From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] National Institute of Standards and Technology Attn: Computer Security Division
Date:	Friday, July 14, 2023 10:30:49 AM
Attachments:	image001.png image002.png image003.png ND-ISAC_ NIST 800-171 Rev 3 Comment Ltr_FINAL_13JUL2023.pdf ND-ISAC sp800-171r3-ipd-comments 07132023.xlsx

---

FROM: NATIONAL DEFENSE INFORMATION SHARING & ANALYSIS CENTER (ND-ISAC)

TO: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES (NIST)
Computer Security Resource Center
Attn: Computer Security Division, Information Technology Laboratory
Email address: 800-171comments@list.nist.gov

Reference: NIST SP 800-171 revision3, invitation to comment – suspense July 14, 2023

Ladies and Gentlemen,

Thank you for the opportunity to provide feedback on the latest revision to the special publication 800-171: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations revision 3 (SP 800-171r3); Initial Public Draft,* as outlined at this link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.ipd.pdf

In that regard, we focused our review on the capabilities associated with implementing cybersecurity procedures and business operations as represented by our Member Companies who, more broadly, represent the Defense Industrial Base (DIB) sector. Accordingly, the subject matter experts from our Member Companies recommend augmenting / aligning the focus around these key areas:

- NIST standards should consider complex real-world network infrastructure implementation challenges within the private sector
- ODPs without sufficient suggested implementation guidance post potential extraordinary challenges for the private sector
- NIST influence on federal agency cybersecurity policy and regulatory compliance requirements for industry

Thank you for considering more specific details in the comment matrix attached to this email, which is accompanied by a cover letter.

The ~140 member companies of ND-ISAC are committed to contributing to the improved cybersecurity and resilience of the Defense Industrial Base. In that spirit, we look forward to collaborating with NIST to develop fruitful and effective approaches to achieve that. Thank you again for the opportunity to submit the referenced comments.

V/r
Steve Shirley
Executive Director
[redacted]

[redacted]

National Defense ISAC

[redacted]

[redacted] | [redacted] | www.ndisac.org

July 14, 2023

Dear Dr Ross and Ms Pillitteri

Reference: Invited comments -- Ross R, Pillitteri V (2023) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3 ipd

Thank you for the invitation to provide feedback on the NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Initial Public Draft, dated May 2023. Based on extensive review, ND-ISAC cybersecurity subject matter experts within our technical working groups respectfully submit the attached spreadsheet, but also encourage the following overarching perspective:

- **NIST should develop implementable standards, supported by rationale, which consider complex real-world network infrastructure implementation challenges within the private sector.**

  Rationale -- In its scope R3 reaches toward a technical ideal, to the extent it seems isolated in considering private sector (contractors' and subcontractors) system environments, cyber security risks, and operational efficiencies. This circumstance will translate to corresponding implementation challenges, escalated cost and, ironically, implementations suboptimal to objectives to improve cybersecurity resilience in the private sector.

- **The introduction of Organization Defined Parameters (ODP) without sufficient suggested implementation guidance poses potential extraordinary challenges for the private sector. For example, there will be significant implementation and cost issues in working to comply with conflicting ODPs in the routine circumstance where companies perform on dozens-to-hundreds of contracts issued by multiple federal entities which contain differing CUI specified by those entities.**

  Rationale -- Does NIST intend the authority to promulgate ODPs to vest exclusively in a specific federal agency and with the discretion for that federal agency to modify ODPs on a contract-by-contract basis? Or, alternatively, does NIST envisage a schema for common ODPs to be pre-agreed across multiple federal agencies? A NIST webinar related to R3 further complicated understanding when NIST speakers described an overview for NIST SP 800-171 that incorporated two planned revisions, augmented by a "CUI overlay" (cited as a prototype), and culminated with an apparent reach-back and integration of NIST SP 800-53 security requirements, controls, and control enhancements. Does this plan, especially the 800-53 reach-back, imply a "federal-agency-pick-your own-menu" of controls for their cybersecurity contract requirements? If so, this assumes a simply unrealistic degree of flexibility on part of the private sector to meet multiple and varying federal agency requirements. We earnestly encourage clear, precisely defined, and harmonized guidelines and standards which, ideally, can also be reciprocally accepted in an increasingly global cybersecurity ecosystem.

- **NIST influence on federal agency cybersecurity policy and regulation**

  Rationale -- ND-ISAC member companies respect and regard NIST's role as indispensable in developing recommendations and guidance for science-based cybersecurity technical controls. We

note, though, that NIST statements carefully exclude NIST from a federal cybersecurity policy or regulatory role. However, the real-world fact of life is the science role is not isolated from the federal cybersecurity policy it stimulates. NIST, therefore, exercises enormous influence on companies who seek to do business with the federal government. In that vein we respectfully request NIST consider the challenges that arise when the optimal technical instantiation and related recommendations collide with the invariably complicated real-world implementation.

Please find attached the results of our review documented in the NIST comment template. ND-ISAC looks forward to reviewing NIST's 2nd public draft and NIST 800-171A as planned for FY24/Q2 and looks forward to collaborating on proposed controls to protect Controlled Unclassified Information (CUI).

The ~140 member companies of ND-ISAC are committed to contributing to the improved cybersecurity and resilience of the Defense Industrial Base. In that spirit, we look forward to collaborating with NIST to develop fruitful and effective approaches to achieve that. Thank you again for the opportunity to submit the referenced comments.

