From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments on Draft 1 of NIST 800-171 Revision 3
Date: Friday, May 19, 2023 10:05:03 PM
Attachments: sp800-171r3-ipd-comment-template_Jacob Hill-GRC Academy.xlsx

---

Good Evening,

Thank you for the excellent work on revision 3 of NIST 800-171! I really appreciate the positive changes.

I've attached my comments which are summarized below:

1. Add a data retention requirement for CUI.
2. Align with NIST 800-53 terminology by renaming "security requirement" to "security control."

Thank you again and have a great weekend!

Jacob Hill, CEO (CISSP-ISSEP | CEH | ITIL v3)
GRC Academy: a training and research platform for GRC professionals and SMBs
[redacted]
[redacted] | LinkedIn

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Jacob Hill / GRC Aca	Technical		89	3048	After fulfilling a contract, it is common for companies to continue storing sensitive customer data within their systems, sometimes indefinitely. However, this practice brings unnecessary liability to the company and increases the risk of the information being compromised. It is critical that NIST 800-171 r3 includes data retention requirements for CUI. Without a security control in place, CUI will persist on nonfederal systems even after contracts have concluded, leaving the information vulnerable to compromise. The security control text might look like this: “Establish and implement a data retention policy which	Add a security control to address data retention. This control would map to SI-12 which was tailored out as "FED."
2	Jacob Hill / GRC Aca	Editorial		1	18	NIST 800-53 calls them "securi	Align terminology with NIST 800-53 by renaming "security requirements" to "security controls."