From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] Comments on NIST SP 800-171r3 final public draft - RTX cover letter and comments list
Date: Thursday, January 25, 2024 12:58:35 PM
Attachments: RTX-CommentsLetter-NIST-SP800-171r3fpd-23Jan24.pdf
RTX-CommentsList-NIST-SP800-171r3fpd-23Jan2024.xlsx

Please see attached cover letter and comments list from RTX for the NIST SP 800-171 Revision 3 Final Public 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
Cybersecurity Compliance
[redacted]
RTX

RTX
1000 Wilson Blvd.
Arlington, VA 22209
United States

January 25, 2024

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

Subject: Final Public Draft National Institute of Standards and Technology Special Publication 800-171 Rev. 3 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

Enclosures: (1) RTX Comments Spreadsheet

RTX would like to thank National Institute of Standards and Technology (NIST) for the opportunity to provide comments regarding the Final Public Draft (FPD) Special Publication (SP) 800-171 Rev. 3, and we fully support NIST's effort to deliver cybersecurity standards across the federal government. We have reviewed FPD SP 800-171 Rev. 3 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 global cybersecurity standards.
   Suggested Change: We recommend NIST work with government and private industry to establish standard ODP values that can be implemented uniformly. Alternatively, consistent with the purpose and applicability of NIST SP 800-171 Rev. 3, we recommend NIST specify that ODP values for nonfederal systems only be specified by nonfederal organizations, and not federal agencies, which would be more appropriate for federal systems subject to NIST SP 800-53 Rev. 5.

2. **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 number of changes that have been made, companies should be given adequate time to implement them.
   Suggested Change: We recommend defining a transitional period to implement NIST SP 800-171 Rev. 3 changes, which are expected to be time consuming, labor intensive, and costly.

Thank you for soliciting and considering our comments.