V/r

STEVEN D. SHIRLEY
Executive Director

Attachment:
Comment Matrix

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	National Defense Information Sharing and Analysis Center (ND-ISAC) and ND-ISAC Small and Medium Business	Important Note	Publication	0	Note: Small Medium Business Designation (SMB) in Comment/Change	Small to Medium Businesses are burdened by the compliance load while larger companies require the flexibility to manage multiple sources of requirements through their own risk management processes. Please note the designation of SMB has been added throughout the template to indicate the potential divergence in the comments and suggested changes by line number. Due to existing resource constraints in personnel, money, and other resources, small businesses cannot afford outsourcing (or tasking inexperienced/ill-equipped internal personnel) the interpretation of requirements. Many of the risks that the "in-the-weeds" technical and procedural changes seek to mitigate are not value-added in a small business environment – particularly those who operate as subcontractors/sub tiers, but still receive NIST 800-171 flow-down	NIST should update interpretation of the requirements through guidance as standards become more critical. Small Business cannot afford to hire a consultant especially when the consultant(s) may or may not provide the "right" interpretation of the requirement, discussion, and/or references. NIST should offer a "sliding scale" allowance or percentage range of compliance to incentivize small business to seek security and compliance in ways that make the biggest impacts to their environments, where "all or nothing" would discourage them and result in minimal (or no) security compliance at all.
2	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	0	Page i Keywords	With the change to eliminate the distinction between basic and derived, the basic security requirement and derived security requirement terms as Keywords may no longer be relevant	Removed basic security requirement and derived security requirement from the Keywords Section. Re-evaluate the criteria and selection of Keywords
3	National Defense Information Sharing and Analysis Center (ND-ISAC)	General &Technical	Publication	0	Page i Reports on Computer System Technology	Section states ITL at NIST reports on tests, reference data, proof of concept implementations, and analysis without sources and references.	Provide reports on tests, reference data, proof of concept implementations, and analysis for Government owned CUI on Non-Federal Systems. Report on Collaborative activities as to deliverables and timelines.
4	National Defense Information Sharing and Analysis Center (ND-ISAC)	General &Technical	Publication	0	Page ii Audience	The use of the term perspective/perspectives is not definitive. NIST is not a regulatory authority and as a standards entity and laboratory shouldn t document perspectives.	Recommend adding a focus on definitions and terminology as established in CFR or International source(s) by establishing a partnership with external organizations willing to participate in a document inspection type activity. Statement on the two perspectives should be deleted or the nonfederal responsibility augmented by risk ownership. Appears the perspective commentary is focused on compliance over protection via security requirements.
5	National Defense Information Sharing and Analysis Center (ND-ISAC)	General, Editorial, & Technical	Publication	0	Page iii Note to Reviewers	Summary should be aligned with a published Errata and Redline Document	Provide mechanisms for review and participation by nonfederal entities on data collection, technical analysis, customer interaction, etc. to include trade-offs. As stated, "a summary of significant changes" with the term significant and deemed by the extensive overhaul, the publication should be supported with a detailed Errata and Redline for reviewers reference and time limited analysis.
6	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	0	Page iii Note to Reviewers	Term "customer" is vague in terms NIST/ITL and both federal and nonfederal entities to include representation	Define term "customer" or consider the term stakeholder
7	National Defense Information Sharing and Analysis Center (ND-ISAC)	General, Editorial, & Technical	Publication	0	Page iii Note to Reviewers, Bullet 1	Revision 3 should include mapping tables to ISO for global stakeholders	Include mapping source upon release of Revision 3 2nd public draft.
8	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	0	Page iii Note to Reviewers, Bullet 10 & 14	Appears redundant to Bullet 2	Delete or modify for intention
9	National Defense Information Sharing and Analysis Center (ND-ISAC)	General, Editorial, & Technical	Publication	0	Page iii Note to Reviewers, Bullet 11 & 12	The use of term recast for the security requirements conflicts with the difference in CUI data owner (federal) and risk owner (non-federal).	With NIST ITL's plan to utilize the CUI Overlay, work with global stakeholders to fast track the tool using the NIST Cyber Security Framework expending functional use of time and resources over publishing two or more major revisions that impact implementation and operational protections and extends timelines. Aligns with international entities providing flexibility delivering compatibility
10	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	0	Page iii Note to Reviewers, Bullet 5	Rephrase use of ODP	Collaborate with stakeholders to revise the statement to potentially redirect to - Introduced organization-defined parameters (ODP) in selected security requirements to increase flexibility, promote interoperability, and allow ~~help~~ non-federal organizations ~~better~~ manage risk as the asset owner.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
11	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	0	Page iii Note to Reviewers, Bullets 1, 2, 4-9, & 13	Modifications appear to be focused on compliance and embellishment (clarify, understanding, improve, help), signifying an attempt at a rebuttal for comments received over the years and from the open call for comments. The modification of the security requirements are representative of a regime change over clarity and betterment.	Update the change process for inclusion of global stakeholders, operational and maintenance data, and the varied asset types across ecosystems or scope to protection of Government CUI.
12	National Defense Information Sharing and Analysis Center (ND-ISAC)	General, Editorial, & Technical	Publication	0	Page iv Note to Reviewers	Changes in NFO, NCO, and CUI should be included in the Reviewers summary. All the changes are significant and should be of interest to NIST ITL.	The publication should be supported with a detailed Errata and Redline for reviewers and in this comment context in reference to changes and NFO, NCO, & CUI significance rationale.
13	National Defense Information Sharing and Analysis Center (ND-ISAC)	General & Technical	Publication	0	Page iv Note to Reviewers	The 60 day comment period granted to stakeholders is an inadequate process in comparison to a standards body and specifically NIST ITL's timeline of 2 years for the revision	Update the process with stakeholders across sectors, internationally, and vendors for protection of CUI on non-federal asset types
14	National Defense Information Sharing and Analysis Center (ND-ISAC)	General & Technical	Publication	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	Rewrite the document to agree with the purpose by removing the ODP and providing actual requirements
15	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	2	30	The scoping states that the requirements are ONLY applicable to systems that process, store, or transmit CUI or provide security for those systems. This creates inconsistencies throughout the publication and security concerns such as with limited inventory, logging, etc. based upon the assumptions and scoping. For example, the glossary says "system" but doesn't identify CUI but the scoping states "CUI".	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.
16	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	4	79	ODPs are identified as being defined by the federal agency with the FAQ identifying they can chose how/when/who defines but this leaves open lots of interpretation, adds inconsistencies, adds the potential for significant costs, and makes the ODPs as potential differentiators within RFI/RFPs which should not be the case for a baseline security configuration.	NIST or federal authority (NARA, OMB) should publish a baseline range and/or guidance for the ODPs that could/should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed but then should/could be additional requirements rather than changing the baseline. For example, for encryption/cryptography, publish guidelines for identifying strong crypto/encryption and not just pointing to the NIST 140-X series, but rather the steps to prove strong encryption/crypto. Another example would be the timeline ODPs would be defined as Annually at a minimum.
17	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	4	79	NIST not being part of the regulatory ecosystem creates problems within industry where expectations are not managed and/or tailoring becomes unsupportable and unsustainable.	NIST or CUI Federal Authority 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.
18	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	4	79	Allowing ODPs to define the requirements by program or ODP is a risk for the contractor and DoD and may push many vendors away from doing business with DoD. There are a number of these ODP provisions that will have extensive impacts on how the contractor operates their systems, the cost of operation, and the ability to functionally support those systems. In addition, who bears the cost of an ODP that changes the requirements from what was either originally set by the contractor or by another ODP? Also what happens to a certification that is gained under one set of parameters when an ODP requires those parameters to be changed? The way this is written shows there is sill a lack of understanding of how contractor systems are operated. They are not operated as enclaves for each contract. Most contractors use enterprise systems that support both their defense work and their non-defense work. So when an ODP requires changes to parameters, those changes impact the enterprise, including systems that are supporting other DoD contracts.	Remove the reliance on ODPs and either provide the minimum requirements or leave it to the contractor.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
19	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	4	96	**3.1.8 - Unsuccessful Logon Attempts (reference to ODP): ODP is specific to implementation and seemingly does not provide value as long as there is compliance with the control. ODPs define the number of unsuccessful log on attempts.** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	NIST should publish a baseline for the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed, or when operating system introduces limitations but others meets compliance requirements.
20	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	5	116	Some of the "new" (now explicitly called out) documentation appears to be overkill in a SMB environment. For example: **3.1.1 Account Management** – Define and document the types of system accounts allowed and prohibited.	Allow for more general account management to be defined in the SSP.
21	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	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
22	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	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
23	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	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
24	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	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
25	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	7	214	(SMB) Wording is not clear, could cause problems - recommend aligning with NIST 800-53 Rev 5	(SMB) "Identify and document [Assignment: organization-defined duties of individuals requiring separation]"
26	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	7	215	This control was noted as no significant change however previous wording did not require system access authorizations to be defined in support of SOD, only that the duties be separated	Review revised language and consider if the potential impact of this change aligns with the intent.
27	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	7	229	**Processes** is confusing 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.
28	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	7	230	(SMB) Is confusing and seems redundant with 3.1.5a	(SMB) recommend removing
29	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	7	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".
30	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	8	236	(SMB) This is very open. Since it says “as necessary” everyone will likely reply “yes, we do this” and also gives room to claim it was not necessary.	(SMB) Suggest adding definition of "frequency" [Assignment: organization-defined frequency] so there is some responsibility on the organization
31	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	8	252	3.1.6-Priviledged accounts should not be governed by the ODP requirements	Remove the ODP for this control requirement
32	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	8	254	(SMB) Seems unnecessarily complicated – recommend adhering to the original wording For original wording – recommend making the requirement clearer as the double use of “non” has always been a point of confusion.	(SMB) Require that users with privileged accounts do not use those accounts to perform their normal functions.
33	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	8	254	3.1.6-System accounts and access should not be governed by ODP requirements	Remove the ODP for this control requirement
34	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	9	293	3.1.8-How does limiting the invalid logon attempts and defined period being ODP help with CUI protection	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*
35	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	10	320	3.1.9-Device lock parameters should not be an ODP	Remove the ODP for this control requirement
36	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	10	320	Is this requirement meant to make it less secure by allowing a policy-only approach and relying on the user to lock their device? If that was the intent, this is okay. If not, this should be reevaluated.	Reevaluate if policy-only was not the intended approach, otherwise disregard
37	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	10	323	(SMB) It seems like overkill to require procedures for a user to unlock their device. Is the intent for a device lock to require a user to reauthenticate in order to unlock the device?	(SMB) Remove requirement for procedures and change wording to be more clear as to what is being asked since "retain the device lock" language is odd phrasing and obscure.
38	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	10	341	3.1.11-Terminate user session should not be an ODP	Remove the ODP for this control requirement
39	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	10	341	3.1.11-Terminate user session should not be an ODP	Recommendation -create a definition for "Session". There will be challenges with users who compile code and can't time out.
40	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	10	347	In this section, the use of the term "processes" is confusing. Throughout the publication, the terms processes, applications, system process, system services are commonly used but not clearly differentiated.	Please differentiate what is meant by "processes" in this section, or use a different term that is more clear. Please also define and differentiate these terms in the glossary ... process, system process, application, system service.
41	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	10	347	Processes is confusing for 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.
42	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	11	357	Some of the "new" (now explicitly called out) documentation appears to be overkill in a SMB environment. For example: **3.1.12 Remote Acces**s - Establish, authorize, and document usage restrictions, configurations, and connections allowed for each type of permitted remote access.	Allow for more general account management to be defined in the SSP.
43	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	11	364	Is this cryptography required to follow the other cryptography 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.
44	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	12	397	Is this cryptography required to follow the other cryptography/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.
45	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	12	417	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.	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.
46	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	12	417	Is this cryptography required to follow the other cryptography/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.
47	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	12	417	3.1.19 was incorporated into 3.1.18 but Mobile Computing Platform is not anywhere in the description or discussion.	Should add discussion relating to Mobile Computing Platforms or change Mobile Devices to Mobile Computing Platforms for broader usage.
48	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	12	417	3.1.19 was incorporated into 3.1.18 but Mobile Computing Platform is not anywhere in the description or discussion.	Define whether Mobile Computing Platforms are still in scope or out of scope as discussion for 3.1.18 doesn't appear to discuss platforms at all but only mobile devices.
49	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Needs coordinated with FEDRAMP requirements

