

Lorenzo Vacca

Jan 6, 2026, 9:12:03 AM
to 800-171comments@list.nist.gov

Dear NIST Team,

This email is submitted in response to NIST’s request for public commentary on NIST Special Publication 800-172 Revision 3 and NIST Special Publication 800-172A Revision 3. Please find attached the two files provided in accordance with the provided templates. The documents contain the consolidated commentary produced by the dedicated ISSA Task Force.

We thank you for the opportunity to contribute and for your time and attention in reviewing these materials.

We remain available for any clarification or follow-up discussion.

Kind regards,

Lorenzo Vacca
Director of Industry Outreach
ISSA Special Interest Group on Cyber Resilience

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Issa Special Interest Group on Cyber Resilience	Technical	71	New line	The discussion already stresses enterprise alignment, dependencies, interfaces, and restoration, but not artifact/cadence for audits.	Add a new requirements

2	Issa Special Interest Group on Cyber Resilience	General	73	2462	Make a required pre-deployment test	Test for adverse cross-control interactions
3	Issa Special Interest Group on Cyber Resilience	Technical	73	2482	No planning criteria to prevent monocultures or fragility	Added a shall statement to avoid single-vendor monocultures and call out per architectural layer;
4	Issa Special Interest Group on Cyber Resilience	General	71	New line	Tie all planning enhancements together as a deliverable	Integrate three sub Planning topics into one security architecture package.
5	Issa Special Interest Group on Cyber Resilience	Technical	74	New line	Convert planning concepts into assessment checks for repeatability	Requires assessment checks for each planning sub topic
6	Issa Special Interest Group on Cyber Resilience	Technical	72	New line	A testable design outcome is missing	Doc. how each layer contains blast radius and how monitoring helps detect layer bypass
7	Issa Special Interest Group on Cyber Resilience	Technical	37	1296	ODP: time period - lacks timeframe	A range should be defined

8	Issa Special Interest Group on Cyber Resilience	Technical	48	1642-1643	ODP: frequency - lacks specificity	A range should be given
---	---	-----------	----	-----------	------------------------------------	-------------------------