From:	[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Cc:	[redacted]
Subject:	[800-171 Comments] NIST Comments For 800-171 Submission From Forcepoint Global Governments and Critical Infrastructure (G2CI)
Date:	Friday, July 14, 2023 1:01:57 PM
Attachments:	sp800-171r3-ipd-comment-Response Forcepoint G2CI.xlsx

---

Please see attached 800-171 comments submission from Forcepoint G2CI.

Thank you.

Marlon Walker
Principal Security Strategist
Global Governments and Critical Infrastructure
Forcepoint
[redacted]
www.forcepoint.com

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Dan Valez / Forcepoint G2CI	G	N/A	N/A	There are 98 instances of the term "monitor" in this publication. In some contexts it is used to imply observing or supervising, in other contexts it implies a cyber capability.	Recommend adding a definition of "monitor" that aligns to the concepts of user activity monitoring where appropriate.
2	Dan Valez / Forcepoint G2CI	G	9	286	There are 26 instances of the term “logging” and throughout the publication and in almost all cases the term is coupled to “auditing” which is typically an information system feature. For example in paragraph 3.1.7 line 286 there is a discussion of logging the use of privileged functions. A user activity monitoring solution could “log” the use of privileged functions when the information system lacks specific auditing or logging capability or if the capability lacks sufficient context to understand the user activity.	Recommend a definition of logging that makes it more clear that this control might be a system feature or produced by a user activity monitoring capability.
3	Marlon Walker / Forcepoint G2CI	G	6	180	Section 3.1.3 Discuss enforce approved authorizations for controlling the flow of CUI within the system and between connected systems. It mentions boundary protection devices and techniques that employ rule set or establish configuration setting that restrict system services, provide a packet filtering capability based on header information or provide a message-filtering capability based on message content.	Recommend that in addition to the listed boundary protection devices and techniques, that for mission critical applications with connectivity to segmented networks there should be one-way data transfer devices (such as diodes or other technology), and/or with Cross Domain technology that inspects and validates the data transferring to/from the segmented network.