[redacted] [redacted]

Subject: RE: NIST 800-171 r3 Late Feedback
Date: Thursday, February 1, 2024 2:06:17 PM

From: Jacob Hill @ GRC Academy <[redacted]
Sent: Monday, January 29, 2024 9:46 PM
To: Ross, Ronald S. (Fed) <ronald.ross@nist.gov>
Subject: NIST 800-171 r3 Late Feedback

Hi Ron,

[redacted]

I have attached my comments. I understand if it is too late, I just wanted to try because I believe they are important.

[redacted]

Have a great week!

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

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 / GRCAcademy.io	Technical	Publication	30	1062	3.5.7, "Password Management" should include a requirement to address password reuse. When users reuse passwords among their system accounts, and the password for one of those accounts is compromised, then all of those accounts which also use that password are in danger of being compromised. Password reuse is widely recognized as one the top problems with passwords. I see that 3.5.8 was withdrawn which may initially seem to be related to my suggestion, but my suggestion addresses the problem of password reuse among different accounts, not specifically to individual password changes.	Even when password managers are in use to generate unique and randomized passwords for accounts, the elimination of ALL password reuse may not be possible. The security requirement could be written like this: Require users to limit password reuse among accounts to less than 15%. An ODP could be used in place of the percentage. Authorized password managers can display users' password reuse compliance statistics.

* indicate required fields

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
2	Jacob Hill / GRCAcademy.io	Technical	Publication	31	1111	This is a tough one. Some of the requirement text of 3.5.12, "Authenticator Management" is directly related to 3.5.7, "Password Management," and not showing it in 3.5.7 could cause confusion. 3.5.12d: "Change default authenticators at first use." In my opinion in the context of a federal contractor, this requirement likely would only apply to passwords. I could be wrong? Additionally, 3.5.12d is quite close to 3.5.7e, "Select a new password upon first use after account recovery." Having similar controls like this in separate requirements seems strange. 3.5.12e: "Change or refresh authenticators periodically or when the following events occur: [Assignment: organization-defined events]" This requirement could apply to different types of authenticators such as passwords, certificates, etc, so I understand its placement here, but the absence of a requirement to "change passwords when there are indicators of compromise" in 3.5.7 is odd.	1. Consider placing 3.5.12 closer in sequence to 3.5.7 to show the relationship? 2. Consider moving 3.5.12d ("Change default authenticators at first use") into 3.5.7. 3. Consider also showing 3.5.12e under 3.5.7? ("Change or refresh authenticators periodically or when the following events occur: [Assignment: organization-defined events]") - If action item (1) can be completed, then this request is not as important. I'm just nervous that password change requirements will be forgotten because it isn't in 3.5.7.