From: "Strickler, Paul" via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments on NIST SP 800-171r3 initial public draft
Date: Wednesday, July 12, 2023 8:34:13 AM
Attachments: image001.png
sp800-171r3-ipd-CPI.xlsx

Paul M. Strickler, Ph.D.
Sr. Director, IT Governance, Risk, and Compliance (GRC)
Communications & Power Industries LLC
[redacted]
www.cpii.com

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Dr. Paul Strickler / Communications & Power Industries LLC	General	NIST SP 800-171r3 ipd	N/A	N/A	Removal of enduring exceptions was not addressed. There will always be exceptions due to legacy systems and system changes/upgrades.	Add a section discussing enduring exceptions and how they will be handled in the new revision.
2	Dr. Paul Strickler / Communications & Power Industries LLC	General	NIST SP 800-171r3 ipd	50	1457	Requiring external personnel, especially cloud services, to comply with a company's security policies and procedures as well as monitoring that compliance is unrealistic.	Redefine this requirement to differentiate role types required for these.
3	Dr. Paul Strickler / Communications & Power Industries LLC	General	NIST SP 800-171r3 ipd	4	79	For contractors that deal with multiple federal agencies, this makes implementation more complex as each agency will define their own requirement. This will become costly to the non-federal agencies especially if the ODP doesn't take into consideration budgets and/or risks specific to the non-federal agency. Also, it's not clear how this would work during a DFARS or CMMC Assessment - how would the requirements be assessed, especially if there are various agencies defining the ODPs? Have there been discussions on the way the federal agencies will define these ODPs? What if ODPs conflict?	Non-federal agencies should define their own ODPs for their environments based on their level of risk. If a federal agency has concerns with the nonfederal agency's definition, that can be addressed through contract language. This still allows flexibility to the non-federal agencies and removes the possibility of conforming to multiple requirements depending on the federal agency.H4
4	Dr. Paul Strickler / Communications & Power Industries LLC	General	NIST SP 800-171r3 ipd	46	1716	More clarity and detailed requirements should be provided for independent assessments. Are independent assessments required any time controls are assessed? Upon what periodicity should this be done? Can independent assessors be part of the same organization as long as they are not also the ones implementing the controls? e.g., utilizing and Internal Audit department?	Provide more clarity on the requirements for independent assessments.