From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] SP800-171 Rev. 3 (Initial Public Draft) - Comments
Date: Friday, January 10, 2025 1:19:49 AM
Attachments: sp800-172r3-ipd-comment-Govindaraj_Palanisamy.xlsx

---

Dear NIST Special Publications Team,

Thank you for allowing me to comment on the standard. I have attached my comments for you to look over. I hope that the comments will help enhance the standard.

Thank you for your time and consideration.

Sincerely,
Govindaraj

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Govindaraj Palanisamy / Global Payments	Technical	13	538	The document introduces attribute-based access control (ABAC) which is a good start but could emphasize dynamic authorization methods for data sharing.	Use dynamic authorization policies based on real-time context (e.g., user location, device posture, time of day) in addition to attributes. This would enhance the security of data by controlling access based on more than just pre-defined attributes.
2	Govindaraj Palanisamy / Global Payments	Technical	16	618	The document emphasizes literacy training for users but could be enhanced with specific training on secure data sharing practices and risks associated with external connections.	Include specific training modules that cover the risks of unauthorized data sharing, how to verify the integrity of data received from external sources, and the best practices for securely sharing data and using remote connections. This could be added to 03.02.01E "Advanced Literacy and Awareness Training".
3	Govindaraj Palanisamy / Global Payments	Technical	26	933	The document promotes device attestation, but could also specify context-aware device authentication for data sharing and external access.	Require that device authentication incorporate contextual information, such as location, device health, and user behavior patterns for data sharing or external access. This ensures that only authorized devices with a suitable security posture can access sensitive data. This could be added to 03.05.03E "Device Attestation" or created as a new enhanced security requirement in the Identification and Authentication family.

4	Govindaraj Palanisamy / Global Payments	Technical	55	1874	The document discusses trusted sources but could add a requirement for verifiable data lineage and secure data pipelines to help protect against supply chain risks	Include mechanisms for tracking data provenance and integrity, especially when data is obtained from external sources, and to use secure data pipelines. This can be added as a requirement to 03.14.04E "Refresh from Trusted Sources" or created as a new enhanced security requirement in the System and Information Integrity family. This approach ensures that only trusted data is used in critical processes, mitigating risks from compromised data sources.
5	Govindaraj Palanisamy / Global Payments	Technical	64	2144	The planning section focuses on a security architecture but could be enhanced by including a formal data governance framework, which is critical for successful data sharing across organizational boundaries.	Include a formal data governance framework that includes policies, procedures, and responsibilities for data management, access control, and sharing, with a specific focus on data sharing across organizational boundaries. This addition could be added to 03.15.01E "Security Architecture" or created as a new enhanced security requirement in the Planning family.