From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] RTX comments list and cover letter for NIST SP 800-171 Rev 3 (Draft)
Date: Thursday, July 13, 2023 8:40:30 AM
Attachments: RTXCommentsLetter-NIST_SP800-171R3-Signed-11Jul2023.pdf
sp800-171r2-to-r3-ipd-RTXcomments-FINAL.xlsx

Please see attached cover letter and comments list from RTX for the NIST SP 800-171 Rev 3 (Draft), Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Thank you for soliciting and considering our comments.

Best Regards,
Angie Bull

Angela Bull, CISSP
Associate Director, Cybersecurity Compliance
[redacted]
RTX

July 11, 2023

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899714737`

Subject: Comments on Draft NIST Special Publication 800-171 R3 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.*

Enclosures: (1) RTX Comments Spreadsheet

RTX would like to thank NIST for the opportunity to provide comments regarding draft Special Publication (SP) 800-171 R3, and we fully support NIST's effort to deliver cybersecurity standards across the federal government. We have reviewed draft SP 800-171 R3 and are pleased to provide comments to help shape the final publication. Some general observations are included below, and a detailed list of comments is provided in enclosure (1).

1. **Comment Type: General**
   Comment: 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. Moreover, while government contracting offices are competent with procurement rules and able to determine when certain requirements can be waived, they may not be able to define detailed ODP requirements or cybersecurity-related controls. There is also no known cadence for managing changes to ODPs, so agencies could change ODPs at any time (unlike revisions to SP 800-171 which are published with a formal comment period). Lastly, SP 800-171 is becoming more recognized and accepted globally. Allowing varying ODPs across federal agencies will weaken the NIST "standard" making it less effective and less likely to achieve reciprocity with other standards.
   Suggested Change: We recommend NIST work with government and private industry to establish standard ODP values that can be implemented uniformly.

2. **Comment Type:** General
   Comment: 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.
   Suggested Change: 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.

3. **Comment Type: General**
   Comment: 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.
   Suggested Change: 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.

4. **Comment Type: General**
   Comment: 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).
   Suggested Change: 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.

5. **Comment Type: General**
   Comment: 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.
   Suggested Change: We recommend defining a transitional period to implement SP 800-171 R3 changes, which are expected to be time consuming, labor intensive, and costly.

Thank you for soliciting and considering our comments.

