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, June 23, 2023 9:43:13 AM
Attachments:	image001.png image003.png image004.png image005.png sp800-171r3-ipd-comment-Southern Company-Shawn Bilak.xlsx

Good Morning,

Attached are the comments from Southern Company. These comments are written from the lens of a Utility provider (Electric and Gas) that provides electrical and gas services to military bases.

Thanks,
Shawn

Shawn Bilak
Security Risk & Compliance Analyst,
Specialist
Cybersecurity Assurance
[redacted]

Southern Company

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Shawn Bilak - Southern Company	Editorial	NIST SP 800-171r3 ipd (Initial Public Draft) May 2024	1	18	Please add clear direction that the federal agencies are responsible to define to nonfederal organizations what data is considered CUI, per Dr Ross comments at time 7:25 of the public comments webinar. There is various interpretation by different agencies and non federal organizations on who defines what CUI is.	or transmitted by nonfederal organizations using nonfederal systems.5 "It is the responsibility of the federal agency after consulting the NARA CUI registry, to specify and notify nonfederal organizations what data is considered CUI."
2	Shawn Bilak - Southern Company	Technical	NIST SP 800-171r3 ipd (Initial Public Draft) May 2024	8	85	The uniqueness of OT systems may be beyond the expertise of the federal agency. Recommend a provision for federal agencies to reach out to other federal agencies to help define ODP's by the agency.	For contracts which include "Critical Infrastructure Sectors" agencies should consult with sector specific subject matter experts (DoE, TSA) to aid in defining ODP's
3	Shawn Bilak - Southern Company	Technical	Analysis of changes from NIST SP 800-171 Rev. 2 to Rev. 3 initial public draft	8	85	The FAQ sheet provides a provision for non federal organizations to define ODP's and submit to the government agency for approval. Recommend specific call out on the process non federal organizations should use to define ODP's	In the absence of government agency defined ODP's, non federal organizations should define local ODP's and submit their definitions to the federal agency for approval. Once approved, the values for the organization-defined parameters become part of the requirement.
4	Shawn Bilak - Southern Company	Technical	NIST SP 800-171r3 ipd (Initial Public Draft) May 2023	42	1556	Please provide a definition of "system distribution and transmission lines", In the electrical sector transmission and distribution lines are used for providing power to various buildings.	
5	Shawn Bilak - Southern Company	Technical	Analysis of changes from NIST SP 800-171 Rev. 2 to Rev. 3 initial public draft	44	1717	Independent assessments should only be a requirement for contracts requiring a 800-172 assessment, or CMMC level 2	Add ODP to 3.12.5 requirement to reflect that an independent assessment is required for CMMC certification. Not a requirement for cyber requirements under DFARS 7012.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
6	Shawn Bilak - Southern Company	Technical	Analysis of changes from NIST SP 800-171 Rev. 2 to Rev. 3 initial public draft	79	3004	This section is confusing as it is unclear if implementors should use this section to tailor their SSP's. It appears to describe the methodology NIST used to tailor revision 3 off of 800-53. This section may not be helpful to non federal organizations and should include some clarifying language to eliminate any confusion.	Change section title to "Appendix C. Tailoring Criteria used in development of revision 3"
7	Shawn Bilak - Southern Company	Technical	Analysis of changes from NIST SP 800-171 Rev. 2 to Rev. 3 initial public draft	79	3005	This section is confusing as it is unclear if implementors should use this section to tailor their SSP's. It appears to describe the methodology NIST used to tailor revision 3 off of 800-53. This section may not be helpful to non federal organizations and should include some clarifying language to eliminate any confusion.	Add language to reflect that this section describes the tailoring that was used to develop this publication

* indicate required fields