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
50	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	13	455	No definition for Trust Relationships.	Please add a definition for "trust relationships" in the glossary.
51	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
52	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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?	Please clarify how this applies to authorized external systems such as in the case of DoD's new Zero Trust requirement. It is critical to incorporate Zero Trust into NISTs requirements for 800-171 and 800-53.
53	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
54	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	13	461	Why are cloud and services 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.
55	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	14	481	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?	Provide a definition for organization security policy and clarification regarding who, what, when, and where verification should come from.
56	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	14	481	Why isn't there an ODP on how often to verify controls such as annually?	Add ODP that requires re-assessment to verify security controls such as annually
57	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
58	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	14	485	3.1.21-Portable storage devices should not be controlled by ODP as it will restrict organizations business functions if too restrictive	Remove the ODP for this control requirement
59	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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.
60	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	14	500	Why isn't there an additional assessment objective to review content prior to publishing on public domain.	Add additional objective to Control and Review content for CUI prior to posting on publicly accessible system.
61	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	14	500	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.
62	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
63	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	15	512	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? Forcing 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.
64	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	15	513	(SMB) We are wondering what the anticipated response is for most organizations. This is written in a way that is very open (ex. Org could specify over a week).	(SMB) No change, conveying our response on reading
65	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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	Remove the ODP for this control requirement
66	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	15	524	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?	Define Literacy Training Make consistent and define all terms Add awareness to a.
67	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	15	524	**3.2.1 Literacy Training and Awareness (reference to ODP) - ODPs define how often training material needs to be reviewed and updated.** ODP infringes upon contractor's Corporate policies and procedures.	Where a timeline is mentioned - the ODP should be set at annually or refer to contractor's existing policies (whichever is more frequent).
68	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Training 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
69	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	15	526	(SMB) 3.2.1 and 3.2.2 L- ODP for roles is a challenge - allow organization to define - event driven ODPs are harder - provide examples of "events" - suggestion - during an after action - decide if training should be updated	(SMB) Either state the required frequency or leave it to the contractor
70	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	16	552	Why doesn't this have Literacy as part of the training discussion?	Make consistent and define all terms
71	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	16	552	**3.2.2 Role-Based Training (reference to ODP) - ODPs define how often training material needs to be reviewed and updated.** ODP infringes upon contractor's Corporate policies and procedures.	Where a timeline is mentioned - the ODP should be set at annually or refer to contractor's existing policies (whichever is more frequent).
72	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
73	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	16	577	Why does 3.2.3 exist when Advanced Literacy training is discussed in 3.2.1? Why doesn't this have an ODP?	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.
74	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	16	577	Why doesn't this have an ODP?	Add an ODP

