From: 800-171comments@list.nist.gov on behalf of [redacted]
To: "800-171comments@list.nist.gov"
Subject: [800-171 Comments] Comments on NIST SP 800-171r3 initial public draft
Date: Friday, January 26, 2024 6:05:11 PM
Attachments: sp800-171r3-fpd-comment.xlsx

Thank you for your consideration and efforts!

Regards,
-Jonathan Olson
CompTIA (CASP+CE, CySA+CE, Network+, i-Net+)
Cyber AB (Registered Practitioner)

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Jonathan Olson	General	Publication	2	31	Comment: I am recommending either clarifying more explicitly which systems or components would be considered to "provide protection for such systems", or more preferably, allow the nonfederal organizations to decide what level of security of those systems or components would be required through an ODP. Rationale: It makes a lot of sense as written to protect Active Directory which provides protection (through account and authentication services) to endpoints at the same level as those endpoints that processes, stores, or transmits CUI. However, that level of protection may not be necessary and could be overburdensome for the following situation (which is more likely to happen in a SMB). If, in order to meet the requirements of 03.10.01[a and b] (page 41, lines 1484-1486) and 03.10.02[a] (page 42, lines 1503-1504) an organization elects to use multiple, separate systems/components (e.g., an Excel spreadsheet for 03.10.01[a], a proximity badge system for 03.10.01[b], and a security camera system for 03.10.02[a]), fewer protections may be needed, applicable, or even configurable as these systems/components are only providing protection for a limited portion of the environment (e.g., three separate systems/components for three pieces of two different controls). This situation may be more common in SMBs, as they tend to have tighter budgets, and therefore may try to cobble together the least expensive solutions. It could also be argued that using these diverse systems/components to handle pieces of different controls could aid in improving security as mentioned in NIST SP 800-172 control 3.13.1e.	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 only applicable to components of nonfederal systems that process, store, or transmit CUI. These security requirements also apply to components providing protection to nonfederal systems that process, store, or transmit CUI commensurate to the level of protection that they provide.
2	Jonathan Olson	General	Publication	2	31	Comment: I am requesting clarification of the terms in "process, store, or transmit". Rationale: Some people have defined "process" to include the word "access". While I completely understand their reasoning, and I could even argue that "transmit" could include that definition too, it brings up the biggest question I've had since I began focusing on cybersecurity half a decade ago. That question is: "Where do you draw the line?" If "access" is truly a definition of "process", then no matter how many virtual machines, jump boxes, bastion hosts, remote desktop connections, etc. that I have in place in between my CUI server and my non-CUI desktop endpoint, "access" travels through each and every level, and therefore leaves me without an option to scope down my environment. This can further complicate matters with the DIB as without a formal definition or clarification, organizations seeking to implement these best practices could be put in a situation where they can argue that a component is not "processing" CUI, while an assessor could argue that it is.	Please define and give examples of "process, store, or transmit", or allow for some gradation of protection the further away from CUI an accessing component is located. For example: 1) Components that directly process, store, or transmit CUI need all controls applied to them. 2) Components that process, store, or transmit CUI as an intermediary for clients need all controls applied to them. 3) Clients that access CUI through the intermediary, need fewer controls.
3	Jonathan Olson	Editorial	Publication	6	138	It may seem minor, but I wanted to give you a complement on prepending zeros to the control numbers. Well done!	No change.