Hello,
Our comment on section 3.8.9 of the standard is attached.
Thanks in advance,
Leor F.
<table>
<thead>
<tr>
<th>Comment #</th>
<th>Submitted By (Name/Org.)*</th>
<th>Type (General / Editorial / Technical)</th>
<th>Source (publication, analysis, overlay)</th>
<th>Starting Page #</th>
<th>Starting Line #</th>
<th>Comment (include rationale)*</th>
<th>Suggested Change*</th>
</tr>
</thead>
</table>
| 1         | Fortress Labs Technical   | NISTIR 8320                          | 37                                     | 1399            |                | System Backups should mention hardware enabled security technologies (as recommended by NISTIR 8320) as an augmentation to cryptographic protections for backup data. | System Backups – Cryptographic and Hardware Protection

Implement cryptographic and hardware mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.

**DISCUSSION**

Organizations can employ cryptographic mechanisms as well as alternative physical controls to protect the confidentiality of backup information at designated storage locations. Specifically, devices like hardware security modules (HSMs) and Trusted Execution Environments (TEEs) may be used to improve the security of cryptographic operations on backups. Backed-up information that contains CUI may include system-level information and user-level information. System-level information includes system-state information, operating system software, application software, and licenses. User-level information includes information other than system-level information.

NIST SP 800-171r3 ipd (Initial Public Draft) Protecting Controlled Unclassified Information May 2023

**REFERENCES**

Source Controls: CP-9[8]

Supporting Publications: SP 800-34 [56], SP 800-130 [57], SP 800-152 [58], SP NISTIR 8320 [59] |