[redacted]

From: Kenneth Benjamin [redacted]
Date: Wednesday, July 20, 2022 at 2:43:37 PM UTC-4
Subject: Suggested improvements to 800-171 / 171A
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

Island Systems deploys 800-171 compliant VDI solutions for customers handling CUI, primarily the Defense Industrial Base and supporting External Service Providers, e.g., MSPs. Most are SMBs or small departments inside larger enterprises. Our experience suggests the following areas for improvement:

1. NFO controls cannot be assumed to be "expected to be routinely satisfied by nonfederal organizations without specification."
    a. Re. policy and procedure NFOs, organizations go through a maturation process that begins with simply doing business. Eventually, they grow large enough that managing procedures without documentation becomes difficult and they begin writing those. Only later, or when mandated to do so, will they mature to the point of having formal policies.
    b. If you add NFOs as a requirement, less mature organizations will likely need to invest in the development of them. There may be 3rd party products that can ease that process but not for all SMBs. Clarifying the rigor and depth of the policies and procedures could help.
2. NCO controls are "not directly related to protecting the confidentiality of CUI" but there is little guidance on whether organizations should or should not implement them. Most, if not all, would appear to be useful to implement in systems, policies, and procedures. Perhaps, rather than increasing the scope of the assessment objectives, these should be provided as recommendations within the 171 standard and left for organizations to apply a risk-based approach to implementation.
3. In 171A section 2.1 Assessment Procedures, there is a discussion of the depth attribute and a statement that organizations have the flexibility to determine it. In practice, for CMMC for example, it's unclear what depth is required or desired. Guidance on this topic would be helpful. My suggestion is that the following criteria be applied:
    a. Basic – applies for FAR Basic Safeguarding use cases, e.g. FCI; may be used for organizational self-assessments
    b. Focused – applies to formal self and 3rd party assessments
    c. Comprehensive – applies to high-risk / high-value CUI when so determined by an agency, e.g., select CUI specified / limited distribution categories and perhaps only applies to 800-172?
4. In some cases, controls are more prescriptive than may be ideal. Allowing for a documented per-control risk-based strategy could allow for greater flexibility while maintaining protection of CUI. I am not proposing adding something like the RMF as a requirement.
5. Re. 3.13.11 Employ FIPS-validated cryptography when used to protect the

confidentiality of CUI
    a. Validation of systems and code tends to lag behind security patches leading to increased risks. Adding the flexibility to apply the latest patches from previously validated products would prevent the need to manage the current status on a POA&M, for example. Adding a time constraint for revalidation may be appropriate but that should be tied to the FIPS program's ability to deliver.
6. Re. 3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device
    a. Clarify that does not include PC-based scenarios like Teams, Zoom, etc.
7. Re. 3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed
    a. Not all modern anti-malware performs periodic scans. Consider rewording this to represent the current state of the art solutions.
8. Overall, the role of External Service Providers (ESP) is not well defined. For SMBs in particular, this presents challenges, both for the CUI-holding organization and SMB ESPs.
    a. For DoD, ESPs that host CUI are Cloud Service Providers and must meet FedRAMP Moderate equivalency. Clarify if that is appropriate or not as a base requirement for CUI.
    b. For ESPs that may have access to CUI but don't host it, e.g., Managed Service Providers, must they be fully compliant with 171 or is there another, perhaps risk-based, approach?
    c. This is a complex topic but some high-level guidance would be helpful particularly as 171 strongly informs other implementations such as CMMC
    d. Clarify how inheritance works when using an ESP. ESPs are unable to meet all 171 controls but may cover a small or large subset. What assessment approach should be taken and how can providers assure customers of their compliance?

Some of these suggestions are probably unlikely to be fully resolved in 800-171 but are shared to provide context around common areas of discussion and concern I encounter with our solution, customers, and in CUI discussion forums.

Kenneth Benjamin, CEO
Island Systems, LLC
[redacted]

https://islandsystems.net