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
75	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	16	592	Adding social engineering and social mining to the insider threat control is good. Before this, no mention of phishing.	No Change
76	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	17	597	Social engineering and social mining defined in previous sentence, data mining not defined.	Replace "data mining" with "social mining" on line 597.
77	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	17	603	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	Either state the required frequency or leave it to the contractor
78	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	17	603	Dictating all the possible event types by an organization can be very cumbersome with different interpretations between organizations.	Recommend removing the ODP from part a. Also, change "remains necessary and sufficient" to "remains relevant and sufficient.".
79	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	17	603	**3.3.1-3.3.9 Audit & Accountability (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define event types, audit record content, retention time, alerting procedures, frequency of reviews, etc.** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	NIST should publish a baseline for the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed, or when operating system introduces limitations but others meets compliance requirements. (where a timeline is mentioned - annually should be set as the baseline)
80	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	17	603	Why was this worded this way? Why not reword to have the ODP?	Reword to "Specify [ODP] for logging within the system"
81	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
82	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	17	625	The wording is confusing	Change "necessary" to "relevant"
83	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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"
84	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 the ODP for this control requirement
85	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	18	664	(SMB) 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	(SMB) Contractor organization defines how we review (whether automated or a person)
86	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	19	680	What defines inappropriate or unusual activity?	Add an ODP for inappropriate and unusual activity.
87	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	19	680	In 3.3.5, How do we define systems that actually store process and CUI and "or that provide protection for such components."? For e.g., How should a SIEM be treated as, as it does not, for the purpose of this discussion, store, process, transmit CUI? As part of scoping, it is important to define the specific protections that are needed, including the requirements for systems that are specific to the implementation, such as Cloud SaaS.	Need clear, consistent, and easily understood guidance for components to ensure that we have reasonable assurance that it is doing its capability correctly.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
88	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 not related to any one specific contract	Remove this statement. Allowing ODP to define this can create conflicts with other USGOV reporting requirements and may cause issues related to multiple contracts for non-DoD work on contractor systems
89	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	19	683	What is a finding?	Add clarity or change wording to "inappropriate or unusual activity" instead of "findings"
90	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	19	705	What is definition of on-demand and why does it have to be on-demand?	Remove "on-demand".
91	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 "authoritative time source" back into the requirement.
92	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
93	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	20	741	In 3.3.8, "Protect audit information…." request clarification. How do we define the minimum level of protection requirements that a component has to meet based on the architecture, the capability being provided and used. For example, in a SIEM, we need to ensure (a) that the component generating the log files does not allow modification of log files, and (b) the capability that is analyzing the log files allows no changes to those files.	We need to assess assets that provide security protections based on the functions that the SPA provides and not required to implement all controls that apply to assets the S/P/T CUI. Please clarify the assessment requirements for components that are in scope because they provide protections to assets that do handle CUI.
94	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	21	754	For consistency, why isn't an ODP defined here for the subset of users?	Rewrite and replace "subset of privileged users or roles" to ODP with users and roles.
95	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
96	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 ODP is a significant risk to the contractor	Either state the required frequency or leave it to the contractor
97	ND-ISAC Small and Medium Business (SMB)	Technical	Publication	21	783	(SMB) **3.4.2 Configuration Settings (reference to ODP)** - ODPs define common secure configurations. This opens up agencies to add to the regulatory requirement (which DoD is prone to do). Requirements of Prime Contractors are not necessarily requirements of subcontractors. Lower tiers would be subject for what the higher tiers are subject to. Depending on the STIG, if it becomes part of the ODP, there could be a tremendous amount of burden to SMB.	(SMB) Remove ODPs unless absolutely vital (and consistent), and clarify which tiers are responsible for meeting.
98	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	21	783	**3.4.2 Configuration Settings** – "common secure configs" - this should not be defined in the discussion section. Terms should be defined in the Glossary.	Formally define term in Glossary
99	ND-ISAC Small and Medium Business (SMB)	Technical	Publication	21	783	(SMB) **3.4.2 Configuration Settings** – "common secure configs" - this should not be defined in the discussion section. Terms should be defined in the Glossary.	(SMB) Allow contractor defined security configuration standards they follow - but not mandated by government (e.g., follow the STIGS)
100	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
101	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
102	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	21	784	3.4.2.a-This allows the ODP to redefine what a secure configuration is. In addition the statement "ODP 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.
103	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	22	814	Rewrite as an ODP for consistency	Rewrite a as an ODP for consistency
104	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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	Add or modify ODP to require org-defined approvers
105	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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.
106	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	23	862	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 protocols used, the program execution parameters, or the system review requirements	Leave this to the contractor. Remove the ODP for this control requirement
107	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	23	862	**3.4.6 Least Functionality (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define ports, functions, protocols that are prohibited.** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	NIST should publish a baseline for the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed, or when operating system introduces limitations but others meets compliance requirements.
108	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	23	862	Why isn't this an ODP such as Org-defined capabilities?	Change to ODP for defining missing-essential capabilities
109	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	23	862	(SMB) Why isn't this an ODP such as Org-defined capabilities?	(SMB) Allow contractor organizationally defined parameters - ports and protocols, policies, etc. NOT Federal definition
110	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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).
111	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	24	895	**3.4.8 Authorized Software -** Allow by Exception - blacklisting is no longer allowed, only whitelisting. In a SMB environment, particularly a small manufacturer or job shop with many customers across many industries, working in an enterprise environment, this is extremely burdensome. Implementing an “Allow List” only is a large impact for small businesses that will require on-boarding more technical implementations. If resources are available for this, setup can be relatively easy, but maintenance – especially in a SMB environment – is not.	Allow blacklisting.
112	ND-ISAC Small and Medium Business (SMB)	Technical	Publication	24	895	**(SMB) 3.4.8 Authorized Software -** Allow by Exception - blacklisting is no longer allowed, only whitelisting. In a SMB environment, particularly a small manufacturer or job shop with many customers across many industries, working in an enterprise environment, this is extremely burdensome. Implementing an “Allow List” only is a large impact for small businesses that will require on-boarding more technical implementations. If resources are available for this, setup can be relatively easy, but maintenance – especially in a SMB environment – is not.	(SMB) Allow whitelisting; the cyber risk is lower in small organizations that use cloud only solutions. Updating and managing a whitelist is time-consuming for Small Businesses who have limited resources.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
113	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Remove the ODP for this control requirement
114	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	25	924	(SMB) User-Installed Software a. Establish policies governing the installation of software by users. b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]. c. Monitor policy compliance [Assignment: organization-defined frequency].	(SMB) Recommend clarifying definition of "Method". Is "Method" a technical control or is a policy sufficient in the example of "b". Depending on the "method" used to control user installed software, it may have a dependency on the frequency to monitor. As such it should be left to the DIB to determine frequency.
115	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	25	940	Why only system components and not a full inventory list?	Add/modify previous requirements to identify the need to have a complete inventory.
116	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	25	940	System component is confusing as it seems to be what is in the systems and not the systems themselves.	Change the requirement to be "System and System Component Inventory"
117	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	26	958	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.
118	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	26	959	3.4.11-Is this control defining the restriction for data sovereignty and nationality requirement for accessing the CUI data	Provide more guidance on what details are required for this control
119	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	26	959	(SMB) This is written broadly so that an org could specify that their entire network is suitable for CUI, could provide entire staff list, could provide high-level list of changes to overall system. "System components" is present in the discussion but not in the requirement. Adding the word "component" to the language would completely change the requirement.	(SMB) If the intent is to get a specific inventory, selective list of users and changes, this would need to be made more clear and use less open-ended language (e.g., asking for system components)
120	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	26	971	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?	Re-word line 972 a. "The contractor defines countries that are 'high risk areas' and implements controls to limit the amount of CUI and proprietary 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."
121	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	26	971	Terminology is conflicting/confusing - **3.4.12 High Risk** - Issue [Assignment: organization-defined system] with [Assignment: organization-defined system configurations] to individuals traveling to locations that the organization deems to be of significant risk. Is the word usage of the 3rd organization Federal or the contractor?	Use different terminology when actually referring to the contractor s organization and not an Organization-Defined Parameter (ODP) where the organization is a Federal agency.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
122	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	26	971	Why isn't there an ODP that defines areas/locations of significant risk?	Modify/add ODP that defines the areas/locations of significant risk
123	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	26	972	"Organization Defined System" is not listed in the glossary.	Define "Organization Defined System" in the glossary
124	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Remove the ODP for this control requirement
125	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	27	993	User Identification, Authentication, and Re-Authentication a. Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users. b. Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication].	Please confirm how this is intended to be applied to legacy automated systems that are running processes behind the scenes. Example - applications that monitor a process and then generate an email alert informing of a failure. How does this apply to those automated type processes. General statement: DIB contractors should define "circumstances" or "situations".
126	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	27	993	3.5.1.b-Allowing ODPs to redefine the requirements for re-authentication can be very disruptive to the operations of the contractor	Either state the required frequency or leave it to the contractor. Remove the ODP for this control requirement
127	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	27	993	The use of processes is confusing to many users. Tense of nouns should be consistent as it says authenticate system user but then says acting on behalf of users.	Rewrite as "system processes" to differentiate from "workflow processes". Change "system user" to "system users" for consistency with the rest of the requirement objectives or change "users" to "user" in all instances.
128	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
129	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	27	1011	3.5.2-This is really unclear what the ODP is intended to define	Leave this to the contractor. Remove the ODP for this control requirement
130	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	27	1011	(SMB) Device Identification and Authentication Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a system or network connection.	(SMB) Federal agencies should not define this ODP. Recommendation: suggest products that could help with this requirement
131	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
132	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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.
133	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	27	1025	**3.5.3 MFA** - Multifactor authentication for all access can be costly and cumbersome in a SMB environment. Additionally, not all software supports MFA.	Allow for exceptions to MFA, referencing other ways to mitigate risk when software or application is otherwise compliant.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
134	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	27	1026	How is "System Account" defined?	Define what a "System Account" is in the control and the glossary.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
135	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	28	1049	**3.5.5 Identifier Management** is burdensome to SMB. There will be a need to change account naming conventions to include nomenclature that identifies non-employees with corporate accounts.	This is overkill. Remove the requirement.
136	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	28	1049	**3.5.5 Identifier Management** is burdensome to SMB. d. Identify the status of each individual with the following characteristic: [Assignment: organization-defined characteristic].	Federal agencies should not define roles. Assumption "d" means "active" "inactive" etc.,,, please provide examples.
137	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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?	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.
138	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	28	1049	Why is unique not listed anywhere in this requirement?	Add "to assign a unique identifier" to the different requirement. B. should be "select and assign a unique identifier …"
139	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Remove the ODP for this control requirement
140	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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).
141	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
142	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	29	1069	**3.5.7 Password Management (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define composition and complexity rules – What if system cannot support? Microsoft only enforces 8 characters in Azure AD.** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	NIST should publish a baseline for the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed, or when operating system introduces limitations but others meets compliance requirements.
143	ND-ISAC Small and Medium Business (SMB)	Technical	Publication	29	1069	(SMB) **3.5.7 Password Management Password Management.** Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords.	(SMB) Recommend providing examples for how to achieve "c".
144	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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"
145	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	29	1069	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	Remove "including spaces and all printable characters" from the requirement
146	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	29	1069	Does the cryptographically protected channels fall into the cryptography requirements in this document? If so, that should be reiterated.	Reiterate that the cryptographically-protected channels have to meet the cryptography requirements in the requirements.
147	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
148	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	29	1070	(SMB) 3.5.7.a is at the top of the requirement while what it is pulling from (IA-5(1)h) is at the bottom of the control. From the perspective of someone who has to maintain multiple SSPs this mis-alignment seems unnecessary and is burdensome when trying to keep answers consistent between SSPs.	(SMB) Recommend aligning closer to 800-53 Rev 5 and keeping the 171 requirement and 800-53 control objectives in the same order
149	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	29	1072	In 3.5.7 "b. Allow user selection of long passwords and passphrases, including spaces and all printable characters.", some systems just cannot allow them due to technical limitations and/or government policy.	Delete "b." as it is redundant to "a. Enforce the following password composition and complexity rules: [Assignment: organization defined composition and complexity rules]."
150	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	29	1072	Not every system still supported and in use can accept long passwords and all printable characters	Leave this to the contractor. Remove the ODP for this control requirement
151	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	29	1072	In 3.5.7 "b. Allow user selection of long passwords and passphrases, including spaces and all printable characters.", some systems just cannot allow them due to technical limitations and/or government policy.	Delete "b." as it is redundant to "a. Enforce the following password composition and complexity rules: [Assignment: organization defined composition and complexity rules]."
152	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	29	1074	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.
153	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	29	1074	(SMB) "The list of commonly-used, expected, or compromised passwords" should be a requirement if we expect users to have access to/use one. The requirement references "the list" without establishing what it is. We had multiple questions while reading this - is this a common reference we should be using? Is this a list we are expected to develop and update based on our experience? We assume this is something that the organization should make on it own although the requirement does not make this clear.	(SMB) Recommend aligning more with IA-5(1)a "Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;"
154	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
155	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	30	1116	Why aren't "shared" accounts not discussed and only "group" or "role" accounts?	Add "shared" to the types of accounts for consistency with other requirements.
156	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	30	1116	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."
