

From: 800-171comments@list.nist.gov on behalf of [REDACTED]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comment Submission
Date: Thursday, July 13, 2023 1:51:53 PM
Attachments: [sp800-171r3-ipd-comment EY.xlsx](#)

Hi,

Please see attached comments. Thank you for the consideration.

Thanks,
Mitch



Mitchell Hayes | Consulting - Technology Risk

Government and Public Sector

Ernst & Young, LLP

[REDACTED]
Website: <http://www.ey.com>

Any tax advice in this e-mail should be considered in the context of the tax services we are providing to you. Preliminary tax advice should not be relied upon and may be insufficient for penalty protection.

The information contained in this message may be privileged and confidential and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by replying to the message and deleting it from your computer.

Notice required by law: This e-mail may constitute an advertisement or solicitation under U.S. law, if its primary purpose is to advertise or promote a commercial product or service. You may choose not to receive advertising and promotional messages from Ernst & Young LLP (except for My EY, which tracks e-mail preferences through a separate process) at this e-mail address by opting out of emails through EY's [REDACTED]. Our principal postal address is [REDACTED]. Thank you. Ernst & Young LLP

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	EY	General		7	234	There is not a specific requirement to review access to CUI. Could this requirement be expanded (or a requirement added) to include the periodic review of all individuals or privileges that have access to CUI?	Incorporate periodic review of CUI access permissions
2	EY	General		16	578	Is the intent for the frequency of the advanced literacy training to occur in line with the frequency assigned in 3.2.1?	Add a frequency definition to 3.2.3
3	EY	General		32	1194	3.6.3 Does not contain requirements of how to use the test to improve processes.	Potentially add a requirement that the lessons learned from the test be used to update the incident response plan or trainings accordingly, as well as document results of the test.
4	EY	General		44	1655	Unsure if control assessments required by 3.12.1 have to be performed by independent assessors (3.12.5), or if the intent is to have internal organizational assessments as well as external assessments.	Clarify internal and external assessment requirements, and potentially the frequency of independent assessors. Also include a definition of what an 'independent' assessor is. What is the output of the assessment?
5	EY	General		N/A	N/A	Control families are not aligned between 800-53 and 800-171.	Align families for consistency (ex. "Security Assessment and Monitoring" in 800-171 aligns to "Assessment, Authorization, and Monitoring" in 800-53

* indicate required fields