Brad Maiorino

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	NIST SP 800-171r3 fpd	-	-	We remain concerned with agencies having the option to set differing Organization-Defined	We recommend NIST work with government and private industry to establish standard ODP
2	RTX	General	NIST SP 800-171r3 fpd	-	-	It is unclear what the effective date for this publication will be once it is finalized and published. Due to the number of changes that have been made, companies should be given adequate time to implement them.	We recommend defining a transitional period to implement SP 800-171 R3 changes, which are expected to be time consuming, labor intensive, and costly.
3	RTX	Technical	NIST SP 800-171r3 fpd	40	1434	It is not common for nonfederal (or federal) organizations to screen or rescreen for conduct, integrity, judgment, loyalty, reliability, or stability, particularly in the context of access to unclassified information and/or systems. These types of attributes require personal knowledge of individuals that is not typically gained by employers through their hiring or other processes. More typically, nonfederal organizations screen for work authorization, credit history, criminal background, denied or restricted party, etc. Further, the type and frequency of such screenings and rescreening are contingent upon an organization’s business and risk appetite, as well as applicable laws and regulations.	We recommend removal of 3.9.1.b or specify such screening and rescreening shall be in accordance with, and only as required by, any applicable law, regulation, or government-wide policy.
4	RTX	General	NIST SP 800-171r3 fpd	7	189	The control objective states, "Enforce approved authorizations," but the discussion mentions access enforcement, not authorization enforcement, which could cause some confusion.	If these terms are interchangeable, then we recommend NIST update the control objective to, "enforce approved access" (Line 188) or update the discussion section to "authorization enforcement.” mechanisms..." (Line 193)
5	RTX	Editorial	NIST SP 800-171r3 fpd	9 12	254 370	Throughout the publication there are multiple terms used that are not defined or clearly differentiated. These Terms include: processes applications system process system services application	We recommend NIST define the terms or if the terms are "interchangeable," we recommended NIST use one term throughout the publication.
6	RTX	Technical	NIST SP 800-171r3 fpd	10	315	This will be significantly harder to meet as it requires limiting all invalid logon attempts within a time period instead of by a single user. You would not want to lock a system when X number of failed logons by XX number of accounts, as this could ultimately block legitimate users from logging in. To minimize the impact to the system users, you can limit the number of logins within a specified time period. If the intent is to lock the system and not a specific user account, then this should be identified as a significant change.	We recommend adding "by a user" back into the requirement from 800-171r3 or modify the requirement to "Limit the number of consecutive invalid logon attempts to a system to [Assignment: organization-defined time period]."
7	RTX	Technical	NIST SP 800-171r3 fpd	15	481	b should have the ODP removed and remove "following" b should be "Establish and maintain the terms, …." and remove c2 as it is redundant with b.	We recommend rewording 3.1.20.b to "Establish and maintain the terms..." and removing the ODP at the end of 3.1.20.b. With the updated statement in 3.1.20.b, c2 becomes redundant with b.
8	RTX	Editorial	NIST SP 800-171r3 fpd	18	603	Dictating all possible logging event types by organization is impractical.	We recommend removing the ODP from part a.
9	RTX	Technical	NIST SP 800-171r3 fpd	21	728	It is not clear that an ODP is required here given the discussion about varying inputs based on the needs of the application/system.	We recommend removing the ODP from 3.3.7.b and changing b to read, "b. Record time stamps for audit records that meet system granularity of time requirements and that:..."
10	RTX	Technical	NIST SP 800-171r3 fpd	25	868	The scope of 3.4.6.b ODP could be misinterpreted to mean that an individual must do this for all of the items listed (functions, ports, protocols, and services) when they may not all apply to an information system.	We recommend changing the wording of 3.4.6.b to "...functions, ports, protocols, OR services" and identifying the relationships between controls.
11	RTX	Editorial	NIST SP 800-171r3 fpd	27	944	Documenting the location of all existing CUI within a large organization is dependent upon the Government’s identification and marking of CUI. Further, it will take considerable time to verify the location of any existing CUI currently stored on a contractor network, particularly since the Government has not consistently identified or marked CUI. It may be more feasible to begin tracking CUI locations as it is provided to or created by organizations instead of attempting to locate all CUI currently in an organization’s possession.	We recommend tracking the location of CUI insofar as the Government has appropriately identified and/or marked it, based on new contracts after the date that R3 is approved and effective. Additionally, we recommend defining the level of granularity needed to meet this requirement; for example, identifying the information systems that contain CUI or identifying the file locations of CUI within the systems. We also recommend including "identify and document" on c, to be consistent with a and b, and add "identify and document" on c.
12	RTX	Editorial	NIST SP 800-171r3 fpd	29	1017	This new requirement combined with the information in 3.1.1 states that the 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 and could increase the scope and require more MFA devices.	We recommend reducing what is defined as a system account in 3.1.1 and updating the Discussion to identify if this is for all accounts within a system (which could be different for each device).