157	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	30	1118	This control could be interpreted to mean Identity Proofing which could be costly for Contractors to implement depending on the Assurance Level needed to meet this requirement.	Revise language to "Ensure the identity of the individual, group, role, service, or device receiving the authenticator has been validated as part of the initial authenticator distribution."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
158	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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"
159	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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."
160	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	30	1124	(SMB) In 3.5.12 "f. Change or refresh authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events]." For organizations that are moving to passwordless environments, all references to passwords are moot.	(SMB) Suggest defining examples of organization-defined events. Federal government should not identify defined-events.
161	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	30	1124	In 3.5.12 "f. Change or refresh authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events]." For organizations that are moving to passwordless environments, all references to passwords are moot.	Refer to discussion on ODPs, as you may have conflicts. Add a definition for term "authenticator".
162	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Remove the ODP for this control requirement
163	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	31	1171	**3.6.2 Incident Monitoring, Reporting, and Response Assistance (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define who you report to – Reporting comes from higher regulations (DFARS, etc.), allowing customer to define gets unruly when working with multiple customers with varying options on who needs to be informed.** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	Reference regulations that the contractor is beholden to.
164	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	31	1173	DFARS 7012 and the NISPOM already define the reporting requirements.	Remove the ODP for this control requirement
165	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	31	1174	What evidence will the C3PAO be looking for this control?	Make sure to include evidence types that will satisfy this control for 3.6.2
166	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Remove the ODP for this control requirement
167	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	32	1210	3.6.4-Allowing each ODP to redefine the incident response training requirements is unnecessary.	Leave this to the contractor. Remove the ODP for this control requirement
168	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Remove the ODP for this control requirement
169	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	34	1272	This requirement seems to be overly broad especially with the additional of "technical competence" required for supervising maintenance activities. This could become 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 knowledgeable 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.
170	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. 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*
171	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Remove the ODP for this control requirement
172	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	36	1351	In 3.8.5, "Media Transport a. Protect, control, and maintain accountability for system media containing CUI and during transport outside of controlled areas. b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI stored on digital media during transport."	significant change as there is no "or" between "a" and "b"
173	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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.
174	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	36	1351	**3.8.5 Media Protection** was encrypt OR physically protect. Now, the updated requirement is "encrypt AND physically protect." This is overkill.	Allow for encryption OR physical protection.
175	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.	Add an ODP for controlled areas that mirrors 3.8.4
176	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	36	1351	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 call out to 3.13.11 in the discussion regarding approved cryptography within the discussion to identify that it is related.
177	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	36	1354	3.8.5-There are occasions 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
178	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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
179	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 consistent to the new wording in a.
180	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	37	1374	Why doesn't b. have the same "Selection: Restrict; Prohibit" as a. since they are interrelated?	Add "Selection: Restrict; Prohibit" to b
181	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
182	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Remove the ODP for this control requirement
183	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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	Add call out to 3.13.11 in the discussion regarding approved cryptography within the discussion to identify that it is related.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
184	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	37	1399	The discussion identifies that "alternate physical controls" is acceptable but that is not what the requirement states.	Change the requirement to "implement cryptographic mechanisms or alternate controls .." in the requirement to be consistent with the discussion.
185	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
186	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	38	1425	**3.9.2 Personnel Termination and Transfer (reference to ODP): ODPs define when system access is disabled and when transfer actions are taken.** ODP infringes upon contractor's Corporate policies and procedures.	Where a timeline is mentioned - the ODP should be set at annually or refer to contractor's existing policies (whichever is more frequent).
187	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	38	1425	Why doesn't b have a ODP time period for reviewing and confirming the need for access?	Add ODP for b. 1. for time period review.
188	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	38	1425	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.	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.
189	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	38	1427	3.9.2-System access disablement and action initiation are driven by the standing KR systems and processes. To allow each ODP to redefine these time periods may require significant changes to the KR systems and processes for each ODP	Either state the required frequency or leave it to the contractor
190	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
191	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	39	1457	**3.9.3 External Personnel Security/3.16.3 External System Services** – "external providers", "external system service" – NIST should formally define these terms in the Glossary. This is an important definition as other entities have competing definitions and will certainly impact industry going forward.	Formally define terms in Glossary
192	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.	Redefine this requirement to differentiate the types of roles that would be required for these vs just stating all external providers.
193	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	39	1457	Why are there no ODP for time periods for reviewing compliance?	Add ODPs for timeframes for reviews and monitoring of compliance.
194	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	39	1457	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	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
195	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	39	1457	Companies will be required to document the external providers security requirements including security roles and responsibilities. In addition, it will require them to monitor compliance.	The control does not limit the requirement to contractors on site nor with organization network access. The requirement does not have any clarifications regarding whether they are handling CUI or not. The definition of External Provider is overly broad and does not specify which roles of an External Provider is included. The existing requirements in 3.9.1 and 3.9.2 have been difficult to manage with contractors.
196	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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"
197	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.	Change b to state "Require authorization credentials for physical location access"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
198	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.	Need to define "facility" and "physical location(s)"
199	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.	c. should change "facility" to "physical location(s)"
200	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.	d. should change "facility" to "physical location(s)"
201	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	39	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"
202	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 employees
203	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	40	1516	The updated language does not make it clear if each alternate work site must be individually identified and documented or if the intent of the control is to identify broad categories/types of alternate work sites. For example, does each employee residence need to be documented for teleworking purposes?	Revise language to "Determine and document criteria for types of alternate work sites allowed for use by employees."
204	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. Remove the ODP for this control requirement
205	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
206	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	41	1530	There doesn't appear to be 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]"
207	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 systems to satisfy the desires of each ODP	Leave this to the contractor. Remove the ODP for this control requirement
208	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	42	1555	**3.10.8 Access Control for Transmission and Output Devices** – "output devices", "system distribution", "transmission lines" - this should not be defined in the discussion section. Terms should be defined in the Glossary.	Formally define terms in Glossary
209	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
210	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	42	1556	In 3.10.8, "a. Control physical access to system distribution and transmission lines within organizational". Please clarify if we need to harden transmission lines, or add additional physical protections (e.g., drop ceiling not enough and we need conduits or PDS)? How do we address employees working from home/remote locations? Second, the terms "system distribution and transmission lines", "output devices" must not be defined in the control discussion. It needs to be formally defined.	Change from "within organizational facilities" to "external" as it is not clear if we should be looking at lines going outside the building or those within. If the word "may" is used in sentence "Security controls used to control physical access to system distribution and transmission lines **"may"** include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors", it makes it more optional than required. Add definitions to terms used in the control and control descriptions to clearly indicate what they mean.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
211	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.	Revert back to the original requiring risk assessments to flow with many of the other requirements. Otherwise, the overall intent is lost
212	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	42	1576	With the new wording of a, b seems to only affect assessments of unauthorized disclosure so limited in scope and applicability.	Revert back to the original requiring risk assessments to flow with many of the other requirements. Otherwise, the overall intent is lost
213	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	42	1576	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	If this is the intent of the new requirement, update the Discussion to highlight the limited scope
214	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
215	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
216	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	43	1600	In 3.11.2, "a. Monitor and scan for vulnerabilities in the system [Assignment: organization-defined frequency] and when new vulnerabilities affecting the system are identified." Clarify "Monitor" as the discussion describes scanning in detail but not the expectation for "monitor". Clarify how this relates to. or is different from 3.14.1. In modern technologies that monitor (e.g., Crowdstrike), they may not scan periodically (e.g., like a vulnerability scan tool). Most new next-gen behavioral/ai based endpoint protection tools do not scan routinely, they scan on add/change to files.	Recommend use of "and/or", or deconflict with 3.14.1, or combine them to include scan, monitor, update, implement, etc. In addition, the use of the term "system" seems to change according to context, and replace with "component" where appropriate.
217	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 organization and the ability to digest the scan results	Leave this to the contractor. Remove the ODP for this control requirement
218	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 contractual problems or operational problems for the KR	Leave this to the contractor. Remove the ODP for this control requirement
219	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	43	1605	In 3.11.2.d should be removed. Privileged access requirements are covered elsewhere and the doc should not set requirements for use of specific software.	Remove d.
220	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	44	1638	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
221	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	44	1638	There is no direct relationship to risk in the requirement.	Add "risk" into the requirement such as with "Respond to findings from risk and security assessments, monitoring, and audits"
222	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	44	1639	(SMB) Language here is open and vague	(SMB) Recommend rewriting to more closely adhere to the NIST 800-53 Rev 5 language
223	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
224	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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?	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.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
225	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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.
226	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
227	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	45	1681	This requirement now changed from POAMs for requirements not met to POAMs for the normal monitoring and remediation processes of the system.	Better clarity and/or association with other requirements, especially for vulnerability remediation, should be in the discussion.
228	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 continuous monitoring (i.e., vulnerabilities) vs unimplemented security controls (missing requirements) and thus are inconsistently 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.
229	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	45	1686	3.12.2.b-POAM update requirements will be covered based on assessment. CMMC, CSF, RMF, other certification or frameworks may have defined POAM update requirements. To allow ODPs to redefine this may disrupt other certification processes	Remove the ODP for this control requirement
230	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	45	1701	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.
231	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	45	1701	The Discussion states that "ongoing" and "continuous" imply that an organization assesses and monitors at a frequency sufficient to support decisions.	Change to an ODP to define the frequency for monitoring for the ODP types of controls to identify how different controls require different frequencies.
232	ND-ISAC Small and Medium Business (SMB)	Editorial & Technical	Publication	45	1701	(SMB) Expectation of "system-level continuous monitoring strategy" is not clear. What is expected of those implementing Rev 3? This is very open and hard to understand how to take action on the requirement.	(SMB) Recommend adding clarifying language so there are clearer requirements for what the continuous monitoring strategy must include. Rev 5 goes further into detail so that may be helpful here.
233	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	46	1716	Can the internal auditor perform this assessment, or does it need to be an external provider, like a C3PAO? SMBs can find this cost prohibitive due not having an internal audit team.	Clarify this control with regards to whom 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.
234	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	46	1716	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: 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.
235	ND-ISAC Small and Medium Business (SMB)	Technical	Publication	46	1716	(SMB) **3.12.5 Independent Assessments** - 800-53 references "annual" assessments. There should be clarification on Independent Assessments should take place. Per 800-53, regulatory agencies are outside the scope of control. This means the CMMC Assessment is not part of the control. The cost of assessments would be a huge cost burden on SMB if required in NIST 800-171	(SMB) Do not require assessments as part of NIST 800-171. Allow agencies to drive this.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
236	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	46	1716	The wording in the discussion highlights that small organizations or organizations without any independent assessment org must use a 3rd party to assess which then significantly raises the costs of doing business with the government.	Better clarity or the ability to provide attestations/assessments by internal groups for an organization should be allowed especially if a frequency for review is yearly or less.
237	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	46	1716	There is no frequency defined for these independent assessments so it is left to interpretation instead of defining	Add ODP for frequency of assessments
238	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 assessors before Audit?	Having an additional assessment prior to audit will be a huge burden on the control owners plus will have monetary implications
239	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	46	1730	**3.12.6 Information Exchange (reference to ODP) - ODPs define what and how often agreements need to be reviewed and updated.** ODP infringes upon contractor's Corporate policies and procedures.	Where a timeline is mentioned - the ODP should be set at annually or refer to contractor's existing policies (whichever is more frequent).
240	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
241	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
242	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	46	1731	3.12.6-CUI exchange 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 the ODP for this control requirement
243	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	46	1750	The discussion bringing up Intra-system connections seems very arbitrary and adds confusion to what is in scope for this requirement.	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 .. "
244	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	46	1750	**3.12.7 Internal System Connections (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define system components or classes of components – For internal systems? Every contractor will have different classes of components. There is no way to apply uniformly to all contractors.** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	NIST should publish a baseline for the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed, or when operating system introduces limitations but others meets compliance requirements.
245	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	46	1750	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 update the other requirements or update the discussion to relate how this requirement is different than the others and how they interrelate.
246	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	46	1750	Should this say "authorize and manage"?	Change to "Authorize and manage internal system connections .. "
247	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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)
248	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	46	1751	3.12.7-KRs already have processes for approving internal systems 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 the ODP for this control requirement
249	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	46	1751	3.12.7-What does authorize mean here for system connections. Does it require 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

