

Derek Kernus

Jan 16, 2026, 7:59:10 AM
to 800-171comments@list.nist.gov,

Good morning,

Attached are comments from the MSPs for the Protection of Critical Infrastructure.

Derek Kernus

Policy & Standards

MSP Collective

Comment #	Submitted By (Name/Org): *	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Aethon Security	General	9	446	Enforcing dual authorization is ideal for organizations that can implement it, but what if the organization being evaluated only has one user?	There are multiple "micro small" businesses like this supporting the government and this control would be impossible for them to implement. There should be an alternative option for those smaller organizations. Consider limiting to a risk level. For

						example, required for anything over moderate or specific technical controls for anything over moderate and procedural for anything moderate and below. Clarify if MSSP can be an authorizing party.
2	Aethon Security	General	11	513	The Discussion section is lacking in fully explaining how wearable devices will be used in employing automated mechanisms to monitor and control remote access methods.	Remove "wearables" or clearly define how wearables would be implemented.
3	Aethon Security	General	21	822	The current Discussion section does not give examples of counterfeit system	Suggest adding some examples like integrated circuits (ICs), End-of-Life (EOL) components

					components .	that are increasingly targeted by counterfeiters, recycled or refurbished parts, etc.
4	Aethon Security	General	23	870	Enforcing dual authorization is ideal for organizations that can implement it, but what if the organization being evaluated only has one user?	There are multiple "micro small" businesses like this supporting the government and this control would be impossible for them to implement. There should be an alternative option for those smaller organizations.
	Aethon Security	General	27	997	Enforcing dual authorization is ideal for organizations that can implement it, but what if the organization being evaluated only has one user?	There are multiple "micro small" businesses like this supporting the government and this control would be impossible for them to implement. There should be an alternative option for

						those smaller organizations.
6	Aethon Security	General	27	1017	Vague in terms of scope and retention. There is risk to consider with rolling back to previous configurations in terms of vulnerabilities or outdated configurations causing error.	Consider including the requirement to clearly document the vulnerabilities associated with previous baselines. Consider defining minimums to alleviate burden of documentation which would be the most cost effective for small businesses.
6	Aethon Security	General	36	1292	Enforcing dual authorization is ideal for organizations that can implement it, but what if the organization being evaluated only has one user?	There are multiple "micro small" businesses like this supporting the government and this control would be impossible for them to implement. There should be an

						alternative option for those smaller organizations.
7	Aethon Security	General	37	1315	Enforcing dual authorization is ideal for organizations that can implement it, but what if the organization being evaluated only has one user?	There are multiple "micro small" businesses like this supporting the government and this control would be impossible for them to implement. There should be an alternative option for those smaller organizations.