From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments to NIST SP 800-172 rev 3 Initial Public Draft
Date: Friday, January 17, 2025 1:57:57 PM
Attachments: sp800-172r3-ipd-comments Guissanie 250116.xlsx

Attached are comments to the NIST SP 800-172rev3 Initial Public Draft.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Gary Guissanie NA (Self)	General	5	311	A significant issue with the Initial Public Draft of 800-172rev3 is its change to align with the security control language in NIST SP 800-53 rather than retaining the purpose-built security requirement statements used in -172rev0. NIST SP 800-172rev0 evolved from a study to isolate data from foreign adversaries -- in particular, the Advanced Persistent Threat (APT). The original 800-172 requirement statements were adopted from that study and specifically constructed to counter the APT. Although each 800-172rev0 requirement was typically associated with one or more 800-53rev5 controls, the effectiveness of the tailored 800-172rev0 requirements in addressing risk from the APT surpassed the effectiveness of the sum of the~~se~~ associated 800-53 controls. Accordingly, abandoning the tailored 800-172rev0 security requirements/discussion and converting to the 800-53rev5 controls in 800-172r3 will result in a system less able to respond to the APT than a system employing the more specific -172rev0 requirements. For example, a significant 800-172rev0 requirement to implement a secure information transfer capability (3.1.3e) has been withdrawn and replaced with the far less specific 'flow-enforcement' 800-53r5 controls. In another example, the requirement in 172rev0 3.14.4e to periodically refresh the system components from a known trusted state has changed, because of the change to 800-53r5 wording, to a 03.14.04E requirement to refresh from a trusted source, but no mandate to actually refresh the IT (which is the point). Many of the following comments relate to this general issue: the transition to 800-53r5 control text has unnecessarily reduced the effectiveness of the original 800-172rev0 requirements .	While recognizing the efficiency of using 800-53 control statements/discussions vice maintaining separate and unique 800-172 requirement statements, this should be avoided in situations where the effectiveness of the resulting security requirement is reduced. In such cases, a better approach would be to revise these 800-172 requirement statements to what will eventually become new security control/enhancement statements to be published in 800-53rev6.
2	Gary Guissanie NA (Self)	Technical	5	315	The statement at line 315 that a threat-centric approach to security requirement specification is a key element of 800-172 is correct. However, unfortunately, this is no longer the case as most of the 800-172rev0 requirements that addressed relating a specific requirement solution to a specific threat have been withdrawn.	Restore withdrawn 800-172rev0 requirements 03.11.04e, 03.11.05e, and 3.11.06e which require relating security solutions to specific threats so the statement at line 315 will be correct.
3	Gary Guissanie NA (Self)	Technical	5	316	The statement at line 316 that employing system and security architectures supporting logical and physical isolation is an essential element to addressing the APT is correct, but no longer supported in this revision. The 800-172rev0 3.13.4e requirement to apply logical or physical isolation of the critical/High Value Asset system has been changed in 800-172rev3 03.13.04E to what will be interpreted as optional application of boundary protection measures.	Restore original 800-172rev0 3.13.4e requirement statement and discussion so this statement at line 316 will be correct and risk from APT will be addressed by requiring logical or physical isolation of the system.

4	Gary Guissanie NA (Self)	Technical	6	321	The statement at line 321 that authoritative sources for addressing changes to systems and system components is an essential element in addressing the APT is correct, but no longer supported by this revision. The original 800-172rev0 3.4.1e requirement for a authoritative source/repository was withdrawn replacing it with separate requirements to use trusted sources, but requires no capability to insure this is done properly.	Restore withdrawn 800-172rev0 3.4.1e requirement statement and discussion so this statement at line 321 will be correct and risk from APT will be properly addressed.
5	Gary Guissanie NA (Self)	Technical	6	323	The statement at line 323 that periodically refreshing/upgrading organizational systems and components is essential to addressing the APT is no longer supported in this revision. This was true in 800-172rev0 but now requirement has been changed such that refresh is not required -- requirement 03.14.04E does not require a refresh -- just that a trusted source be used IF a refresh is conducted.	Restore original 800-172 3.14.4e requirement statement and discussion so this statement at line 323 will be correct and risk from APT will be properly addressed.
6	Gary Guissanie NA (Self)	General	6	338	Text states that ODPs are used in certain enhanced security requirements. In fact, they are used in most of the requirements. The ODPs make it very difficult to apply 172 contractually, make many requirements overly vague, and are, for the most part wholly unnecessary. The need for each ODP should be re-evaluated and eliminated whenever possible.	Re-evaluate need for each ODP and eliminate whenever possible.
7	Gary Guissanie NA (Self)	Technical	11	461	Withdrawn requirement 03.01.03E, Secure Information Transfer, is not addressed by 03.01.09E (ABAC). It is partially addressed by the other listed requirements (03.01.10E and 03.01.03), but the intent of a focused protected and highly secure data transfer mechanism envisioned by 03.01.03E is NOT achieved by the cited requirements, which basically just relies on the 800-171 flow control requirement, which is inadequate.	Restore the original 800-172 secure information transfer requirement, associated discussion and 800-53 references (e.g., not just AC-04 but AC-04(1)(6)(8)(12)(13)(15).
8	Gary Guissanie NA (Self)	Technical	20	744	The withdrawn 03.04.01E 'Authoritative source/repository' is not fully addressed by the cited requirements (03.14.04E, 03.17.03E, 03.04.01, 03.04.03, 03.04.10). The intent was for organizations to establish a central repository that would ensure software/hardware was obtained only from authoritative sources, hence the requirement to: "'establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components". This requirement is now completely missing, replaced by requirements to use 'authoritative sources' without any mechanism to insure this actually will be accomplished.	Restore the original 800-172 03.04.01E authoritative source/repository' requirement and associated discussion and add cite for CM-08(07), Centralized Repository. Consider revising CM-08(07) 'Discussion' in future 800-53r6 to address functioning as a source of vetted, trusted SW.
9	Gary Guissanie NA (Self)	Technical	21	780	The Discussion for 03.04.03E mentions verifying configuration items based on the 'authoritative source' -- but what authoritative source? -- the 03.04.01E requirement to establish an authoritative source/repository was withdrawn.	Restore the original 800-172 03.04.01E authoritative source/repository' requirement and associated discussion.

