From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] Feedback on NIST SP 800-171 r3 Initial Public Draft
Date: Friday, July 14, 2023 4:23:03 PM
Attachments: SAIC sp800-171r3-ipd-comments 14July2023.xlsx

Good Afternoon,

Attached please find comments and feedback on the IPD of NIST SP 800-171 r3.

Regards,

Amanda M. Allen | SAIC
Cybersecurity Compliance Manager
Governance, Risk, & Compliance (GRC) | IE Chief Information Security Office

[redacted]

Please note that I follow SAIC's 9/80 work schedule and am out of the office every other Friday.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	SAIC, Inc.	Technical	Publication	5	133	This ODP cannot be defined by an Agency for a Contractor system without a deep understanding of the Contractor's environment and business model. Determining the roles and/or persons who must be notified should be left up to the contractor to prevent an Agency from making an assignment to a role that doesn't make sense in the Contractor's system environment.	Remove this ODP and revise language to "Notify key personnel or roles within a specified period of time."
2	SAIC, Inc.	Editorital	Analysis	N/A	5	This control was noted as no significant change however previous wording did not require system access authorizations to be defined in support of Separation of Duties, only that the duties be separated	Review updated control language and ensure the impact of the change aligns with the intent of the change.
3	SAIC, Inc.	Editorital	Analysis	N/A	10	This control was noted as no significant change however previous wording would allow for out-of-band notices whereas new language lends itself more to a notices displayed on the system at login.	Review updated control language and ensure the impact of the change aligns with the intent of the change. Consider revising langauge to "Provide system use notification message or banner to users that is visible before accessing the system that provides privacy and security notices consistent with applicable CUI rules."
4	SAIC, Inc.	Technical	Publication	10	341	This ODP cannot be defined by an Agency for a Contractor system without a deep understanding of the Contractor's environment and business model. An Agency may select conditions or trigger events that the Contractor cannot maintain.	Remove this ODP and revise language to "Terminate a user session after pre-defined conditions or trigger events."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
5	SAIC, Inc.	Technical	Publication	17	632	This ODP cannot be defined by an Agency for a Contractor system without a deep understanding of the Contractor's environment and business model. An Agency cannot define what additional data should be captured in audit records without detailed understanding of the specific tools and processes in use on the Contractor system.	Remove this ODP and revise language to "Include 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 other information as approproate."
6	SAIC, Inc.	Technical	Publication	19	683	This ODP cannot be defined by an Agency for a Contractor system without a deep understanding of the Contractor's environment and business model. An Agency cannot define which roles or personnel findings should be reported to without a detailed understanding of the Contractor's environment and operating structure.	Remove ODP and revise language to "Report findings to appropriate personnel."
7	SAIC, Inc.	Technical	Publication	27	1011	This ODP cannot be defined by an Agency for a Contractor system without a deep understanding of the Contractor's environment and business model. An Agency cannot define what specific devices or types of devices can authenticate to the Contractor's network without fully understanding the Contractor's business processes and needs. Many companies secure their entire enterprise network to store and process CUI. An Agency may not take this into account when scoping what devices to allow to connect to the network creating a situation where the Contractor is unable to comply.	Remove ODP and revise language to "Uniquely identify and authenticate devices before establishing a system or network connection."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
8	SAIC, Inc.	Technical	Publication	30	1118	This control could be interpreted to mean Identity Proofing which could be costly for Contractors to implement depending on the Assurance Level needed to meet this requirement.	Revise language to "Ensure the identity of the individual, group, role, service, or device receiving the authenticator has been validated as part of the initial authenticator distribution."
9	SAIC, Inc.	Technical	Publication	40	1516	The updated language does not make it clear if each alternate work site must be individually identified and documented or if the intent of the control is to identify broad categories/types of alternate work sites. For example, does each employee residence need to be documented for teleworking purposes?	Revise language to "Determine and document guidelines for appropriate alternate work sites allowed for use by employees."
10	SAIC, Inc.	Technical	Publication	50	1903	This control should be updated to include requirement for key rotation.	Revise language to "Establish and manage cryptographic keys when cryptography is implemented in the system in accordance with the following key management requirements: [Assignment: organization defined requirements for key generation, distribution, storage, access, rotation, and destruction."
11	SAIC, Inc.	Technical	Publication	51	1916	While the removal of the specific control languge requiring FIPS-validated cryptography is a welcome change, the addition of an ODP for this control is worrisome. This ODP cannot be defined by an Agency for a Contractor system without a deep understanding of the Contractor's environment and business model. The previous requirement for FIPS-validation created many compliance deficiencies due to the limited nature of available FIPS-validated versions of existing products in use by many companies today.	Revise language to "Implement cryptography compliant with FIPS 140-3 when protecting the confidentiality of CUI."