From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] 800-171 Rev. 3 Pre-Draft Call for Comments
Date: Saturday, September 17, 2022 2:33:13 AM

Greetings,

Unfortunately, the poor state of security maturity in the federal contracting base has resulted in 800-171 being asked to do things it was never designed to do. Small and medium-sized businesses look to 800-171 as a tutorial for establishing security programs. CUI systems were deployed with no thought given to security by design; requirements and verification; or the SDLC.

NIST has the unfortunate burden of being constrained by the federal CUI program to focus narrowly on the confidentiality of CUI at the expense of a more holistic view that would benefit nonfederal organizations the most. However, within these constraints NIST can still thread the needle in three ways:

- Tailoring NFOs into the standard;
- Using full 800-53 controls rather than tailored snippets; and
- Including verification procedures and requirements definitions in a single document.

First, NFO controls must be tailored back into 800-171. The fundamental assumption that nonfederal organizations have existing security programs is incorrect. The level of security maturity within the federal contracting base is nearly non-existent. There is no management of external service providers a la the SA family. There is no documented policy and procedure a la the -1 controls. Nearly all of the major stumbling blocks to understanding and conceptualizing 800-171 stem from organizations not having NFO controls in place while attempting to tackle the performance requirements listed in 800-171.

Second, the requirements in 800-171 rev. 3 need to be expressed in their full 800-53 form rather than their heavily tailored 800-171 rev. 3 form. Removing the detail from 800-53 controls to create derived 800-171 requirements has the unintended consequence of leaving people without a clear idea of what needs to be done. The most common sequence for understanding a given NIST SP 800-171 requirement is to compare the information 800-171 and 800-171A to the corresponding controls and procedures in 800-53 and 800-53A. Most organizations don't do this and thus lead themselves away from the intent of the controls.

Third, regardless of the changes to NIST SP 800-171 in revision 3, it should be combined with NIST SP 800-171A. Documenting the requirements in 171 and their verification criteria in 171A is extremely confusing. Although NIST has fully embraced a systems engineering approach to security, that philosophy is almost completely absent within the nonfederal organizations that need to interpret, implement, and assess the requirements in 800-171. Tremendous time is wasted simply attempting to explain the fundamental relationship between 171 and 171A. Revision 3 needs extremely clear and concise explanations about the fundamental relationship between requirements and verification.

I look forward to the opportunity for more robust comments on the initial public draft of 800-171 rev. 3

Best,

Jacob Horne