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
250	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
251	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
252	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	47	1769	Why was "protect" removed?	Identify why "protect" was removed from the old requirement.
253	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
254	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	47	1769	The entire discussion paragraph on shared commercial telecom 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.
255	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
256	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 parameters, etc. to help in understanding as well as to identify how COTS software/OS/HW may not allow for typical changes by an organization.
257	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
258	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	49	1845	**3.13.7 Split Tunneling (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define the safeguards - What if one customer says use a VPN and another says do not use a VPN?** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	NIST should publish a baseline for the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed, or when operating system introduces limitations but others meets compliance requirements.
259	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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. 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

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
260	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	49	1846	In 3.13.7 Split Tunneling on lines 1846-1847. "Prevent split tunneling for remote devices unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards]." Lines 1860-1863 go on to explain that "A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments or to a specific set of pre-approved addresses without user control." There are lots of ways to fill that assignment, and different CO s or agencies could give conflicting answers that are mutually incompatible with each other. What if one agency or branch says that their "organization-defined safeguard" is to only permit access to US-hosted resources? Meanwhile, a different branch has adopted 800-207 and is collaborating with the UK MoD (say, for F-35, or E7) and expects DIB contractors to not use VPN at all, but instead connect directly to an "external" shared collaboration service in the UK? How is a contractor to meet both conflicting requirements?	The safeguards can not be dictated by each contract, it only works if they are selected and defined by the Non-Federal Organization
261	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 the ODP for this control requirement or refer to change above "The safeguards can not be dictated by each contract, it only works if they are selected and defined by the Non-Federal Organization" - 3.13.7 is one example of many that signifies the issue and concerns with ODP requirements and management.
262	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	49	1867	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.
263	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	49	1867	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.
264	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	49	1867	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.
265	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	49	1867	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.
266	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	49	1867	In 3.13.8, removal of " unless otherwise protected by alternative physical safeguards" and addition of "...and while in storage." is a new requirement for encryption for data at rest during storage and a significant change. Previously, data center protections were good enough.	Non-reliance on physical safeguards introduces
267	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	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)
268	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	49	1867	**3.13.8 Transmission and Storage** - Removed "unless otherwise protected by alternative physical safeguards" and added "while in storage" – This is a significant cost increase to SMB to obtain FIPS validated crypto in storage. This is not value added.	This is overkill. Remove the requirement.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
269	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	49	1867	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.	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)
270	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	49	1868	3.13.8-This control adds a requirement 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. Servers in the KR datacenter that have adequate physical protections should not be mandated for encryption at rest, and many current file storage systems cannot support this.
271	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 the ODP for this control requirement
272	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
273	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	50	1903	3.13.10-KRs will have established key management and regeneration criteria established based on KR systems and requirements. To allow each ODP to redefine this will be impossible for the KR to manage	Remove the ODP for this control requirement
274	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	50	1915	FIPS validated ODP leaves the usage of multiple of algorithms.	Suggest using NSA and FIPS validated algorithms.
275	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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.	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.
276	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	51	1915	**3.13.11 Crypto (reference to ODP) – Although FIPS was taken out of the control, ODPs define the type of crypto and the discussion references still point to FIPS documentation. Agencies will fall back on FIPS as that is their requirement and they know nothing else.** Requirements of Prime Contractors are not necessarily requirements of subcontractors. Lower tiers would be subject for what the higher tiers are subject to.	Remove ODPs unless absolutely vital (and consistent), and clarify which tiers are responsible for meeting.
277	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	51	1915	The discussion doesn't identify the relationship with the other cryptographic requirements.	Update discussion with relationships with other requirements.
278	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	51	1915	The discussion 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.	Update the discussion to provide guidance on identifying strong cryptography.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
279	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	51	1915	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.	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.
280	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	51	1915	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 algorithms or FIPS compliant modules with strong key management. ITAR is only requiring FIPS compliant.	Change the encryption requirements to identify FIPS compliant with strong key management is considered strong encryption and cryptography rather than FIPS validated.
281	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	51	1916	3.13.11-To allow each ODP to redefine the types of encryption to be used will be impossible for the KR to manage, particularly in enterprise systems	Remove the ODP for this control requirement
282	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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".
283	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	51	1927	3.13.12-To allow each ODP to define the requirements for remote activation of collaborative systems could easily make it impossible for a KR to initiate a collaborative call session as these frequently require remote activation	Leave this to the contractor. Remove the ODP for this control requirement
284	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	51	1940	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.
285	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	51	1940	Some of the "new" (now explicitly called out) documentation appears to be overkill in a SMB environment. For example: **3.13.13 Mobile Code** - Define acceptable and unacceptable mobile code and mobile code technologies.	Define acceptable and unacceptable mobile code technologies.
286	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	51	1940	**3.13.13 Mobile Code** – “mobile code” - The definition in glossary and definition in discussion are not the same.	Formally define terms in Glossary
287	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	51	1940	The discussion should be updated to more user friendly examples such as PDFs and Macros.	Update the discussion with better every day examples such as PDFs and Macros.
288	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
289	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
290	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	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. 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 implementation.	Remove the requirement or remove the technology specific requirement. 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".

