From:	[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Cc:	[redacted]
Subject:	[800-171 Comments] Google Submission to NIST SP 800-171 Rev. 3
Date:	Friday, January 26, 2024 2:31:08 PM
Attachments:	Google Submission NIST SP 800-171r3.xlsx

Dear Editors,

Please find attached Google's comments to NIST SP 800-171 Rev. 3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Sincerely,

Connor

Connor Applegate
Standards Development and Intelligence
[redacted]

Comment #	Submitted By (Name/Org):*	Type (General /	Source (publication	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Asjad Nasir/Google	Technical	Publication	6	141	Add multi-factor authentication requirements for privileged accounts to improve security. Standards like NIST 800-63B recommend MFA for high-risk accounts. Privileged admins fall into this category.	**Add under Requirement 3.1.1**: "h. Add multi-factor authentication requirements for privileged accounts to improve security."
2		Technical	Publication	6	149	Expand on the type of system account monitoring and emphasize the importance of detecting unauthorized access/anomalies.	**Modify**: "e. Monitor the use of system accounts." **To**: "e. Implement continuous monitoring of system accounts focusing on detecting unauthorized access and/or anomalies."
3		Technical	Publication	7	175	Expand on the meaning of "significant security risk" and specify what individuals constitute that type of risk.	**Modify**: "Users who pose a significant security risk include individuals for whom reliable evidence indicates either the intention to use authorized access to the system to cause harm or that adversaries will cause harm through them. Close coordination among human resource managers, mission/business owners, system administrators, and legal staff is essential when disabling system accounts for high-risk individuals. Time periods for the notification of organizational personnel or roles may vary." **To**: "Individuals considered a significant security risk are those who, based on reliable evidence, are likely to misuse their authorized system access for harmful purposes, or are vulnerable to exploitation by adversaries to cause harm. It is crucial to establish a collaborative approach involving human resource managers, business and mission leaders, system administrators, and legal teams when it comes to deactivating system accounts belonging to such high-risk individuals. The timeframe for notifying relevant organizational members or roles about these actions can differ based on specific circumstances."
4		Technical	Publication	8	223	Recommended additional guidance for robust flow control and enforcement.	**Modify**: "Transferring information between systems that represent different security domains with different security policies introduces the risk that such transfers violate one or more domain security policies. In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes prohibiting information transfers between interconnected systems (i.e., allowing information access only), employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security attributes and security labels." **To**: "**The trustworthiness of filtering and inspection components is critical for effective information flow enforcement. Guidance on selecting hardened network security devices and evaluating software quality may be beneficial. For large or complex environments, reference architectures with robust information flow control should be considered. Resources on zero trust and microsegmentation architectures can provide additional guidance.** Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes prohibiting information transfers between interconnected systems (i.e., allowing information access only), employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security attributes and security labels."

5		Technical	Publication	9	270	Periodical reviews of assigned privileges are essential to ensure users do not retain unnecessary access over time. Microsegmentation, encryption, and access control solutions are industry standard solutions that should be mentioned.	**Add under DISCUSSION**: "Frequent reviews of assigned privileges are essential to ensure accounts, roles, and processes do not accumulate unnecessary access over time. Automated tools can also help continuously monitor and enforce least privilege principles across an environment. Microsegmentation, encryption, and access control solutions should be employed to securely restrict access to privileged functions and security-critical information."
6		Technical	Publication	9	273	NIST SP 800-207 Zero Trust Architecture should be included (and linked) if Comment 5 is accepted. Comment 5 includes tools/practices mentioned in NIST SP 800-207.	**Modify**: "Supporting Publications: None" **To**: "Supporting Publications: ~~None~~ **NIST SP 800-207 Zero Trust Architecture**"
7		Technical	Publication	10	309	MFA is an industry standard practice that should be included in this section.	**Add under DISCUSSION**: "Consider requiring multi-factor authentication after a certain number of failed attempts to mitigate brute force attacks while still allowing users to recover from forgetting credentials."
8		Technical	Publication	11	330	Include additional verbiage that encourages the customization of system requirements as it provides an opportunity to reinforce key security policies before system login	**Add under DISCUSSION**: "System notifications should be specific and customized to the organization, not just generic message. They provide an opportunity to reinforce key security policies before system login. For systems accessible by third parties, customized notifications highlighting additional organizational controls are recommended."