From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] NIST SP800-171 R3 Draft 1 Feedback
Date: Friday, July 14, 2023 7:48:46 PM
Attachments: sp800-171r3-feedback.xlsx

To Whom It May Concern:

As Idaho's land-grant research university, the University of Idaho performs research and handles data on behalf of multiple public, private, commercial, state and federal organizations and is keenly aware of the impacts of technical requirements in NIST 800-171. We appreciate this opportunity to provide feedback on NIST 800-171 revision 3 draft 1.

A major area of flexibility added to draft 1 via the organization-defined parameters (ODP), but we are also concerned with the variability of compliance expected across different organizations. This uniquely affects Higher Education institutions performing research for multiple federal agencies with now potentially unique requirements. Any opportunities to encourage consistency across these organizations will only serve to simplify and streamline compliance for all of us, and allow for efforts to be focused on actual research and not compliance.

See attached spreadsheet with specific feedback on individual standards.

Sincerely,

Mitch Parks
Chief Information Security Officer

Nathan Flynn
Cybersecurity Analyst, Research

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	University of Idaho	General	SP 800-171r3	17	604	The change in 3.3.1 to an ODP which, as a university working with multiple organizations, may result in conflicting requirements, and makes it difficult to plan for what logging needs may be.	This should either revert back to what r2 stated or specifically define log requirements. Alternatively providing a default unless otherwise defined as ODP such as the requirements in General Records Schedule.
2	University of Idaho	General	SP 800-171r3	24	897	Changing 3.4.8 from either a deny-all or allow-all with a deny list to only a deny-all requirements will be difficult for Universities to implement without a large disruption to researchers as well as significant labor to review and approve every piece of software in use across all the different departments performing research. Additionally, having a deny list of bad software and using modern EDR tools reduce the risk of rogue software acting maliciously.	This should either revert back to what r2 stated which allows for either a deny-all or an allow-all, or switch to an ODP requirement to define which should be used, or allow for compensating controls such as EDR.
3	University of Idaho	General	SP 800-171r3	29	1070	Changing 3.5.7 to use an ODP for password rules may result in conflicting requirements as we are a university working with multiple organizations, which would then lead to requiring different credentials per user per project. Leading users to set multiple passwords increasing the risk of insecure passwords.	This should be aligned with 800-63 and use an ODP to define if it is AAL1, AAL2, or AAL3.
4	University of Idaho	General	SP 800-171r3	41	1517	Changing the alternate work site requirements in 3.10.6 to an ODP makes it impossible to plan for as requirements may change from project to project. As a university researchers may be working with multiple organizations who may define conflicting and unresolvable requirements.	This should be aligned with 800-46.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
5	University of Idaho	General	SP 800-171r3	46	1717	3.12.5 sets the only criteria to be an assessor is that they are independent, which some organization do not currently require. The current lack of availability of qualified 3rd party assessors could inhibit compliance.	Have the criteria to be an assessor as an ODP. This allows organizations that do not require independent assessments to continue, as well as allow other organizations to require additional qualifications (such as C3PAO certification by the cyber-AB).
6	University of Idaho	General	SP 800-171r3	46	1717	The vague working around 'assess controls' in 3.12.5 doesn't specify if it is just the controls required by 171 or all organizational controls.	Please specify the scope of the assessment.
7	University of Idaho	General	SP 800-171r3	52	1973	Wording in 3.13.17 does not specify the type of proxy. The language of 'web proxy' implies a full web proxy however the core requirements imply a transparent proxy with url filtering such as a next-gen firewall may be sufficient.	Please specify the type of proxy required. It is preferred for transparent proxies with web content filtering/logging to be included.
8	University of Idaho	General	SP 800-171r3	59	2225	Using ODPs for the requirements for external services in 3.16.3 which, as a university working with multiple organizations, may result in conflicting requirements, and makes it difficult to plan for what requirements may be.	This should be aligned with 800-161.