From:	[redacted] 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

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

[redacted]

Peraton

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Garrett/Peraton	Technical	N/A	5	138	Revise Discussion Section	Add a discussion of least privilege access (LPA approach to access control
2	Garrett/Peraton	Technical	NIST 800-207	6	167	Revise Discussion Section	Add the use of Zero Trust Architecture (ZTA) design tenets for access control policies
3	Garrett/Peraton	Technical	CISA OD 23-02	6	183	Revise Discussion Section	Add the use of Cloud Based Internet Isolation (CBII) technologies to be consistent with the CISA Operational Directive 23-02
4	Garrett/Peraton	Technical	N/A	15	541	Revise Discussion Section	Add awareness techniques include: cyber training presentations, podcasts, videos, and webinars
5	Garrett/Peraton	Technical	MITRE ATT&CK	16	570	Revise Discussion Section	Training should include the use of Table-Top Exercises, cyber-ranges with cyber-attack scenarios, and case study based cyber-attack exercises
6	Garrett/Peraton	Technical	Peraton Labs	21	779	Revise Discussion Section	Add the use of graphic software for visualization tools significant enhances the documentation and analysis of software, hardware, and firmware configuration management
7	Garrett/Peraton	Technical	NIST 800-207	27	1000	Revise Discussion Section	Add the use of MFA as a part of ZTA
8	Garrett/Peraton	Technical	Peraton Labs	31	1158	Add new subtask (d.)	Add: Test the incident Response Plan at least twice a year via Table Top Cyber Exercises or via the use of cyber-range simulations with senior leadership involvement
9	Garrett/Peraton	Technical	FBI Cyber Alert	32	1192	Add to the REFERENCES	Add: CISA and FBI Cyber Incident and Data Breach Reporting Information
10	Garrett/Peraton	Technical	MITRE ATT&CK	32	1220	Revise Discussion Section	Add: The use of cyber-ranges with emulated networks and simulated cyber-attacks using the MITRE Cyber ATT&CK Framework or MITRE DEFEND Framework
11	Garrett/Peraton	Technical	NIST 800-161	42	1580	Add new subtask (c.)	Add: Conduct periodic Cybersecurity-Supply Chain Risk Management (C-SCRM) assessments of high risk suppliers, especially the Software Bills of Materials (SBOMs)
12	Garrett/Peraton	Technical	NSA Advisories	54	2063	Revise Discussion Section	Add: the NSA Cyber Advisories and FBI Cyber Alerts
13	Garrett/Peraton	Technical	NIST Third-Par	60	2305	Add new subtasks (c.) and (d.)	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 risk factors/suppliers