From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] 800-171 rev 3 fpd comments
Date: Thursday, January 4, 2024 2:43:26 PM
Attachments: image001.png
sp800-171r3-fpd-comment_Totem-Technologies.xlsx

Thank you for the opportunity to submit comments on the -171 rev 3 fpd. Please find comments from Totem Technologies attached.

Very respectfully,

Adam Austin | Co-founder, CTO, and Cybersecurity Lead
Totem.Tech | 1972 W 2550 S Suite B, West Haven, UT 84401
[redacted]
www.totem.tech
[redacted]

Book a meeting with me!

*** Do not send Controlled Unclassified Information (CUI) in the body or as an attachment to this email address. If you have CUI you must send me, and do not have a method of secure transmission, please let me know and I'll provide an alternate transmission method. ***

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Totem Technologies	Technical	publication	43	1546	3.10.7: can NIST provide examples on how to "control egress" from a facility? Is this implying an individual must authenticate him/herself to _exit_ the building? Is this requirement obviated during times of emergency evacuation? What about exit doors that must, to meet fire code, must have panic bars installed?	Remove "and egress" in 3.10.7(a)(2) and change "or" to "and" in 3.10.7(b)
2	Totem Technologies	Technical	publication	47	1689	the bracketed ODP text suggests a non-disclosure agreement between two organizations as a sufficient "exchange agreement" for this control. Is that NIST's intention, or would an NDA require an additional form of exchange agreement between the organizations, such as an SLA? For instance, an NDA would typically not include an interface control description (ICD), but an ICD is required by part b of this control as well.	Remove nondisclosure agreement as an option for a document to manage exhange of CUI, or indicate that multiple of the suggested documents must be maintained

* indicate required fields

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
3	Totem Technologies	Technical	publication	49	1770	Why did NIST remove the requirement for content filtering services? NIST says this is ORC or addressed by other controls now?	We think it's a good idea to keep some sort of content filtering service as an explicit requirement. Just clarify that in addition to "proxy" servers, other services, such as application layer firewalls, DNS filtering, etc. can suffice.
4	Totem Technologies	Technical	publication	57	2077	What is the difference between 3.16.1 and 3.16.3a?	Merge 3.16.1 and 3.16.3. Remove redundant controls requiring inclusion of security requirements into subcontracts and supplier agreements.
5	Totem Technologies	Technical	publication	59	2146	Maintaining an SCRM Plan implies implementation of the plan. By meeting 3.17.1, an organization will meet 3.17.2 and 3.17.3.	Consolidate the SCRM family into one control that organizations develop and implement an SCRM Plan. We understand that NIST would like to make the number of families in 800-171 consistent with the number of families in 800-53, but the proposed SCRM family in 800-171 rev 3 fpd could be consolidated down to one control in the Risk Assessment family.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
6	Totem Technologies	Technical	publication	82	2901	Maintenance of a Configuration/Change Management Plan (CMP) most definitely contributes to protecting the confidentiality of CUI. Not sure why CM-09 was re-tailored from NFO to NCO.	Instead of recategorizing CM-09 from NFO to NCO, make managing a CMP a firm requirement of 3.4.3.