges. • Differing ODPs will make 3rd party assessments difficult, as the assessor must have the ODP details from all contracts to validate all ODP requirements. • Assessors, rather than referring to a single baseline standard, will rely on individual experience to interpret different ODP requirements, resulting in inconsistent assessment results. Moreover, while government contracting offices are competent with procurement rules and able to determine when certain requirements can be waived, they may not be able to define detailed ODP requirements or cybersecurity-related controls. There is also no known cadence for managing changes to ODPs, so agencies could change ODPs at any time (unlike revisions to SP 800-171 which are published with a formal comment period). Lastly, SP 800-171 is becoming more recognized and accepted globally. Allowing varying ODPs across federal agencies will weaken the NIST "standard" making it less effective and less likely to achieve reciprocity with other standards.	We recommend NIST work with government and private industry to establish standard ODP values that can be implemented uniformly.
241	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	NIST's effort to consistently align the language of SP 800-171 with SP 800-53 is greatly appreciated; however, it appears that key elements and context from SP 800-53 were not included in draft SP 800-171 R3. For example, 3.14.1 "Flaw Remediation" in draft SP 800-171 R3 includes parts a-c from SP 800-53 but does not include part d. The draft SP 800-171 R3 derivative also omits key information that explains parts of the requirement, making it difficult for organizations and assessors to implement risk-based approaches.	We recommend NIST continue to align requirements with SP 800-53 and provide justifications as to why certain SP 800-53 control parts have been omitted from SP 800-171 requirement objectives. Including an objective level cross-reference to SP 800-53 for additional guidance and information would also be helpful.
242	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	It is unclear how to implement the requirements and determine what is expected even with the relevant discussions included. The assessment guide provides better insight into the level of effort expected to fully implement the requirements. It is difficult to submit comments on the requirements and their intended implementation without the SP 800-171A assessment guide, as it outlines the objectives and clarifies the tasks needed to implement the requirements.	We recommended that SP 800-171A assessment guide be released in tandem with draft SP 800-171 R3, to allow for more constructive and useful comments to be submitted.
243	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Many discussion sections associated with requirements contain inconsistent and/or incoherent language, making it difficult to understand the intent of the requirement. Additionally, some discussion sections that refer to interrelated requirements fail to adequately describe how or why the requirements are interrelated (e.g., 3.1.23).	We recommended that the discussion sections be updated for consistency, with descriptions to address the intent of the requirement, and updated to be more concise, removing information not directly related to the requirement.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
244	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	It is unclear what the effective date for this publication will be once it is finalized and published. Due to the significant changes being introduced, companies should be given adequate time to implement.	We recommend defining a transitional period to implement SP 800-171 R3 changes, which are expected to be time consuming, labor intensive, and costly.
245	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Exceptions should be made for legacy systems (where implementation of new requirements is not reasonably feasible or cost effective to implement these controls retoractively, where the legacy system still maintains reasonable security controls	
246	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Limit cross-references to supporting publications - that significantly increases the burden and confusion of what is required, or alternatively clarify that they are for guidance only.	
247	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	The statement should clarify that any changes to requirements, to the extent incorporated into a government contract, only apply to new contract actions after the contractor has had an opportunity to consider and negotiate the cost for such changes.	
248	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Removal of enduring exceptions was not addressed and should have a comment section regarding the change and how to address in the new revision rather than just dropping the entire paragraph that was in previous revisions.	Add a section discussing enduring exceptions and how they would now be handled in the new revision as well as adding some additional context in the FAQ.
249	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	when containing ODP, not all statements make complete sentences	Fix all ODPs to be readable and complete sentences
250	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	The requirements need to be rewritten to allow for understanding how to implement and what is expected including the relevant discussions to provide clarity of understanding.	The requirements need to be rewritten to allow for understanding how to implement and what is expected including the relevant discussions to provide clarity of understanding.
251	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Many of the new changes make it harder for small businesses to adequately and effectively meet the requirements due to some additional on-demand and automation requirements.	Review the intent of these requirements to be able to be met by small businesses in a cost effective and efficient manner
252	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	There are too many assumptions based on NFO and NCO tailoring criteria that may not be occurring for most small businesses and thus they won't be performed which will cause challenges for them to successfully meet the requirements.	Remove the tailoring criteria, especially NFO and add them to the requirements using ODPs
253	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Discussions should be more tailored and readable instead of a stream of inconsistent and incohesive sentences. Break down the discussion as the requirements are broken down for easier readability and understandability.	Break down the discussion as the requirements are broken down for easier readability and understandability.
254	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Appreciate NIST's effort to consistently align langauge between 800-171 with 800-53	Continue
255	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	N/A	N/A	"a. Mark system media containing CUI indicating distribution limitations, handling caveats, and security markings."	Recommend carrying over word "necessary" from rev 2: "a. Mark system media containing **necessary** CUI indicating distribution limitations, handling caveats, and security markings."
256	AIA / NDIA	Technical	NIST SP 800-171r3 ipd	N/A	N/A	3.16.2. Unsupported System Components a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide options for alternative sources for continued support for unsupported components.	Consider replacing "provide" with "offer"; provide implies a level of certainy/control for unsupported components that may not exist
257	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Further reviews of the discussions under each requirement need to be performed to provide references to the interrelated requirements which is done is a few but most do not contain.	Further reviews of the discussions under each requirement need to be performed to provide references to the interrelated requirements which is done is a few but most do not contain.
258	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	The assumption is made that an information system is only in a single facility. This is not true in many cases even before cloud and remote data centers.	Change "facility" to "physical location(s)" or "physically secured location(s)" and add definitions to the glossary
259	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Why does the CUI Overlay not address any element of what/why requirements were changed from 171rev2? The overlay discusses what what changed from 800-53r5 but not 171rev2 which is the point from where we are moving since we were not moving from 800-53r5.	Provide additional discussion, clarity, and guidance on the reasoning why the 171rev2 requirements were drastically changed, including many with the context drastically changing, to help understand the rationale and reasoning for the changes. This can be provided in the CUI Overlay template to help consolidate an understanding of the changes.
260	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	Tailoring criteria comments on the changes and why are inconsistent and incomplete as several of the 800-53r5 requirements do not match the 800-171r3 requirement but there is no explanation on the change.	Fix the inconsistencies within the document to document "every" change and not just some.
261	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	The Discussions need to be reviewed to make sure they are consistent and adequately describe the intent and options of the listed requirements and remove all extraneous information that is not directly related to the requirements.	The Discussions need to be reviewed to make sure they are consistent and adequately describe the intent and options of the listed requirements and remove all extraneous information that is not directly related to the requirements.

Enclosure 2: AIA / NDIA Comments Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
262	AIA / NDIA	General	NIST SP 800-171r3 ipd	N/A	N/A	The discussions in every requirement should accurately reflect the intent of the requirement and be very specific on examples and definitions that relate directly to the requirement.	Update the discussions under every requirement to be more concise, identify the relationship to the other requirements, identify the intent and context of the requirement, and remove extraneous information the does not directly relate to the requirement.