Brad Maiorino

Vice President and Chief Information Security Officer
RTX

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	RTX	General	Publication	N/A	N/A	We remain concerned with agencies having the option to set differing Organization-Defined Parameters (ODPs). The stated objective of Executive Order (EO) 13556 is to establish a governmentwide program to standardize the handling of Controlled Unclassified Information (CUI). Allowing federal agencies to use ODPs to define unique requirements is contrary to the objective, as it promotes inconsistent and potentially competing standards across the federal government. Agency baseline expectations will diverge resulting in a patchwork approach to cybersecurity, rather than allowing a single baseline standard as intended. Companies supporting multiple agencies may determine that some requirements are too costly to implement based on financial/risk analysis. Having these contradictory ODP requirements across agencies will make it difficult for companies to fully comply and will create operational challenges as noted below: • Differing ODPs being specified in RFI/RFPs will result in no single baseline security configuration. • Companies will be burdened with coordinating different ODP assignments across multiple agencies. • As ODP assignments may be incompatible, companies will find it difficult to have one 'enterprise' level SSP that complies with all ODPs. • Companies being forced to implement varying agency mandated ODPs will result in significant impact on government programs due to additional unnecessary costs and compliance challenges. • Differing ODPs will make 3rd party assessments difficult, as the assessor must have the ODP details from all contracts to validate all ODP requirements. • Assessors, rather than referring to a single baseline standard, will rely on individual experience to interpret different ODP requirements, resulting in inconsistent assessment results. Moreover, while government contracting offices are competent with procurement rules and able to determine when certain requirements can be waived, they may not be able to define detailed ODP requirements or cybersecurity-related controls. There is also no known cadence for managing changes to ODPs, so agencies could change ODPs at any time (unlike revisions to SP 800-171 which are published with a formal comment period). Lastly, SP 800-171 is becoming more recognized and accepted globally. Allowing varying ODPs across federal agencies will weaken the NIST "standard" making it less effective and less likely to achieve reciprocity with other standards.	We recommend NIST work with government and private industry to establish standard ODP values that can be implemented uniformly.
2	RTX	General	Publication	N/A	N/A	NIST's effort to consistently align the language of SP 800-171 with SP 800-53 is greatly appreciated; however, it appears that key elements and context from SP 800-53 were not included in draft SP 800-171 R3. For example, 3.14.1 "Flaw Remediation" in draft SP 800-171 R3 includes parts a-c from SP 800-53 but does not include part d. The draft SP 800-171 R3 derivative also omits key information that explains parts of the requirement, making it difficult for organizations and assessors to implement risk-based approaches.	We recommend NIST continue to align requirements with SP 800-53 and provide justifications as to why certain SP 800-53 control parts have been omitted from SP 800-171 requirement objectives. Including an objective level cross-reference to SP 800-53 for additional guidance and information would also be helpful.
3	RTX	General	Publication	N/A	N/A	It is unclear how to implement the requirements and determine what is expected even with the relevant discussions included. The assessment guide provides better insight into the level of effort expected to fully implement the requirements. It is difficult to submit comments on the requirements and their intended implementation without the SP 800-171A assessment guide, as it outlines the objectives and clarifies the tasks needed to implement the requirements.	We recommended that SP 800-171A assessment guide be released in tandem with draft SP 800-171 R3, to allow for more constructive and useful comments to be submitted.
4	RTX	General	Publication	N/A	N/A	Many discussion sections associated with requirements contain inconsistent and/or incoherent language, making it difficult to understand the intent of the requirement. Additionally, some discussion sections that refer to interrelated requirements fail to adequately describe how or why the requirements are interrelated (e.g., 3.1.23).	We recommended that the discussion sections be updated for consistency, with descriptions to address the intent of the requirement, and updated to be more concise, removing information not directly related to the requirement.
5	RTX	General	Publication	N/A	N/A	It is unclear what the effective date for this publication will be once it is finalized and published. Due to the significant changes being introduced, companies should be given adequate time to implement.	We recommend defining a transitional period to implement SP 800-171 R3 changes, which are expected to be time consuming, labor intensive, and costly.
6	RTX	Editorial	Publication	2	30	In the Introduction section 1.1 "Purpose and Applicability", 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 defines "system" and doesn't identify CUI as part of the definition, but the Introduction scoping states "CUI". Also, what level of separation is needed for systems that do not have CUI that are connected to the same network and using the same enterprise services?	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 Introduction definition of scope.
7	RTX	Editorial	Publication	7	229	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.
8	RTX	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.
9	RTX	Technical	Publication	11	364	Is this crytography required to follow the other crytography requirements? If so, then the discussion should highlight the requirement. Otherwise, identify what is strong cryptography.	Add information relating the cryptography requirement to the ODP cryptography requirement and/or how to validate strong cryptography.
10	RTX	Technical	Publication	12	397	Is this crytography required to follow the other crytography/encryption requirements? If so, then the discussion should highlight the requirement. Otherwise, identify what is strong cryptography/encryption.	Add information relating the cryptography/encryption requirement to the ODP cryptography requirement and/or how to validate strong cryptography/encryption.
11	RTX	Editorial	Publication	13	455	No definition for Trust Relationships.	Please add a definition for "trust relationships" in the glossary.
12	RTX	Editorial	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
13	RTX	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.
14	RTX	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.
15	RTX	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? Forceably logging off an account after the defined period of inactivity could adversely impact applications and has the potential for loss of data. In addition, some mission or business critical industrial control systems, software, or hardware require a user to be logged in for proper operation and automatically logging them off could leave some connections orphaned which will eventually result in performance issues. This could also have a huge ripple effect on factories and could impact some production lines and systems supporting business infrastructure (i.e., HVAC systems) that cannot be logged off without impacting the operation of the system.	Recommend allowing for exceptions or other risk mitigating controls for mission and business critical systems, software, and/or hardware, Industrial control systems, and systems supporting business infrastructure.
