[redacted]

From: Hall, Scott [redacted]
Date: Tuesday, July 19, 2022 at 11:53:19 AM UTC-4
Subject: Comments on CUI Series Publications
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

RE: Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Note: All comments herein are my personal opinion and not that of my employer.

Regarding section 3.13.8 on encryption, I would suggest more clarity and guidance regarding encryption inside the organization's network. The requirement says it applies both internally and externally, but offers many alternatives or "escape" phrases allowing encryption to be deferred.

In my experience, many organizations are not encrypting inside the firewall. This especially applies to interface transmissions containing CUI such as PII and PHI, but also goes to data at rest in databases.

Assessing the value of internal encryption is complex and interdisciplinary. Some system administrators feel their server and network protections amount to a "protected distribution system" (PDS) as referenced in 3.13.8. As such, they feel that encryption is not needed or of lower priority.

The audience for this publication series and other NIST documents needs further guidance on this topic. Regarding encryption for internal data, both in motion and at rest, it would help to have NIST provide the following:

- How should internal encryption's value be evaluated in a risk assessment?
- How much does internal encryption increase an organization's security posture?
- What are specific ways that internal encryption increase security? (Please provide examples.)
- If an organization cannot encrypt all internal CUI, is it worth encrypting anything?

Can encryption be implemented incrementally and still offer value?

Thanks,

Thanks!

Scott

Scott Hall

Mercy Medical Center Cedar Rapids

[redacted]

[redacted]