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
291	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	52	1972	**3.13.17 Internal Communication** uses outdated language: "authenticated proxy server." Control does not align w/modern network management such as transparent web filters or next gen firewall (NGFW)	Update language, align with modern network management.
292	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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"
293	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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?	Highlight the inconsistencies between requirements and how they interrelate.
294	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	52	1972	The requirement is technology/solution specific and should be changed.	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"
295	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	52	1973	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.	Remove this. 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 unnecessary cost. The costs greatly exceed any potential risk mitigation already found elsewhere.
296	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	53	1993	What is the number that this should be limited to?	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.
297	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	53	1993	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.	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.
298	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
299	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	53	1993	The discussion creates confusion and needs to be rewritten.	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.
300	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	53	1994	3.13.18-There is no defined limit for this control which has been defined. Is the number of connections left to organizations to define and manage	Provide more guidance on what details are required for this control
301	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	53	2006	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 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.	Modify b. with and ODP that is requiring the testing for Critical and Key systems.
302	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	53	2010	3.14.1-Installation of software 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. 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*
303	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	53	2010	**3.14.1 Flaw Remediation - (reference to ODP)** - In section "c" - the ODP related to the time allowed to install security-relevant software and firmware updates is problematic. SMBs with limited resources may be limited in time, or manufacturing facilities may need to take production down or manage this during planned maintenance, which could fall beyond the ODP parameters.	Remove ODP. This is not a way to standardize this.
304	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 a. for designated locations/boundaries.
305	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
306	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	54	2028	The second paragraph is good information but extraneous to the requirement and should be removed.	Remove the second paragraph under Discussion.
307	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	54	2031	In 3.14.2 "b. Update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures."	Use a different term for "organization" in two different contexts to avoid confusion with ODPs. Suggest other terms such as ""
308	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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
309	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	54	2057	The example in Discussion implies that response activities should include notifying external organizations which is not part of the requirement. It is a good practice but now it becomes additional requirement to notify external entities. This example should be modified as an internal example and refer to incident response management for anything externally.	Change the example to reflect an "internal" example and remove the "external" example as that causes confusion and adds to the requirement by inferring the reporting to external entities.
310	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	55	2077	The discussion should relate to the other requirements that do very similar actions (i.e., detecting unauthorized use, logging, etc.)	Update the discussion to identify the relationship between relevant requirements such as in the AC, IA, and AU domains.
311	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	56	2114	In 3.14.8 Spam Protection - this requirement should be removed.	Spam is an annoyance but is not a direct threat to CUI.
312	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	56	2114	**3.14.8 Spam** - Control is irrelevant to protection of CUI.	Remove control, spam is an annoyance but not a direct threat to the confidentiality of CUI.
313	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	56	2114	What is the definition of Spam?	This needs defined to help understand how to meet the requirement
314	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
315	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
316	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
317	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	56	2117	3.14.8-To allow each ODP to redefine spam protection updates will be disruptive to KR operations	Leave this to the contractor. Remove the ODP for this control requirement
318	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	56	2127	**3.15.1 Policy and Procedures (reference to ODP) - ODPs define how often CUI policy and procedures need to be reviewed and updated.** ODP infringes upon contractor's Corporate policies and procedures.	Where a timeline is mentioned - the ODP should be set at annually or refer to contractor's existing policies (whichever is more frequent).
319	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	57	2143	**3.15.2 System Security Plan (reference to ODP) - ODPs define how often SSP needs to be reviewed and updated.** ODP infringes upon contractor's Corporate policies and procedures.	Where a timeline is mentioned - the ODP should be set at annually or refer to contractor's existing policies (whichever is more frequent).
320	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	57	2148	3.15.2-SSP update frequency will likely be covered by CMMC or other certification criteria. To allow ODPs to redefine these requirements is duplicative and unnecessary	Remove the ODP for this control requirement
321	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	57	2165	**3.15.3 Rules of Behavior (reference to ODP) - ODPs define how often rules of behavior needs to be reviewed and updated.** ODP infringes upon contractor's Corporate policies and procedures.	Where a timeline is mentioned - the ODP should be set at annually or refer to contractor's existing policies (whichever is more frequent).
322	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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.
323	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	57	2165	The discussion should relate back to 3.1.9.	Update the discussion to relate to 3.1.9
324	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
325	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	57	2168	3.15.3-KRs will already have established processes for updating any required rules of behavior so to allow each ODP to redefine this is unnecessary	Remove the ODP for this control requirement
326	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	58	2199	**3.16.2 Unsupported System Components** - requiring unsupported systems to be replaced is extremely burdensome to SMB. In a manufacturing environment, many machines costing hundreds of thousands of dollars may not "talk" to the latest Operating Systems but are machines producing validated and conforming quality product.	There are other measures to consider to mitigating these risks. Remove the requirement to replace unsupported systems, or include risk mitigation requirements to allow for unsupported systems.
327	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	58	2199	This needs to be rewritten to identify how risk is managed and unsupported components are managed.	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.
328	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	58	2199	How does this relate to identifying and maintaining a list? The discussion should relate to the other requirements for inventory and component management.	Update the discussion to relate to managing the list of components 3.4.10.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
329	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	59	2224	**3.16.3 External System Services (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define what controls, processes, methods and techniques are implemented - What if different agencies want different things? There can be no consistency to this.** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	NIST should publish a baseline for the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed, or when operating system introduces limitations but others meets compliance requirements.
330	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	59	2224	Terminology is conflicting/confusing - **3.16.3 External Systems Services** – a, b, c all have the term organization used for both federal and contractor	Use different terminology when actually referring to the contractor s organization and not an Organization-Defined Parameter (ODP) where the organization is a Federal agency.
331	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	59	2224	**3.16.3 External System Services (reference to ODP)** – ODPs define controls – Customer could require compliance with a variety of competing regulations. The intent to lower risk could actually introduce more risk by reducing the amount of vendors available willing and compliant.	Clarify which tiers are responsible for meeting. Define ESP, MSP, CSP (recognizing they are not all equal and perform different roles in the environment).
332	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
333	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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
334	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 contractual issues with the external suppliers	Remove the ODP for this control requirement
335	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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.
336	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	59	2251	**3.17-1-4 Supply Chain -** It s unclear whether a SCRM is needed for all systems with a corporation or just the systems processing CUI.	SCRM should only apply to the systems processing, storing, or transmitting CUI.
337	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	59	2251	Consider using “system” or “process” terminology instead of “plan” to connote persistence. “Plan” is typically used at program level and in many cases companies would want to show persistent compliance artifacts at the enterprise or division level.	Consider using “system” or “process” terminology instead of “plan” to connote persistence. “Plan” is typically used at program level and in many cases companies would want to show persistent compliance artifacts at the enterprise or division level.
338	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
339	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	59	2251	This requirement seems overly broad for all supply chain plans to understand development and manufacturing of COTS, for example.	Create an ODP to Select From: to add relevant items depending on the supply chain plan.
340	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	59	2251	This requirement seems overly broad for all supply chain plans to understand development and manufacturing of COTS, for example.	Create a template Supply Chain Plan that organizations can use.
341	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	59	2251	Change the wording to remove many of the words since this is multiple requirements. All of the additional text is extraneous and adds confusion and complexity.	Remove "the development, manufacturing, acquisition, delivery, operations, maintenance, and disposal of"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
342	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	59	2251	The second paragraph is extraneous and adds confusion and should be removed from this document.	Remove the second paragraph under Discussion.
343	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	59	2251	The system-level SCRM plan is implementation-specific and provides policy implementation, requirements, constraints and implications. It can either be stand-alone or incorporated into system security plans. Use of the acquisition process to protect the Supply Chain. Ex: obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. Increased specify of previous requirement to remove ambiguity on disposal of the system components, documentation or tools in a manner that reduces risk of compromise and when it can be disposed of.	Companies will need to allocate funding to support with impacts to cost constraints. Instead of the incentives, the organization could make an evaluation criteria. Recommend 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.
344	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 additional 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
345	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	59	2255	3.17.1-It is unnecessary to allow each ODP to redefine the update frequency of the supplier risk management plan	Remove the ODP for this control requirement
346	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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”
347	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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 sentence 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."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
348	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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.
349	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	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".
350	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	60	2300	**3.17.3 Supply Chain Control & Processes (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define the supply chain controls to implement – What if there are conflicting controls?** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	NIST should publish a baseline for the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed, or when operating system introduces limitations but others meets compliance requirements.
351	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	60	2300	**3.17.3 Supply Chain Controls and Processes (reference to ODP) – ODPs define the controls used to protect against supply chain risks – This is very broad and could result in a whole new set of policy controls every time a new contract or customer is onboarded.** ODP infringes upon contractor's Corporate policies and procedures.	Where a timeline is mentioned - the ODP should be set at annually or refer to contractor's existing policies (whichever is more frequent).
352	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	60	2300	It would be better for NIST to define a minimum set of controls in part b. It is very difficult to maintain compliance at the enterprise level when the controls in part b are organization-defined, i.e., change per customer set.	It would be better for NIST to define a minimum set of controls in part b. It is very difficult to maintain compliance at the enterprise level when the controls in part b are organization-defined, i.e., change per customer set.
353	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	60	2300	A related concept is to define a minimum set for NIST SP 800-171 and then a separate, additional set for NIST SP 800-172	A related concept is to define a minimum set for NIST SP 800-171 and then a separate, additional set for NIST SP 800-172
354	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	60	2303	In 3.17.3 Supply Chain Controls and Processes, we are to: "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]. " This ODP is wide open. What if one agency demands the use of it s standard solution, and that contradicts the choice of another agency?	Identify a set of common baselines, ways to validate strong practices (i.e., crypto/encryption) and ones that would always be allowed to be done by the DIB. It is critical that ODPs are set in a way that it does not introduce conflicting requirements.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
355	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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 the ODP for this control requirement
356	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial	Publication	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 different.
357	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
358	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	61	2322	A related concept is to define a minimum set of techniques and methods for NIST SP 800-171 and then a separate, additional set for NIST SP 800-172	A related concept is to define a minimum set of techniques and methods for NIST SP 800-171 and then a separate, additional set for NIST SP 800-172
359	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
360	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	61	2323	3.17.4-Component disposal should not be ODP assigned. If the USGOV wants particular disposal techniques and methods to be implemented then those requirements should be directly stated in this document	Define the requirement and remove the ODP
361	National Defense Information Sharing and Analysis Center (ND-ISAC)	Editorial & Technical	Publication	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.
362	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	ODPs are based on NIST 800-53 RMF/ATO environment where an organization determines risk to their program. ODPs dictated by a dept/agency/program will introduce variability into the DIB and makes it difficulty to be standardize.	Recommend a standard be defined (minimum value or a range of accepted values) across the USG, and/or self-determined by federal contractors based on risk, and the size of the organization and type of work.
363	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	The word “system” appears 745 times in 800-171 and in 72 of the 800-171 requirements. The definition for “information system” listed in the sub bullets from Pages 1 & 2 is easily confused with the generic IT term “system”. The “information system” definition will vary wildly depending on how the contractor applies it, and the size of the work being conducted by the contractor. For some contractors it could include hundreds or thousands of servers, encompassing large segments of the contractor s network. This is very different from the traditional idea of an IT “system”, which would normally include at most a small handful of servers. It is not clear if every use of the term “system” in 800-171 actually means “information system”, or if the term is instead referring to a more traditional definition of “system” that implies a smaller scope.	At a minimum, NIST should change every instance of system to “information system” if that is what is intended. When determining intent, NIST should keep in mind that for some contractors, “information system” will be the entire network, not just a single server. If the control actually is intended to be applied to each box on the network, a different definition should be used (possibly the “component” definition that was introduced). There are many examples where the word “system” used in 800-171 does not seem to be achievable at the scale needed to meet the control for a large enterprise s information system. o 3.1.3, p. 6, line 181: is “within the system” the same as “within the network” or is it “within 2 applications on the same box”? o 3.1.23, p. 15, line 513: does logging out of the system mean the whole network, or does it mean each individual application, server, endpoint, etc.? o 3.5.4, p. 20, line 1040: is this a one-time 2FA to the network, or 2FA to every account on every box, both local and via the network? The latter is unachievable in a large enterprise.
364	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Purpose of NARA CUI /EO was to drive consistency across executive agencies, and 800-171 as the common standard. By introducing ODPs, NIST 800-171 R3 is moving everyone toward not being standard, irrespective of a department/ agency/ program. The Intent of the original 171 was lost with new reviewers and the ability of small businesses to successfully meet them as well as providing a baseline for adequate security across the DIB.	ODPs are good, but it needs to be defined by the federal contractor
365	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Variability will introduce costs for assessments. Assessors do not have the authority to specify rules, only audit existing ones. if ODP specifies 1 year, the assessors cannot say "that's too long".	If a department specifies ODPs, assessors need to be trained on all variations.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
366	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	ODPs need to be scoped correctly and in alignment with technology changes, and environment complexities. Variations could also introduce cost impacts to government and industry.	how long should it take to break a password which changes based on technology advancements. So 12 might be okay today, but in three years maybe you need 15 to keep brute force attacks from working for x number of years
367	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	FIPS is one of the examples where ODPs are intended to "relax" the original requirement by letting the Org specify the standard that best meets their requirements	FIPS validation maybe it's better to say modern encryption so that you aren't stuck on AES 128 or AES256 but anything that meets criteria
368	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Requirements needs to be consistent across all of USG for contractors to meet within US (Federal, state, Local) and with International Partners	Leverage Sector specific coordinating councils, like the ND-ISAC for DIB sector, to provide suggested values for that sector/industry. With consistency we can, over time, figure out how to manage security and how to charge for it.
369	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Small business struggle to define adequate security controls that are risk based decisions for ODPs due to lack of skills or personnel.	NIST should working directly with the Small Business Administration to identify cost, impact, effectiveness, etc. impact as part of our response as that is where a major part of the pain will occur
370	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Describe the intent of the requirement to help the reader and the assessor.	See examples in NIST Cyber Security Framework CSF 2.0. NIST CSF aligns with the National Cybersecurity Implementation Plan published on 13 July. Initiative 1.1.3 is to increase agency use of frameworks and international standards to inform regulatory alignment. NIST 800-171 should be aligned with the CSF. Per the plan, CSF as a "performance based Framework keep pace with technology and threat trends, integrate lessons learned, and move best practice to common practice". References from the plan include "consensus standards and guidance"
371	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Discussion section cannot be used to define the requirement, and not cause confusion.	Rework Discussion Section for the Section 3. The Requirements
372	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	We understand that the interim draft has maintained the Rev 2 numbering to show what has changed or is changing, and we expect the final version will have consecutive numbering and a trace back to the old version.	When the final document is published the numbering must be consecutive.
373	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	As the sole IT person at a SMB doing piece work part assembly for many primes for hundreds of defense contracts from several different government agencies, I just need to be told what to do clearly and specifically, with minimal effort, so I can just do my job.	Make the instructions clear, but make them achievable without setting impossible goals that I can t reach or I ll have to just stop doing defense work.
374	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	As an IT architect at a Prime who has shared infrastructure providing consolidated security services from a core team for many defense contracts from several different government agencies, I want clear risk goals as outcomes that guide me to architect my own solutions without proscribed dictated inflexible demands.	Give me SP 800-53 to work with and let me specify my own “[organization-defined controls]” just like my partners within the government do, because I have the systems and tools to demonstrate the trustworthiness of the controls to a high degree of assurance to an auditor.
375	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	As a 3PAO auditor, I want concrete proof that the intent of the controls are being met, not just “checking the box”. My role is to review the evidence and provide assurance to the CO s, the DIB CIO office, and to the DIB contractor s own executives about the quality of the controls that protect CUI through assessments.	As said in 800-53, “Such assessments help determine whether the controls are implemented correctly, operating as intended, and satisfying security and privacy policies—thus, providing essential information for senior leaders to make informed risk-based decisions.” The assessment objectives, criteria for meeting the intent, and evaluating supporting evidence must be consistent to achieve the outcomes.
376	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	As a Contracting Officer, I want to know that the primes and their sub tier suppliers protect the confidentiality of CUI, without gaming the system for compliance without actually securing the data. I recognize that DIB companies can provide better assurance when security systems are consolidated, but my focus is on the data for *MY* contract foremost (e.g. I don t care how they do things over there in the Navy, I know better…).	Guidelines are required
377	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	As an executive at a DIB company, I want the control requirements to be consistent across different contracts from different agencies, as we discussed a decade ago before 800-171 was first released.	If ODPs were different, I can t satisfy conflicting requirements from different “organizations” who all think they are “special”; that was the problem before 252.204-7012!

