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, July 14, 2023 1:15:42 PM
Attachments:	image001.png sp800-171r3-ipd-comment-RC.xlsx

Attached are my comments for the NIST 800-171 R3 draft.

Regards,

Rebecca Conner
Qualcomm

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Rebecca C Qualcomm, Inc.		3.1.5			Control speaks to generic accounts (a) and eludes to privileged accounts in (b) due to access to "security functions and security-relevant information" but the discussion jumps into security functions as part of the 2nd sentence. I realize this is due to AC-6(1) but it made it seem like the entire control is for least privilege on privileged accounts vs. least privilege for any account. Consider 2 separate paragraphs to break up 800-53 AC-6 from AC-6(1):	Organizations employ the principle of least privilege for specific duties and authorized access for users and processes. Organizations consider creating additional processes, roles, and system accounts to achieve least privilege. Least privilege is also applied to the development, implementation, and operation of the system. When considering least privilege, account for authorized access to security functions which include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.
2	Rebecca C Qualcomm, Inc.		3.1.12				References should include AC-17(2) for 3.1.12e.
3			3.1.23			This is telling users to LOGOUT & says enforced by 3.1.10 but 3.1.10 is just locking the device, NOT LOGGING USERS OUT. If the ODP is similar to Fedramp Moderate Baseline then this control is reasonably managed by the OSC. If the ODP is different then logging users out after a ODP defined period of inactivity has the potential for being pretty problematic in an engineering environment where users may have something running through a weekend or even longer, especially on a test setup.	

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
4	Rebecca C Qualcomm, Inc.		3.3.1			1. Change summary states that this includes content from 3.3.2(withdrawn) but I don't recognize content from 3.3.2, only content from 800-53 AU-2. 2. If the ODP for event types matches FedRAMP Moderate then no issues. Otherwise: The ODP for event types precludes an organization's ability to adjust their logging to match the risks associated with their environment. Per the Discussion: Organizations identify event types for which a logging functionality is needed as those events that are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. ..... In determining event types that require logging, organizations consider the system monitoring and auditing that are appropriate for each of the CUI security requirements. .... Monitoring and auditing requirements can be balanced with other system needs. By making the event types an ODP you are effectively elminiating the organization's ability to manage any of the the items noted in bold which can significantly impact their staffing, costs and impact to system needs.	
5	Rebecca C Qualcomm, Inc.		3.3.3				Recommend merging 3.3.1, 3.3.2 & 3.3.3 as this would be much simpler. a. Specify and generate the following event types for logging within the system: [Assignment: organization defined event types]. b. Specify and generate the following content in audit records: what type of event occurred; when and where the event occurred; source and outcome of the event; identity of individuals, subjects, objects, or entities associated with the event; and [Assignment: organization-defined additional information]. c. Review and update the event types selected for logging [Assignment: organization-defined 606 frequency]. d. Retain audit records for [Assignment: organization-defined time period consistent with records retention policy, applicable contract requirement, law, or regulation].
6	Rebecca C Qualcomm, Inc.		3.3.5	703			Line 703 needs to include AU-6 as part of source controls

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
7	Rebecca C Qualcomm, Inc.		3.5.3			What is meant by system accounts? Per line 113: "When used in the context of the requirements in Section 3, the term *system* means a nonfederal system that processes, stores, or transmits CUI." So in that context, a "system account" is a user account on such a system? or Per Line 140: "System account types include individual, shared, group, temporary, system, guest, anonymous, emergency, developer, and service." It seems that you are referring to the first example as MFA for all the account types in the 2nd example would be impossible to implement MFA for (ie, system account). Also, your comment for 3.5.4 under Summary of Changes column also eludes to a system account being a user account.	
8	Rebecca C Qualcomm, Inc.		3.5.5			Why include on ODP for the roles to authorize an account? Is the DiB finding issues with separtion of duties that leads to this necessity? Authorization will vary based upon the company size and structure.	It seems this can be managed by an OSC and rewritten as: a. Receive authorization to assign an individual, group, role, service, or device identifier.
9	Rebecca C Qualcomm, Inc.		3.5.7				3.5.7b - Saying "all printable characters" is problematic for some applications that utilize system passwords as the application does not accept "all printable characters". 3.5.7c is difficult in an air-gapped network for an SMB as most solutions are cloud-based.
10	Rebecca C Qualcomm, Inc.		3.12.5			For independent assessments, is NIST referring to the CMMC assessment?	
11	Rebecca C Qualcomm, Inc.		3.12.6			FedRAMP moderate requirements call out annual reviews. Some companies may not have the ability to update agreements annually due to the organizations size and influence in the industry.	Recommend making the reviews an OSC defined control based upon risk.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
12	Rebecca C Qualcomm, Inc.		3.13.8			Compare this with "3.8.9. System Backup – Cryptographic Protection" where the Discussion says "Organizations can employ cryptographic mechanisms or alternative physical controls to protect the confidentiality of backup information." as well as "3.8.5 - Media Transport" where the discussion says "Controls to protect media during transport include cryptography and locked containers." 3.13.8 been changed to require encryption at all times while 3.8.5 and 3.8.9 take into account alternate controls.	Recommend incorporating alternate physical controls into 3.13.8 as they offer a cost-effective option for SMBs working with a diverse endpoint ecosystem.
13	Rebecca C Qualcomm, Inc.		3.14.1.b			3.14.1.b - This should be a risk-based decision for each organization, the vendor patch in question and the situation under which the patch is to be applied.	Recommend changing this to: "Per risk analysis, test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation."
14	Rebecca C Qualcomm, Inc.		3.14.1.c				Given 3.14.1b I recommend that the time period ODP for 3.14.1c be defined by OSCs as it will depend on many factors and the overall risk to their environment which will vary among OSCs.