From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Cc:	[redacted]
Subject:	[800-171 Comments] Submission of Comments on NIST SP 800-172 Rev. 3 IPD | CNLABS Test Services Pvt Ltd
Date:	Friday, January 17, 2025 4:44:23 AM
Attachments:	image001.png NIST SP 800-172R3-IPD comments-CNLabs.xlsx

Dear NIST Team,

Greeting from CNLABS Test Services Pvt Ltd!

We are pleased to submit our comments and feedback on the initial public draft of NIST SP 800-172 Rev. 3: Enhanced Security Requirements for Protecting Controlled Unclassified Information.

CNLABS is an independent, vendor-neutral, interoperability lab for testing and certification of products, technologies & solutions, specializing in Cyber Security, USGv6, IPv6, Networking, SDN, Virtualisation etc.,

We commend NIST's dedication towards advancing the protection Controlled Unclassified Information and appreciate the opportunity to contribute to this critical effort.

Thank you for your consideration, and we look forward to the finalized version of the standard.

Warm Regards,
John Timothy J
Security Test Engineer
CNLabs Test Services Pvt Ltd
Bangalore, India

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	CNLABS Test Services Pvt Ltd	Technical	15	587	The standard talks about concurrent session control. However, including the entropy of session ID and other cookie attributes can improvise session handling related security requirements. Additional requirement can be considered under 03.01.xxE	**Addtional requirement:** 03.01.11E Session Management Hardening: Ensure session management adheres to secure design principles by: 1. Generating session IDs with high randomness and uniqueness to prevent prediction or replay; 2. Protecting session IDs using secure transport mechanisms (e.g., HTTPS); and 3. Properly configuring session cookies with attributes such as domain, path, same site, HTTP only, max age, expires
2	CNLABS Test Services Pvt Ltd	Technical	15	587	The standard can consider "Zero Trust Access" as an additional requirement under clause 03.01.xxE	**Additional requirement:** 03.01.12E Zero Trust Access: Implement a Zero Trust Architecture to verify all access requests and enforce least privilege, ensuring continuous authentication, authorization, and monitoring to protect systems and data from unauthorized access.
3	CNLABS Test Services Pvt Ltd	Technical	35	1210	Clause 03.10.02E Intrusion Alarms and Surveillance Equipment can be improvised by including periodic mock drills for ensuring physical surveillence system and response protocol functioning.	03.10.02E Intrusion Alarms and Surveillance Equipment: Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment. **Conduct periodic mock drills to ensure the proper functioning of physical intrusion alarms and response protocols at [Assignment: organization-defined frequency]**
4	CNLABS Test Services Pvt Ltd	Technical	36	1268	Clause 03.11.02E Threat Hunting can be improvised with "Threat Hunting and Management" by including root cause analysis for identified indicator of compromise and enhancing security policies/configurations to prevent future attempts. This needs to be a continual improvisation process.	a. Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; 2. Detect, track, and disrupt threats that evade existing controls; and b. Implement the threat hunting capability [Assignment: organization-defined frequency]. **c. Ensure a continuous threat management process that includes:** **1. Implementing necessary prevention mechanisms upon identifying indicators of compromise;** **2. Regularly reviewing and updating security policies and configurations based on threat hunting outcomes; and** **3. Maintaining an ongoing improvement cycle to adapt to evolving threats.**

Note: Comment #1 & #2 are additional requirement suggestions. In comment #3 & #4, the portion highlighted in Green colour is suggested to add to enhance the existing requirement