From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Amira Armond / Kieri Solutions LLC comments
Date:	Wednesday, July 12, 2023 11:06:15 AM
Attachments:	sp800-171r3-ipd-comment_AmiraArmond_KieriSolutions.xlsx

---

Best regards,

V. Amira Armond
Kieri Solutions - Resilient IT
[redacted]

This email address is approved for communication up to Federal Contract Information (FCI). For transfer of Controlled Unclassified Information (CUI) or higher, please contact me for secure file transmission methods.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Amira Armond / Kieri Solutions LLC	General	publication	5	115	Re-using the same requirement ID numbers as 800-171 Rev. 2 for changed and different requirements creates conflicts with existing company documentation. For my own company and our clients, re-use of the IDs will necessitate managing two system security plans, one for Rev. 2 and one for Rev. 3, rather than a single plan which cross-references between the versions. Long term, as 800-53 and 800-171 are updated, utilizing the same numbering scheme as 800-53 will reduce rework by both NIST authors and nonfederal organizations. My company and clients would prefer gaps in the numbering to having to re-ID every requirement in our our documentation as new versions are released.	Modify requirement numbering to utilize the unique IDs for 800-53r5 For example, rather than 3.1.1 [a], list AC-02 as the ID.
2	Amira Armond / Kieri Solutions LLC	General	publication	2	30	Rev 3 continues to impose arbitrary IDs for the requirements which will change again in future versions. Every defense contractor will need to spend 10-20 hours re-organizing their compliance documentation each time the IDs are changed. It would be better to utilize an ID scheme that will not change with each revision. Since 800-53 is the source of the controls, and is unlikely to change its ID scheme, it makes sense to utilize 800-53 control IDs.	Modify requirement numbering to utilize the unique IDs for 800-53r5 without regard for the resulting sum number of requirements. As an example, this would result in 3.1.1 being split into its three source controls - AC-2, AC-2(3), and AC-2(13)
3	Amira Armond / Kieri Solutions LLC	General	publication	5	115	NIST has done a disservice to the DIB by increasing the number and complexity of actual controls by almost double while merging them into the same "110" requirements. This camouflages the true impact of Rev. 3 on the DIB from government authorities and lawmakers.	Modify requirement numbering to utilize the unique IDs for 800-53r5 without regard for the resulting sum number of requirements. As an example, this would result in 3.1.1 being split into its three source controls - AC-2, AC-2(3), and AC-2(13)
4	Amira Armond / Kieri Solutions LLC	Technical	publication	2	30	Existing scoping language is interpreted to be overly broad, resulting in some people interpreting the requirements applying to any component providing security functionality (such as NTP servers, log servers, and configuration management databases) without regard to whether applying the requirement to additional systems increases the confidentiality of CUI.	Change "The security requirements in this publication are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components." to "The security requirements in this publication are applicable to components of nonfederal systems that process, store, or transmit CUI. Security requirements may be performed by other components in order to protect CUI components."
5	Amira Armond / Kieri Solutions LLC	Editorial	cui-overlay	row 615	row 615	Typo	Remove last bracket in sentence "requiring the user to initiate a device lock before leaving the system unattended]."
6	Amira Armond / Kieri Solutions LLC	Technical	publication	53	2006	3.14.1 Flaw Remediation "b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation" This requirement will result in a net-negative security for small businesses. Small businesses typically configure their systems to accept and install vendor security updates automatically. Automatic patching results in much quicker flaw remediation, which is very important. The vast majority of small business IT departments are less qualified than their trusted vendors to test and filter patches. For example, many companies use Microsoft as one of their primary vendors. Microsoft spends billions of dollars on cybersecurity and their internal test and review process for patching. This control means we cannot accept push updates from Microsoft, but instead must configure our systems to REJECT patches until the internal IT department manually packages them and pushes them to a test group, then to production. For a small business, this 1) greatly increases latency before patching from ~12 hours to 15-30 days, 2) requires adding extra infrastructure to manage the process, such as a non-FedRAMP patch management solution, which increases the attack surface of the information system, 3) increases IT burden by at about 10 hours per week for a business with less than 10 users. For a typical small business implementing this requirement, the proposed benefit (testing patches to determine if they are malicious) is negligible. Unless an explicit control is added to this effect, small business IT departments will not perform network analysis or behavior analysis during testing to identify malicious behavior. They will simply slow down their patching process dramatically. This change would result in a net negative for security in very small and small business. For small business, the risk of a trusted vendor being compromised and pushing a bad patch is less than the unintended consequence of increasing latency in flaw remediation and increasing attack surface.	Recommended Remove "b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation" Alternate recommendation Modify b to "b. Perform a risk assessment of potential side effects for software and firmware updates by product." And add a new line at c. "c. Identify products which will be manually tested for effectiveness and potential side effects before installation based on the results of the risk assessment. "