10	Gary Guissanie NA (Self)	Technical	27	963	Requirement 03.05.06E states that identity proofing should be based on applicable standards and guidelines. There are such guidelines for USG, but not for contractors unless it means to point to 800-63A. If that is the case, requirement should reference that publication and the associated required Identity Assurance Level (IAL).	Provide appropriate references
11	Gary Guissanie NA (Self)	Technical	27	966	The statement "Resolve user identities to a unique individual' in 03.05.06Eb is unclear and will not be understood by many readers. Should be explained in the 'Discussion' section.	Explain meaning of 03.05.06b in Discussion section
12	Gary Guissanie NA (Self)	Technical	29	1045	In 03.06.03E Discussion the example of 'anomalous adversarial behavior' describes 'anomalous system behavior' ('changes in system performance or usage patterns') but not anomalous adversarial behavior (since it's what one might expect if an adversary were present).	Change 'anomalous adversarial behavior' to 'anomalous system behavior.'
13	Gary Guissanie NA (Self)	Technical	29	1056	Requirement 03.06.04 E ODP [Assignment: organization-defined automated mechanisms] is unnecessary	Replace ODP ('[Assignment: organization-defined automated mechanisms'] with 'automation' or 'automated mechanism.'
14	Gary Guissanie NA (Self)	Technical	29	1060	In Discussion for 03.06.04E, a Computer Incident Response Center is NOT an automated mechanism or a database.	Remove mention of CIRC.
15	Gary Guissanie NA (Self)	Technical	32	1149	The withdrawn 03.09.01E requirement is NOT addressed by 171r3 03.09.01, as that requirement addresses normal screening while the withdrawn 03.09.01E required 'enhanced personnel screening' - over and above the 03.09.01 normal screening - when required by the organization.	Restore 03.09.01E or simply withdraw requirement without reference to 800-171r3 requirement 03.09.01
16	Gary Guissanie NA (Self)	Technical	33	1176	Requirement 03.09.04E restriction of access to CUI to US citizens is too restrictive as it implies any CUI access versus when special circumstances apply -- requirement wording needs to be more nuanced. There is generally no prohibition for non-US citizens access to CUI, assuming there is a lawful govt purpose (e.g., UK subcontractor needs to receive or develop Controlled Technical Information). Some CUI may be restricted to US citizens while other categories of CUI may be restricted to US persons (i.e., US citizens and legal residents),	Add a conditional ODP incorporating text from the Discussion section or delete requirement as unnecessary (generally doesn't apply and is addressed via separate CUI dissemination requirements).
17	Gary Guissanie NA (Self)	Technical	34	1190	Requirement 03.10.01E Visitor Access Records - how is this requirement substantively different from what is in 171r3 requirement 03.10.02?	Delete requirement.
18	Gary Guissanie NA (Self)	Technical	36	1249	In 03.11.01E Requirement's Discussion, TTP's are not threat events but methods of operation. Best to move the parenthetical after 'threat information' and before 'threat events'.	Move the parenthetical after 'threat information' and before 'threat events'.
19	Gary Guissanie NA (Self)	Technical	38	1320	Neither the 03.15.02 171r3 nor 03.15.01E requirements address the essentials of the withdrawn 172 requirement 03.11.04E that the rationale for a specific security solution be identified (if that is the case) so it can be revisited when the threat changes.	Restore withdrawn requirement 03.11.04E. Address issue in future 800-53r6 with a revised PL-02 or addition of a CE. A new CE would allow transition 03.11.04E to new CE wording.