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
13	RTX	Editorial	NIST SP 800-171r3 fpd	36	1281	This requirement seems to be overly broad especially with the addition of "technical competence" required for supervising maintenance activities. This could result in issues with 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.	We recommend updating 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.
14	RTX	Technical	NIST SP 800-171r3 fpd	38	1350	There are media types that could be too small to include distribution, handling, and security markings. NARA has provided the following guidance in their marking guide, "Due to space limitations it may not be possible to include CUI Category, Subcategory, or Limited Dissemination Control Markings. At a minimum, mark media with the CUI Control Marking ("CONTROLLED" or "CUI") and the designating agency."	We recommend updating the Discussion to be consistent with the NARA marking guidance that exempts some media marking requirements due to size limitations.
15	RTX	Technical	NIST SP 800-171r3 fpd	40	1448	The first ODP in 3.9.2.b.2 is unnecessary given the second ODP.	We recommend changing 3.9.2.b.2 to state, "Initiate transfer and reassignment actions within…"
16	RTX	Technical	NIST SP 800-171r3 fpd	43	1542	Change a2 to "systems, devices" by replacing the slash with a comma.	Change a2 to "systems, devices" by replacing the slash with a comma.
17	RTX	Technical	NIST SP 800-171r3 fpd	47	1686	3.12.5.b could significantly impact the implementation of 3.12.5.a as most SLAs lack the level of detail needed to meet the requirement. Therefore, new documentation will likely need to be created when CUI is involved.	We recommend updating 3.12.5.a to "Document, approve, and manage…" and remove 3.12.5.b for better consistency with what most SLAs specify.
18	RTX	Technical	NIST SP 800-171r3 fpd	49	1772	The updated requirement removes wording that allows for alternate physical safeguards. Many companies use alternative measures and implementing this new requirement as stated could have significant impacts; for example, to large data center systems that may not provide encryption. Not allowing for the use of physical safeguards as a mitigation strategy would increase cost on contractors. As the requirement reads now, all transmissions of CUI, even internally, must be encrypted which can be very problematic and is different from previous requirements.	We recommend reverting to the prior wording "unless otherwise protected by alternative physical safeguards" We recommend reverting the applicability only to external transmissions instead of requiring cryptography for all transmissions and at rest, regardless of location (i.e., internal or external)
19	RTX	Editorial	NIST SP 800-171r3 fpd	50	1822	The 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. Most services, applications, and technologies provide some type of cryptography options. This would allow organizations to vet and validate vendor solution cryptography rather than guessing and/or remaining non-compliant due to costs to change. Further, the discussion does not identify the relationship with other cryptographic requirements and does not discuss what would be considered strong crypto or provide a list of examples except FIPS-validated which is very limited in applicability and a cause of organizations having Other Than Satisfied, per DCMA, due to lack of technologies in the industry. In the previous version, there were Discussions that stated encryption was not part of the intent but this now seems to be the intent which may cause increased cost and challenges for industry in requiring encryption at rest and transmission at all times. Requirements for FIPS validated and NSA approved are problematic and hard to obtain. When patches come out, any FIPS 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 instead of FIPS validated. Note, the ITAR only FIPS compliant cryptography.	We recommend modifying the requirement to provide a list of examples for proving strong cryptography instead of only providing for an ODP. This will allow flexibility in meeting the requirement while being secure and provable. We also recommend updating the Discussion with relationships to other requirements providing guidance on identifying strong cryptography. Further, we recommend modifying requirements and Discussions with ODPs that identify and highlight the boundaries and requirements as well as relationships with other requirements in their associated Discussions. Lastly, we recommend changing the encryption requirements from identify FIPS compliant to strong key management is considered strong encryption and cryptography.
20	RTX	Editorial	NIST SP 800-171r3 fpd	51	1850	Please provide examples for monitoring code.	We recommend updating the Discussion with examples of how to monitor mobile code.
21	RTX	Editorial	NIST SP 800-171r3 fpd	57	2059	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.
22	RTX	Technical	NIST SP 800-171r3 fpd	58	2094	It is unclear if NIST intended to require both a and b in its removal of "or." .	If NIST only intends to require a or b, we recommend rewording the requirement to, "a. replace systems components… or b. provide options for mitigation…"
23	RTX	Editorial	NIST SP 800-171r3 fpd	59	2146	This requirement would be very difficult to implement at the enterprise level because plans will vary for each individual program.	We recommend providing an example template for a Supply Chain Plan that organizations can use at an enterprise level.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
24	RTX	Editorial	NIST SP 800-171r3 fpd	60	2175	1. Please clarify what is meant by "filtered buys". 2. NIST has referred financial questions to DoD and DoD has objected to providing financial reimbursements, other than overhead, so it is unclear why NIST would 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.” Further, it is not clear why "identify" and "protect against" have been reordered. 3. The last sentence of the first paragraph is confusing. 4. 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.	1. We recommend deleting the reference to "filtered buys", or if it is retained, please define this term in the glossary. 2. We recommend deleting incentives reference and rewording 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." 3. We recommend rewording 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." 4. We recommend limiting this requirement to critical suppliers.
25	RTX	Editorial	NIST SP 800-171r3 fpd	60	2199	It is 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. 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.	We believe it would be better for NIST to define a minimum set of techniques and methods. Also, we recommend adding a caveat that conditions the requirement to "when contractually requested by the customer."
26	RTX	General	NIST SP 800-171Ar3 ipd	12	628	The 3 assessment objectives specifically call out login attempts by user but 800-171r3 3.1.8 removed "by a user" and thus is inconsistent with the requirement.	We recommend adding "by a user" back into the requirement.