

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: Thursday, July 13, 2023 5:33:44 PM
Attachments: [image001.png](#)
[sp800-171r3-ipd-comment-template \(2\).xlsx](#)

Comment template attached.

Patrick Skinner
Quality and Compliance Manager
CymSTAR, LLC



A HUBZone & SERVICE DISABLED VETERAN OWNED SMALL BUSINESS

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	CymStar	general		15	517	The inactivity logout control states this is a behavior or policy control, and that automatic enforcement is addressed in 3.1.10, however, 3.1.10 does not cover automatic logout, only screen lock. Furthermore, we believe with an adequately restrictive automatic enforcement, there is no need for a policy on manual logout, since automatic enforcement will always log the users out of the system.	Allow use of automatic enforcement in lieu of policy, and remove language saying automatic enforcement is covered in 3.1.10
2	CymStar	technical	analysis	24	895	The policy of requiring a deny all and allow by exception policy for software will potentially add overhead, cost, slow down development, and balloon documentation requirements. Numerous black-lists of software exist, and can integrate with SIEM or other tools with minimal labor required, however, manually reviewing every version of every piece of software requested, and then updating documentation (line 899) will be a significant administrative burden, and may in some cases REDUCE security. If software, such as browsers, various microsoft applications, etc, require updates to patch known vulnerabilities but cannot be updated until the new version is reviewed and added to the approved software list, this could actually delay automatic update processes.	Allow use of black lists instead of deny all and only approve by exception for some users.

* indicate required fields