

Gabrielle Gerecht

Jan 16, 2026, 9:26:18 AM
to 800-171comments@list.nist.gov,

Dear NIST team,

On behalf of OpenPolicy and our coalition of innovative cybersecurity organizations, I am pleased to submit our comments on the Final Public Draft of NIST SP 800-172r3, *Enhanced Security Requirements for Protecting Controlled Unclassified Information*, and the Initial Public Draft of NIST SP 800-172Ar3, *Assessing Enhanced Security Requirements for Controlled Unclassified Information*.

We appreciate NIST's continued leadership in strengthening protections for CUI. Our recommendations focus on enhancing cyber resiliency for critical systems and high-value assets, including strengthened supply chain risk management, integrity of software, firmware, and update mechanisms, continuous monitoring and verification, and governance of emerging technologies across complex, interconnected environments. We aim to help ensure that the enhanced security requirements and associated assessment procedures remain both robust and practical for implementation across diverse nonfederal IT, OT, cloud, and hybrid systems.

Thank you for the opportunity to provide input. We would be happy to discuss any aspect of our comments or provide additional information that may support the revision and assessment development process.

Best,

Gaby Gerecht

--

Gaby Gerecht
Director, Cybersecurity & AI Policy

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	OpenPolicy	Editorial	96	3148	This would mirror SP 800-171 where the requirements are mapped to 800-53 controls and provide easy alignment for auditors to skim and know the reference without having	Include a cross-reference column to the source 800-53 control for each enhanced security requirement under Appendix C.

					to find it in the procedures section.	
2	OpenPolicy	Editorial	102	N/A	Appendix C goes into greater detail and depth about the values included in “depth and coverage attributes” means. Appendix D only points to Appendix C.	Revise the final sentence in footnote 7 to say SP 800-53A [5], Appendix C, beginning on page 708, provides additional guidance on depth and coverage attributes
3	OpenPolicy	Technical	94	Before 3112	In the glossary, provide the definition of an independent assessor that aligns with SP 800-53A. Reference Ch. 3, page 22.	An independent assessor is any individual capable of conducting an impartial assessment of security and privacy controls employed within or inherited by a system. Impartiality implies that security and privacy control assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or

						management of the system or the determination of security and privacy control effectiveness
4	OpenPolicy	General	103	3243	SP 800-172Ar3 does not currently include an evidence log template or example structure to help assessors document findings consistently. Including a standardized or sample evidence log would improve consistency across assessments and streamline reporting, especially for multi-system or multi-organization reviews. It would also support reuse and traceability across OSCAL, POA&M documentation, and audit artifacts.	Include a sample evidence log template in Appendix D or as a supplemental attachment.

5	OpenPolicy	Editorial	N/A	N/A	<p>SP 800-172r3 references “artifacts” that can support assessments but gives limited examples beyond documents. This could lead to overreliance on manual records instead of structured system outputs.</p>	<p>In Appendix D clarify that artifacts may include structured data from SIEMs, CMDBs, and runtime monitoring systems, and highlight the value of integrating GRC and OSCAL-compatible platforms as artifact sources.</p>
6	OpenPolicy	Technical	N/A	N/A	<p>SP 800-172Ar3 is well-structured for automation but is not provided in OSCAL format, which limits integration with tooling, continuous monitoring, and real-time validation</p>	<p>Publish SP 800-172Ar3 assessment procedures in OSCAL format to support automation, alignment with FedRAMP</p>