From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Review of Rev3 as of Nov 2023
Date: Wednesday, November 22, 2023 1:59:24 PM
Attachments: sp800-171r3-ipd-comment-SoundWay.xlsx

Good day Mr. Ross and Ms. Pillitteri,

Attached you will find 8 items identified for review by NIST.

Wishing you and your teams a safe and wonderful Thanksgiving.

Sincerely,

Carter

Carter Schoenberg, CISSP | CCA | QTE
Vice President and Chief Cybersecurity Officer
[redacted]
www.soundwayconsulting.com

SoundWay
Consulting Incorporated
www.soundwayconsulting.com

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Carter Schoenberg, SoundWay Consulting, Inc.	Technical		39	1417	As with rev2, there is no requirement to "back up" only to ensure if it occurs, that it is encrypted. Assuming by incorporated reference will not work.	Create a requirement to actually backup system resources that are critical to the safeguarding of CUI.
2	Carter Schoenberg, SoundWay Consulting, Inc.	Editorial	Associate by reference https://pages.nist.gov/GCTC/uploads/blueprints/2020-GCTC-CPAC-C-SCRM.pdf	15	499	NIST is assuming that organizations are aware of what should be in an SLA or T&Cs. This is not factually correct. Guidance should expound further.	Provide referenceable materials for what should be in an SLA or T&C of a service provider at a minimum (Access Control, Media Protection, Incident Response ,etc)
3	Carter Schoenberg, SoundWay Consulting, Inc.	Editorial		21	711	Assumes all GovCons will incorporate a SIEM.	NIST should allow the system owner to evaluate other means of achieving the goals of 3.3.6 without the purcahse of a SIEM and still be in conformance. Especially for micro-sized businesses.
4	Carter Schoenberg, SoundWay Consulting, Inc.	Technical		22	772	(a) is incomplete due to assumption. Narrative refers to "system" gloassary says system = information system yet assumes the reader fully understands what constitutes information system resources.	Include system defintion earlier in doc or at this control (endpoints, servers, etc.)

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
5	Carter Schoenberg, SoundWay Consulting, Inc.	Technical		55	2017	(a) is to generalized and does not implicityly imply a "policy" is necessary to address all 17 control families.	"Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements ***across all security families defined herein*** ."
6	Carter Schoenberg, SoundWay Consulting, Inc.	editorial		57	2076	no alpha character exists to describe the requirement objective(s) yet the narrative on 2077 describes "the following security requirements"	ensure objectives are created to align with "the following security requirements"
7	Carter Schoenberg, SoundWay Consulting, Inc.	general		59	2148	NIST does not properly identify all elements of a SCRM. It cannot include words described in 2156-2158 and not include ramifications assocaited with "financial impacts".	d. Develop a plan for determing cost exposure to a crisis event stemming from the supply chain and manage SLAs/T&Cs to offset exposure to an acceptable level of risk. (ie. Cyber liability insurance)
8	Carter Schoenberg, SoundWay Consulting, Inc.	editorial				no alpha character exists to describe the acquisition strategies, etc.	ensure objectives are created to align with line 2177-2178.