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
378	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Who are all of the stakeholders?	Conduct an analysis of stakeholders, systems, type of assets in collaboration with agencies and companies as stakeholders. Provide an authoritative moderated discussion forum for comments, questions, operational issues, and maintenance. Produce strategy, timelines for planning and implementation.
379	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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	We recommend NIST work with government and private industry to establish standard ODP values that can be implemented uniformly.
380	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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.
381	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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.
382	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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.
383	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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.
384	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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.
385	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	when containing ODP, not all statements make complete sentences	Fix all ODPs to be readable and complete sentences

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
386	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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.
387	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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
388	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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
389	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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.
390	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	Comment	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."
391	National Defense Information Sharing and Analysis Center (ND-ISAC)	Technical	Publication	Comment	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 certainty/control for unsupported components that may not exist
392	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Further reviews of the discussions under each requirement need to be performed to provide references to the interrelated requirements which is done in 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.
393	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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
394	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Overlay	Comment	N/A	Why does the CUI Overlay not address any element of what/why requirements were changed from 171rev2? The overlay discusses 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.
395	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Overlay	Comment	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.
396	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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.
397	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	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.
398	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Understanding how agencies or the customer is going to define the 112 ODPs would need to be made a part of the RFI/RFP process. Large businesses have an advantage, as they are more equipped to handle the implementation and interpretation of potentially varying ODPs. Small business would need to have expanded resources available to them (to be flexible enough to adjust/evolve set ODPs) in order to be competitive.	**NIST should publish a baseline for the standard**, in lieu of the ODPs, that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed, or when operating system introduces limitations but others meets compliance requirements. (where a timeline is mentioned - annually should be set as the baseline) Where there is low-risk, or a baseline is inconsequential but still needs definition, the contractor should be able to define.
399	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Removal of enduring exceptions was not addressed.	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.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
400	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	The addition of Planning (PL), System and Services Acquisition (SA), and Supply Chain Risk Management (SR) will require review, evaluation, and implementation. This is burdensome on SMB, many of which are sub tiers but will be required to be compliant with the new revision of NIST 800-171.	Offer ranges for implementation, or set basic/low threshold minimum actions to be taken for sub tiers.
401	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Overlay	Comment	N/A	The development of the CUI Overlay assumes SMBs are consistently receiving clearly marked and identified CUI, which they are not. Not all CUI is created equal. The document assumes it is. This increases risk by introducing variables where they didn't exist before.	NIST and NARA should collaborate on guidance with agencies and companies as stakeholders
402	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	171, by nature of its alignment with 53, seems to only target classic IT architecture and does not align with emerging models like those in SMB where CUI primarily lives in a SaaS tool and is pulled to employee laptops, who are working remotely and not on a corporate network.	Account for more modern architecture that's used in SMB (and larger companies).
403	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	An information system may not able to apply an ODP due to a limitation of the system, such as in a SAAS solution.	Provide guidance to allow for exception by the organization that procures the information system.
404	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	Scoping is not clear. This risks over-scope in any environment, burdensome in a SMB environment. "CUI Systems" are not just servers and static environments - they can be laptops and workstations. Controls are more effectively and efficiently managed in some pieces of a network rather than others.	Clarify/define/refine scoping. Define what requirements should apply, if not all, to "systems that provide for the protection of" the systems with CUI, or at least direct "not all requirements should apply to a system that provides security" etc.
405	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	"Organization Defined System" is not listed in the glossary.	Define "Organization Defined System," and clarify who actually defines this - the government agency? Or the contractor to be compliant with the standard?
406	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	It is not possible for the government to understand all the different organizational systems, information systems, and parameters for every different organization.	ODPs that require procedure or processes definitions should be left to the DIB organization to define.
407	National Defense Information Sharing and Analysis Center (ND-ISAC)	General	Publication	Comment	N/A	NIST 800-53 is geared to an enclave/one-system environment, 800-171 is intended for flexibility so it could apply to a corporate environment	returning to the 800-53 verbiage and format makes for a better understanding of the controls and what is expected, the ODP variability moves us away from corporate environment scopes to enclave only scopes.
408	ND-ISAC Small and Medium Business (SMB)	General	Publication	Comment	N/A	(SMB) Cost considerations have not been factored for SMBs. Some of the requirements require technical controls that add burden. While the DFARS 252.204-7012 is not NIST's concern… it requires compliance with the version of NIST in effect at the time the clause is added to the contract. This will add burden to SMBs when they receive new solicitations this Spring of 2024 when NIST SP 800-171 Rev 3 is finalized.	(SMB) Please coordinate the requirements to implement NIST SP 800-171 Rev 3 Final for at least 12 months due to budget cycles and the economy. (e.g. DoD Class Deviation). NIST should publish strategies, timelines, and collaborate on impacts due to the regulatory implications of nonfederal standards.
409	ND-ISAC Small and Medium Business (SMB)	General	Publication	Comment	N/A	(SMB) ODPs should not be left to be defined by federal agencies. DIB companies who work for multiple government agencies will be at the mercy of implementing the "most restrictive" requirements of the federal agency who decides to require "ODPs" that are burdensome and / or do not account for the differences of organizations	(SMB) ODPs should be developed by committee of non-federal entities who understand the complexities of different networks and environments.
410	ND-ISAC Small and Medium Business (SMB)	General	Publication	Comment	N/A	(SMB) Organizations need to completely understand what is required to achieve a requirement	(SMB) Consolidate 800-171 and 800-171A into one document. Many companies seem to be unaware 800-171A exists. 800-171A is critical for companies to understand completely what is required of them.
411	ND-ISAC Small and Medium Business (SMB)	General	Publication	Comment	N/A	(SMB) NIST was pragmatic in improving 800-171 Rev 3 to clarify requirements for organizations.	(SMB) Additional prescription is still needed… in some ways. Please consider adding "discussions" as were developed in the CMMC Assessment guides as it provided examples to companies who struggle to understand the intent.
412	ND-ISAC Small and Medium Business (SMB)	General	Publication	Comment	N/A	(SMB) How do I know "what" I need to do or what "tools" to use?	(SMB) Please make recommendations for tools or solutions that will allow an organization to meet the intent of the requirement to pass the newly added external assessments

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
413	ND-ISAC Small and Medium Business (SMB)	General	Publication	Comment	N/A	(SMB) NIST Small Business Cybersecurity Corner	(SMB) The team has stated their role is not to help interpret the requirements.. But NIST wrote the requirements. Can someone at NIST please provide resources to the Small Business Corner team to help with the interpretation of the requirements? As NIST 800-171 becomes an international standard and required of CMMC this will become more critical to people who cannot afford to hire a consultant to help them (and that consultant may or may not provide the "right" interpretation of the requirement.