From: via 800-171comments

To: 800-171comments@list.nist.gov

Subject: [800-171 Comments] NIST SP 800-171 Comments - Peraton (July 2023)

Date: Wednesday, July 12, 2023 6:37:38 PM

Attachments: Copy of Copy of sp800-171r3-ipd-comment-template - Peraton Comments -July 2023 - GG.xlsx

PERATON CONFIDENTIAL AND/OR PROPRIETARY INFORMATION - This email message and/or its attachment contains confidential and/or proprietary information of Peraton Corp. (Peraton) that may only be received, disclosed, or used as authorized by Peraton. The information in this message may be exempt from release under the Freedom of Information Act. If you received this message in error, please delete all copies, and promptly notify the sender.

NIST,

Attached are the Peraton Corporation comments to the subject document.

Regards, Gregg

Gregory A. Garrett, CISSP, CISM, CPCM, PMP, ITIL 4

Vice President, Cybersecurity Capabilities

Peraton



Peraton

1

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
							Add a discussion of least privilege
1	Garrett/Peraton	Technical	N/A	5	138	Revise Discussion Section	access (LPA approach to access control
							Add the use of Zero Trust Architecture
							(ZTA) design tenets for access control
2	Garrett/Peraton	Technical	NIST 800-207	6	167	Revise Discussion Section	policies
							Add the use of Cloud Based Internet
							Isolation (CBII) technologies to be
2	Carrott/Daraton	Tochnical	CIEV OD 33 03	6	102	Pavisa Discussion Castion	consistent with the CISA Operational Directive 23-02
3	Garrett/Peraton	Technical	CISA OD 23-02	6	183	Revise Discussion Section	Add awareness techniques include:
							cyber training presentations, podcasts,
4	Garrett/Peraton	Technical	N/A	15	541	Revise Discussion Section	videos, and webinars
	Carretty i cratori	recimiea	14774	13	311	nevise biseassion section	Viacos, and vicemans
							Training should include the use of Table-
							Top Exercises, cyber-ranges with cyber-
							attack scenarios, and case study based
5	Garrett/Peraton	Technical	MITRE ATT&C	16	570	Revise Discussion Section	cyber-attack exercises
							Add the use of graphic software for
							visualization tools significant enhances
							the documentation and analysis of
							software, hardware, and firmware
	Garrett/Peraton	Technical	Peraton Labs	21		Revise Discussion Section	configuration management
7	Garrett/Peraton	Technical	NIST 800-207	27	1000	Revise Discussion Section	Add the use of MFA as a part of ZTA
							Add: Test the incident Response Plan at
							least twice a year via Table Top Cyber
							Exercises or via the use of cyber-range
0	Garrett/Peraton	Technical	Poraton Labs	31	1150	Add new subtask (d.)	simulations with senior leadership involvement
	Garrett/Peraton	recrimical	Peraton Labs	51	1156	Add flew subtask (d.)	mvoivement
							Add: CISA and FBI Cyber Incident and
9	Garrett/Peraton	Technical	FBI Cyber Aleri	32	1192	Add to the REFERENCES	Data Breach Reporting Information
	- Carretty : Cratori		. 5. 6,56. 7		1132	rida to the HEI EHEITOES	Add: The use of cyber-ranges with
							emulated networks and simulated
							cyber-attacks using the MITRE Cyber
							ATT&CK Framework or MITRE DEFEND
10	Garrett/Peraton	Technical	MITRE ATT&C	32	1220	Revise Discussion Section	Framework
							Add: Conduct periodic Cybersecurity-
							Supply Chain Risk Management (C-
							SCRM) assessments of high risk
							suppliers, especially the Software Bills
11	Garrett/Peraton	Technical	NIST 800-161	42	1580	Add new subtask (c.)	of Materials (SBOMs)
4.5	C	Tarabas I	NCA A-L · ·		2000	Device Discouri C. II	Add: the NSA Cyber Advisories and FBI
12	Garrett/Peraton	Technical	NSA Advisories	54	2063	Revise Discussion Section	Cyber Alerts
							Add. (a.) Conduct naviadia
							Add: (c.) Conduct periodic independent cyber risk assessments of
							high risk suppliers and (d.) Ctreate a C-
							SCRM Dashboard to identify and track
							cyber supply chain high to moderate
13	Garrett/Peraton	Technical	NIST Third-Par	60	2305	Add new subtasks (c.) and (d	