20	Gary Guissanie NA (Self)	Technical	38	1322	Only one of the specified requirements – 03.12.01 (171r3) -- marginally addresses the effectiveness of the security solutions to address the specific threat risk. 3.11.01E does not focus on reviewing effectiveness of security controls in light of changing threat and 3.11.01 (171r3). has absolutely nothing to do with the risk to effectiveness of security solutions based on threat.	Restore withdrawn requirement 03.11.05E
21	Gary Guissanie NA (Self)	Technical	38	1324	Substitute requirements for withdrawn requirement 03.11.06E do not address supply chain risk specifically except 03.11.01 (171r3) – but 03.11.01 is specifically about risk of unauthorized disclosure of CUI (as if disclosing CUI put the supply chain at risk), which is not relevant. However, while not explicitly using the supply chain term, 03.17.03E seems to address one aspect (counterfeits) of issue.	Restore withdrawn requirement 03.11.06E and point to RA-03(01) or rephrase to align with RA-03(01): "Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain."
22	Gary Guissanie NA (Self)	Technical	47	1622	03.13.04E reads as if this is a simple boundary protection control and separation/isolation is optional and might only apply to certain components of the system in question, when the intended requirement (in 172r0) is to physically or logically isolate the critical/High Value Asset 'system' or 'segment' from the 'existing' system. This is the core 172 requirement. Requirement should be reworded similar to original requirement and apply to organization defined 'systems and system components' – not just components.	Replace requirement statement and Discussion with text from 800-172r0 requirement 3.13.4e. As an alternative, revise to read "Isolate system and system components, physically or logically, using [Assignment:] boundary protection measures" and modify SC-07 CE to add CE SC-07(27)(28)(29) & modify, if needed (e.g., replace 'external' to 'network' in SC-07(27)) or create new CE.
23	Gary Guissanie NA (Self)	Technical	55	1872	Withdrawn requirement 03.14.03E was intended to address issues within a critical/High Value Asset system with any IoT or OT that are incapable of meeting security requirements, requiring they either comply with the security requirements or be segregated into a subnetwork where they can be securely managed. The withdrawn requirement should be restored as the 3 referenced requirements do not address this issue.	Restore withdrawn requirement 03.14.03E and cite (in addition to SA-08, SC-07 and PL-08), SC-49 (Hardware-Enforced Separation and Policy Enforcement)

24	Bradley Lanford DoD/OUSD(R&E)/ S&T Program Protection	Technical	55	1875	The original 172r0 3.14.4e requirement to mandate a periodic refresh of system components from a trusted source is missing in this rewrite. The intent is to require a periodic refresh to drive out an established APT presence (and, of course, to use a trusted source for the refresh). This, along with physical/logical isolation of the critical/High Value Asset system - was the most important 172 requirement. This rephrasing of that requirement completely misses the point, and seems to make the refresh optional, and just require, if a refresh is done, it should be from a trusted source. This is likely a result of using the 800-53r5 SI-14(01) Control Enhancement wording without including text from the SI-14 control. Restore the original 172rev0 requirement statement and discussion.	Restore the original 172rev0 requirement statement and discussion. As an alternative, revise new requirement to merge SI-14 (and its 'non-persistence' requirement) and SI-14(01) so the requirement to refresh periodically is clearer. This is not an issue with 800-53 since SI-14(1) implies also SI-14, but this is lost by using just the SI-14(1) text in 172r3.: "Implement non-persistent [Assignment: organization-defined system components and services] that are initiated in a known state, with software and data from the following trusted sources: [Assignment: organization-defined trusted sources] and terminated periodically at [Assignment: organization-defined frequency]"
25	Gary Guissanie NA (Self)	Technical	56	1908	The intent of the withdrawn 03.14.07E requirement to "verify the correctness of critical SW" is completely lost by diluting it among 5 requirements scattered about, none of which actually address the 'correctness' requirement. Need to retain the overarching 'correctness' requirement.	Restore the withdrawn 03.14.07E requirement, or, if impractical, simply withdraw it without reference to the other, added, requirements.
26	Gary Guissanie NA (Self)	Technical	63	2114	The Discussion sentence for 03.14.17E beginning with "In contrast" seems more appropriate to 03.14.18E below. The discussion sentence for 03.14.17E should say "in contrast to alerts generated by the organization, alerts generated by the system ....)."	Revise Discussion text as suggested in comment.
27	Gary Guissanie NA (Self)	Technical	63	2134	The Discussion sentence for 03.14.18E beginning with "In contrast" seems more appropriate to 03.14.17E above. The discussion sentence for 03.14.18E should read "In contrast to alerts generated by the system, alerts generated by the organization ....)."	Revise Discussion text as suggested in comment.
28	Gary Guissanie NA (Self)	Technical	66	2215	Requiring sourcing from different 'suppliers' can be misinterpreted as the same product from different sellers.	Rephrase requirement to specify use of different products (similar to explanation in Discussion).
29	Gary Guissanie NA (Self)	Technical	68	2276	First sentence in Discussion for 03.17.02E doesn't make sense -- how do you 'inspect for detection' or for tamper resistance? Revise to read 'inspect for evidence of tampering'.	Revise to read 'inspect for evidence of tampering.'