

Michael Seeds

Jan 16, 2026, 1:30:47 PM

to 800-171comments@list.nist.gov

Hello, Sir or Madam.

Attached are NDIA's comments for SP 800-172 Rev3 and SP 800-172A Rev3. Thank you for your consideration.

Best,

**Michael Seeds**

Senior Director, Strategy & Policy

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
11	NDIA	Technical	Assessment Procedures	NA	Assessment guidance strongly influences implementation behavior. Without assessable objectives related to AI-enabled analytics and decision-support tools, organizations may not	Align SP 800-172 and SP 800-172A by identifying assessable evidence for AI-enabled security capabilities, such as documentation of AI-assisted tools, governance for model

					operationalize protections beyond baseline technical controls, leaving cognitive and analytic risks unaddressed.	changes, and procedures demonstrating effective human oversight of high-impact decisions.
12	NDIA	General	5	1	Printed copies of this document are likely to be created. Printed documents are easier to read in a serif font.	Use a serif font.
13	NDIA	Editorial	9	450	More correctly, this should be TKPC, not "two-person control". There are multiple occurrences of this in the document (lines 450, 870, 997, 1292, others).	Use "two knowledgeable person control (TKPC)" instead of "two-person control".
14	NDIA	Editorial	13	556	Detection of "atypical" behavior implies that a baseline of "typical" behavior has been established.	Add verbiage to require the creation and maintenance of an organizational baseline of "typical" behavior.
15	NDIA	Technical	17	693	Should this be "binary objects" instead of "bitmap objects"? Audio files are not	Change the wording from "bitmap objects" to "binary objects".

					bitmaps. Not all unstructured data is stored as bitmaps.	
16	NDIA	Editorial	31	1112	Is the intent to prohibit the storage of all static authenticators, or just those which are unencrypted? If the latter, please consider rewording for clarity.	Suggested rewording for clarity "Static authenticators stored in applications or other forms of static storage must be encrypted. The storage of such authenticators in plaintext is prohibited".
17	NDIA	Editorial	35	1248	Detection of "anomalous" behavior implies that a baseline of "typical" behavior has been established.	Add verbiage to require the creation and maintenance of an organizational baseline of "typical" behavior.
18	NDIA	Editorial	40	1406	A citizenship requirement, while important, may not be sufficient to protect CUI from the threat posed by a malicious insider.	Consider adding criminal background checks for individuals having access to CUI.
19	NDIA	Technical	59	2003	Other types of physical ports exist, including fiber optic and	Change wording in the description to specify "all

					RJ-45 (I am surprised that one was not listed).	unused physical ports" instead of listing certain port types, such as USB, Thunderbolt, etc.
20	NDIA	Technical	59	2018	While this requirement is desirable, it may not be sufficient for detection of malicious email attachments or applications. Certain malware will detect the presence of a virtualized environment and not exhibit malicious activity if being executed there.	Consider warning users that this requirement alone may be insufficient to protect them from executing malware.
21	NDIA	Editorial	84	2803	TKPC is missing from the acronym list.	Add TKPC (two knowledgeable person control) to the acronym list.

22	NDIA	Editorial	NA	NA	NDIA would suggest a greater emphasis on continuous monitoring in general. The 171 references a ConMon strategy at section 03.12.03. The 172 has a section devoted to security assessments and monitoring. My suggestion would be expanded requirements on ConMon such that all other controls are not only executed at their defined cadence, but also “meta” monitored to ensure that they are being executed and implemented properly. This ensures that the process isn’t simply generating a “garbage-in, garbage-out” type of scenario, but rather ensures	NA
----	------	-----------	----	----	--	----

					<p>that the implementation matches the requirements. For example, an organization may have a defined patching policy such that they “patch” their systems monthly. However, a meta monitoring would review what was actually installed and ensure there are no gaps (unpatched vulnerabilities, for example), that all patchable software is being addressed and so forth. Otherwise, they are simply concurring with their own internal review as part of a ConMon requirement. This enhancement would facilitate the requirements of</p>	
--	--	--	--	--	--	--

					a risk-based process to mitigate APTs.	
--	--	--	--	--	--	--

23	NDIA	Technical	64	1773	NDIA recommends moving the three SC-30 sourced controls to 800-171 so they will be referenced and applied by the broadest possible set of organizations within the Defense Industrial Base. SC-30 is a cheap-to-implement compensating control that materially reduces the attack surface of imperfectly defended systems while increasing the cost to adversaries of finding and executing attacks. While our corporate members strive to meet the technical spirit and letter of 800-171 and, where applicable, 800-172 the general consensus is most implementation	Shift 03.13.02E, 03.13.03E, and 03.13.05E to NIST 800-171.
----	------	-----------	----	------	--	--

					<p>s--especially amongst smaller business members and new market entrants--are, in practice, quite flawed. By placing the SC-30 referenced controls in 800-172, NDIA believes NIST is signaling to the market that this control should neither be funded nor considered except under exceptional circumstances. This runs exactly opposite to the intent of 800-160 Vol 2.</p>	
--	--	--	--	--	--	--