From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] NIST SP 800-171 r3 Comments
Date: Thursday, June 8, 2023 8:13:09 AM
Attachments: Outlook-uxfit0m5.png
NIST 171r3-Comments-BGTech.docx

NIST,

I have attached a Word doc with my comments.

Please confirm receipt.

Thanks,

Claude Braxton, CTO
Braxton-Grant TECHNOLOGIES
[redacted]

Information contained in this message and any attachment may be proprietary, confidential, and privileged or subject to the work product doctrine and thus protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify me immediately by replying to this message and deleting it and all copies and backups hereof. Thank you.

From: Claude Braxton, Braxton-Grant Technologies, CTO
[redacted]

Comments and questions:

1. In the Notes to Reviewers section: Can you state the new Security Requirement Families and the number of new requirements and merged requirements?
2. On page 4 Table 1: Could you add the number of requirements by family and total?
3. Requirements 3.1.11 and 3.1.23 appear to be the same and if not so close as to not need both.
4. Requirement 3.5.4 Replay-Resistant Authentication seems to be OBE. Most systems utilize SSL. Is this the answer you will be expecting?
5. Requirement 3.8.3, I would like to recommend removing CUI. It is good security practice to sanitize any company system media before disposal.
6. Requirement 3.8.4, why not include company sensitive along with CUI? This would be a good security practice.
7. Requirement 3.8.5, why not include company sensitive along with CUI? This would be a good security practice.
8. Requirement 3.8.9, why not include company sensitive along with CUI? This would be a good security practice.
9. Requirement 3.9.3b is requiring a small company to flow down personnel security policies and procedures to external providers is impractical. Why would a company except this flow down from other companies? This has legal implications. This requirement also does not state anything related to CUI.
10. Requirement 3.12.5 has just introduced additional costs. Are there any requirements for selecting an Independent Assessor? This smells like CMMC without stating it.
11. Requirement 3.13.1 leads to a question on companies that are 100% cloud-based. Would this be a N/A?
12. Requirement 3.13.4 is handled by most modern operating systems. A properly patched OS is really the best when 99% of the user are on Windows 10/11 and IOS operating systems. I think the other requirements by default address this issue.
13. Requirement 3.13.8 is confusing the first statement ” Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.” Is very clear. The Discussion section explains in depth about securing CUI in transit but on a definition of at rest “Information at rest refers to the state of CUI when it resides on the system and is not in process or in transit, including internal or external storage devices, storage area network devices, and databases.”. There is no real guidance on protecting CUI at rest.
14. Requirement 3.13.18 is too vague. How do you determine whether the number of external network connections to a system is too high or low?

15. Requirement 3.14.1: It is impractical in most small businesses to “Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.”. This would companies to have a test system for every system image deployed.
16. Requirement 3.14.8 should include Phishing.
17. Requirements 3.15.1a & b don’t mention CUI. The Discussion section brings in CUI which I think should be company-sensitive information and CUI if you must add a statement.
18. Requirement 3.15.3: I think CU should be CUI and company-sensitive information.
19. Requirement 3.16.3a-c is impractical to think a small company is going to be able to meet. Companies are already forced to use Fedramp certified companies for CUI storage and processing.
20. Requirements in 3.17 are more of a problem with companies selling products and parts to the government. Is this what is attempting to be addressed? If the goal is to tell companies to not purchase Grey market equipment for internal use then that should be stated.
21. Requirement 3.17.4 should apply to company sensitive information and CUI for good cyber security.