

From: [REDACTED] [via 800-171comments](#)
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments on 800-171
Date: Wednesday, May 10, 2023 11:10:18 AM
Attachments: [sp800-171r3-ipd-comment-template.xlsx](#)

NONPUBLIC//FDIC BUSINESS

See attached. Please pay attention to this comment which I have made on previous versions of this document and which continues to persist. Thank you.

Brian Seborg

Senior Enterprise Architect, ADS/ESB/DIT
CIO Organization
VASQ-A-6098
Office: [REDACTED]
Cell: [REDACTED]

NONPUBLIC//FDIC BUSINESS

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Brian Seborg/FDIC	Editorial	Publication	4	4	The statement of applicability continues to be difficult to understand and seems to attempt to apply a federal standard to systems where there is no federal interest or applicability.	<p>Read this statement closely: This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations, when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency, and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.</p> <p>The negatives in this statement appear to make this only applicable to systems over which there is no federal control, which begs the question as to applicability since a company maintaining such information would NOT be subject to federal oversight under the NIST framework. So, my suggestion is to reword it as follows: "This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations, when the nonfederal organization is collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency, and where there are specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry."</p> <p>Because, if there is NO specific safeguarding requirements, then how is this even applicable? It makes no sense. I have made this comment on previous versions but someone doesn't seem to get it. Run this by a lawyer and they will clearly articulate to you that if one does not change this then it is not clear that it applies to anything of consequence without this wording change.</p>

* indicate required fields