From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] Feedback on NIST SP 800-171 r3 Final Public Draft
Date: Friday, January 26, 2024 5:13:13 PM

Good Afternoon,

Below please find comments and feedback on the FPD of NIST SP 800-171 r3.

On the topic of NIST SP 800-171r3 and the NIST SP 800-53r5 CUI Overlay: In lieu of NIST SP 800-171r3 recommend focusing on development and roll out of the NIST SP 800-53r5 CUI Overlay. NIST has stated the intent to move to the CUI Overlay in the future and retiring NIST SP 800-171 altogether. This approach would standardize requirements across Government and Nonfederal Systems and create less overhead for both implementors and NIST. Recommend pursing this path instead of releasing NIST SP 800-171r3. Recommend a delay of one year to allow time for development of the CUI Overlay. In the interim NIST SP 800-171r2 should remain valid and be eventually retired when the NIST SP 800-53r5 CUI Overlay is released. This would benefit NIST by reducing work needed to update NIST SP 800-171 and maintain two standards.
In addition, this would reduce the risk of regulatory conflict between newer standards such as DOD's Cybersecurity Maturity Model Certification (CMMC) which may be leveraging older versions of NIST SP 800-171 and the DFARS 252.204-7012 clause which would require Nonfederal Organizations to implement a newer version of NIST SP 800-171 as soon as it's published as final. This provides Nonfederal Organizations with a steadier and clearer ramp up to meet the new standard versus going through several iterations of updates to NIST SP 800-171 before eventually implementing NIST SP 800-53 via the CUI Overlay. Moving directly from NIST SP 800-171 to a CUI Overlay provides a more predictable path for Nonfederal Organizations, reducing the risk of control deficiencies introduced by ever changing standards.
On the topic of Organization Defined Parameters (ODPs): NIST SP 800-171 is intended to protect confidentiality of CUI at a moderate baseline. Allowing for ODPs to be determined on an organization-by-organization basis defeats the purpose of creating a standard baseline for protection of CUI across Nonfederal Systems. The creation of an acceptable range or predefined set of acceptable values for the ODPs preserves the intent of standardization and reduces the risk introduced by large variances in ODPs. The development of an acceptable range or predefined set of acceptable values for ODPs should occur in partnership with Government and Nonfederal Organizations to ensure values selected are feasible for implementation in an enterprise environment while reducing risk to confidentiality of CUI. NIST SP 800-172 exists to help address areas where more specificity is needed to protect higher risk CUI data.

Regards,

Amanda M. Allen | SAIC
Cybersecurity Compliance Manager
Governance, Risk, & Compliance (GRC) | IE Chief Information Security Office

[redacted]

Please note that I follow SAIC's 9/80 work schedule and am out of the office every other Friday.