16	RTX	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.
17	RTX	Editorial	Publication	16	552	Why doesn't this have Literacy as part of the training discussion?	Make consistent and define all terms
18	RTX	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.
19	RTX	Editorial	Publication	17	603	Dictating all the possible event types by an organziation can be very cumbersome with different intepretations between organizations.	Recommend removing the ODP from part a. Also, change "remains necessary and sufficient" to "remains relevant and sufficient.".
20	RTX	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.
21	RTX	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.
22	RTX	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.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
23	RTX	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.
24	RTX	Editorial	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? Why is unique not listed anywhere in this requirement? What "status" means is highlighted in the discussion but by just reading the requirement in d, it is hard to identify what you are looking for and status is contractor, foreign national, etc. does not seem to be a good fit and really should be called something other than status such as identifying specific characteristics based upon the needs, regulations, and requirements of the org. Why are only users, processes, and devices listed as identifiers when other items are listed in the requirements. This should be consistent with requirement verbiage to reduce confusion.	Change "to assign an individual, group, role, service, or device identifier" to "to assign system account, role, or device identifier" for all instances in this requirement. Add "to assign a unique identifier" to the different requirement. B. should be "select and assign a unique identifier ..." Change d back to original from NIST SP 800-53 IA-4(4). Add the other types of identifiers as listed in a and b.
25	RTX	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."
26	RTX	Technical	Publication	34	1272	This requirement seems to be overly broad especially with the additional "technical competence" required for supervising maintenance activities. This could result in issues with all of the non-CUI related maintenance activities within an organization. For example, if there needs to be HVAC work performed in an area with CUI, having an HVAC knowledgable person available to escort the technician may be unrealistic and unachievable.	Update the requirement to specify maintenance work on the systems in scope per the scoping guidance (i.e., CUI systems or security for those systems) instead of leaving open ended.
27	RTX	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.
28	RTX	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
29	RTX	Editorial	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 The discussion identifies that "alternate physical controls" is acceptable but that is not what the requirement states.	Add call out to 3.13.11 in the discussion regarding approved cryptography within the discussion to identify that it is related. Change the requirement to "implement cryptographic mechanisms or alternate controls .." in the requirement to be consistent with the discussion.
30	RTX	Editorial	Publication	38	1425	Why doesn't b have a ODP time period for reviewing and confirming the need for access? If the assumption is that other requirements provide guidance on ODP time periods for reviews, etc., then the discussion should be updated to reflect that with the appropriate requirement numbers.	Add ODP for b. 1. for time period review. If the assumption is that other requirements provide guidance on ODP time periods for reviews, etc., then the discussion should be updated to reflect that with the appropriate requirement numbers.
31	RTX	Editorial	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. Why are there no ODP for time periods or reviewing compliance?	Redefine this requirement to differentiate the types of roles that would be required for these vs just stating all external providers. Add ODPs for timeframes for reviews and monitoring of compliance. Due to no ODPs for reviews or compliance and if assuming met by other requirements, then the discussion needs updated to reference those other requirements for their ODPs
32	RTX	Editorial	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" b should state "Require authorization credentials for physical location access" c. should change "facility" to "physical location(s)" d. should change "facility" to "physical location(s)" Need to define "facility" and "physical location(s)"
33	RTX	Editorial	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. With the new wording of a, b seems to only affect assessments of unauthorized disclosure so limited in scope and applicability. Based on the update to be risk assessments of unauthorized disclosure, the Discussion seems to not have been updated to discuss the limited scope but rather still discusses an overall risk management program that would assess risk of organizational assets	Revert back to the original requiring risk assessments to flow with many of the other requirements. Otherwise, the overall intent is lost If this is the intent of the new requirement, update the Discussion to highlight the limited scope
34	RTX	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.
35	RTX	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.
36	RTX	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 .. "
37	RTX	Editorial	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.
38	RTX	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)
39	RTX	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. FIPS validated is problematic and NSA approved is even harder to obtain. When patches come out, any validation is typically invalidated. The requirement should describe strong encryption and/or identify the user of FIPS validated algorythms or FIPS compliant modules with strong key management. ITAR is only requiring FIPS compliant.	Remove the reference to FIPS validation to alleviate confusion as to whether FIPS is required of not. Modify the requirement to provide a list of minimum requirements for proving strong cryptography instead of just stating ODP to allow flexibility in meeting the requirement while being secure and provable. Update discussion with relationships with other requirements. Update the discussion to provide guidance on identifying strong cryptography. Modify requirements and discussions with ODPs that identify and highlight the boundaries and requirements as well as relationships with the other requirements in their associated discussions. Change the encryption requirements to identify FIPS compliant with strong key management is considered strong encryption and cryptography rather than FIPS validated.
40	RTX	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.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
41	RTX	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 implemntation.	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".
42	RTX	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
43	RTX	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.
44	RTX	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.
45	RTX	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 sentance to: "Tools and techniques may provide protections against unauthorized production, theft, tampering, poor development practices, and the insertion of counterfeits, malicious software, and backdoors throughout the system life cycle."
46	RTX	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.
47	RTX	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".
48	RTX	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 dofferent.