From:	[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Submission of Public Comments on NIST SP 800-171 rev 3
Date:	Friday, July 14, 2023 5:28:13 PM
Attachments:	image001.png sp800-171r3-ipd-comment-AWS.xlsx

NIST Team,

Attached find comments for the draft version of NIST 800-171 rev 3.

Thank you for allowing public comments.

Regards,

Jim Mueller, CCSP, CSSLP, CISSP
Government Compliance Lead
[redacted]
Visit the RISE Wiki to Learn More.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Topic *	Comment *
1	AWS	General	Clear and consistent CUI Guidance	NIST should help users understand the differences between 800-171 and other related NIST publications. An example would be the alignment of 800-171 and 800-172. Additional guidance on when which document applies could reduce confusion by DIB participants. Encourage NARA, DoD, and other agencies to clarify and provide additional guidance for contractors.
2	AWS	General	Alignment of 800-171 to existing NIST documents and federal regulations	NIST should align 800-171 with other procurement-related cybersecurity guidance. Examples include the Department of Defense CMMC 2.0 program and Homeland Security Acquisition Regulation - Safeguarding of Controlled Unclassified Information. Having NIST collaborate with federal agencies to build alignment is essential.
3	AWS	General	Clarify flow-down of obligations between DIB prime and sub-contractors	NIST should provide additional guidance on what requirements apply at the prime and/or subcontractor level. DIB participants have uncertainty about whether and how prime contractors are expected to ensure subcontractor compliance.
4	AWS	General	Responsible entity for organization-defined parameters (ODP)	Who is ultimately responsible for defining ODPs? Is the NIST intent to allow industry participants to define and manage ODPs based on the risk? Or is the intent the ability of federal agencies and contract officers to define ODPs? NIST should clarify the responsibilities and goals for ODPs.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Topic *	Comment *
5	AWS	General	Adherence for existing contracts	Is the new revision applicable for only new contracts? If the revision applies to existing contracts, what is the timeframe for adherence? Specific NIST guidance will assist contracting officers and industry providers.
6	AWS	General	Ability of small and medium size DIB organziations to meet requirements	With the DIB made up of hundreds businesses providing technology and professional services to all federal agencies, NIST should consider the impact on of medium and small size businesses and their ability to adopt the 800-171 requirements. Can
7	AWS	General	Independent Assessment	NIST should revise the definition of an “independent assessment” such that an organization can define internal controls to support conduct of the assessments by in-house employees.
8	AWS	General	Supply Chain Risk Management section 3.17	NIST should align requirements in 3.17 in the software with NIST SSDF's software supply chain security requirements and provide a mapping as it provided for NIST 800-53.