From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] 800-171 Rev 3 IPD comments
Date: Friday, July 14, 2023 4:31:16 PM
Attachments: Outlook-Graphical .png
Outlook-53afru2q.png
C3 Integrated Solutions 800 171 Rev 3 comments.xlsx

Hello,

Attached are some comments on the 800-171 Rev 3 IPD. I would like to thank NIST for the opportunity to contribute to this publication, and look forward to seeing the final version of rev 3.

All the best,

SCOTT WHITEHOUSE
Director, Compliance Services

[redacted]

C3 + Steel Root have merged. Learn more: c3isit.com

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	C3 Integrated Solutions	Editorial		11	457	Use of External Systems part a contains 3 variables; the number of items to select, organization-defined terms and conditions, and organization-defined controls asserted to be implemented on external systems. This control deserves a verbiage shift as the quantity of variables is too great for a single line item.	
2	C3 Integrated Solutions	General			79	The introduction of ODP's in 800-171 raises challenges for OSC's and do not provide any clarity in comparison to rev 2 as defined standards do not exist in most Federal Agencies. Understanding NIST cannot meet the needs of all Federal agency requirements for all data types for the various ODP's in 800-171 I suggest NIST provide an addendum of suggested values for the ODP's with notation any definitions from specific contracts or agencies superceed NSIT's recommendations. This will help OSC's who wish to implement a secure system but do not have guidance on basic items from a Federal agency.	
3	C3 Integrated Solutions	Technical		53	2008	The requirement to test patched prior to implementation is almost a non-starter for most small buisniess. For oganizations which have less than 30 people, of which the DoD heavily relies upon, there is not the capability to test a patch prior to deployment and any testing will be functional testing and would not identify any APT's like those we saw with Solar Winds. Most small and medium businesses will not have teh capability or labor capacity to accurately identify the behavior (through tasks such as monitoring inbound and outbound network connections, local service calls, and/or effectiveness of the patch) of all updates prior to deployement . Additionally, the act of deploying and testing updates results in a slower time to close vulnerabilities due to the deployment cycle, testing, documentation of test results which are required by this control which will result in a net decrease in cybersecurity. The recommendation is to remove testing of updates from this control as it is unlikely to improve the confidentiality of CUI.	
4	C3 Integrated Solutions	Technical		46	1716	The requirement to have a third party assessment of 800-171 makes sense based on the SPRS vs DIBCAC High assessment numbers reported in Fall of 2022. However, without a defined interval in the control one could perform an assessment once every 10 years and meet the control requirement yet not have a secure system. This control needs a recommended assessment period such as 3-years.	
	C3 Integrated Solutions	Technical		77	84	"Determination of organization-defined 84 parameter values can be guided and informed by laws, Executive Orders, directives, regulations, 85 policies, standards, guidance, or mission and business needs. Once specified, the values for the 86 organization-defined parameters become part of the requirement." It would make sense if for NIST to update the CSF and cite that as the best guideline to use, or something like that. If there is a list of best practice parameters for these ODPs somewhere in a way which is possible to be more dynamically updated and responsive to actual evolving cyber threats, so that they don't need to let 800-171 ossify between revisions. If everyone uses these NIST guidelines as a standard(or an executive order or some other more easily adjusted list) then it's able to keep up with security	
	C3 Integrated Solutions	Editorial				"A noticeable national occurrence before the release of the IPD of the NIST 800-171r3, was that the DOD formally announced its commitment by releasing the document, 'Department of Defense Releases Zero Trust Strategy and Roadmap,' in November of 2022. DOD Releases Path to Cyber Security Through Zero Trust Architecture > U.S. Department of Defense > Defense Department News. It is probably not a coincidence that the NIST 800-171r3 Draft is the first NIST 800-171 (or 53) Framework to explicitly include the term "Zero Trust" (albeit in the form of a reference). Given that the NIST 800-171 is tailored from the NIST 800-53 it should be noted that any reference to the NIST 800-207, which is listed as a "Supporting Publication'" multiple times in the NIST 800-171r3 IPD, is not a normative requirement. Specifically, because data confidentiality is the direct charge of NIST 800-171, it is particularly noteworthy that in the NIST 800-207 the text specifically refers to how Zero Trust Architecture promotes confidentiality. Data confidentiality is the very crux of the NIST 800-171, and Zero Trust Architecture is promoted for this purpose in two (2) specific instances (2.1.2 & 2.2.5) in the NIST 800-207. The previously mentioned NIST 800-171r3 reference, in part derived from the NIST 800-207, was cited multiple times in the NIST 800-171r3. Zero Trust Architecture not only achieves congruence with contemporary policy and promotes confidentiality but it may also make DIB participation more cost-effective for small- and medium-sized companies by allowing the economic benefits of using a secure cloud-based solution for CUI. Zero Trust Architecture should remain, at least as present within ODP options, for contractors whenever practical during the tailoring process available for the government and contractors."	