From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Pre-Draft Call for Comments: CUI Series
Date: Wednesday, September 14, 2022 5:32:27 PM
Attachments: Public Comment 171 2022 FINAL.docx

To Whom It May Concern,

Please see attached for UDRI's comments regarding the pre-draft call for comments for the CUI series of publications.

Thanks,

Ronald Creech, MA (Law), CISSP
Information Systems Security Manager
The Office for Research Security (ORS)

University of Dayton Research Institute
300 College Park Dayton, OH 45469-8112
[redacted]

University of Dayton
Research Institute

National Institute of Standards and Technology
Computer Security Resource Center
100 Bureau Drive
Gaithersburg, MD 20899

SUBJECT: Pre-Draft Call for Comments for the NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and its supporting publications.

To Whom It May Concern,

On behalf of the University of Dayton Research Institute's Office for Research Security, I have reviewed the current revisions of the CUI series of publications and included my comments for the newest revision below:

NIST SP 800-171

1. **Comment Type:** General

   Comment: The current iteration of the SP 800-171 is ambiguous, allowing a bit too much room for interpretation. While some room for interpretation is necessary to ensure that multiple types of organizations can all meet the requirements, the publication does not provide enough clarity, leading to the potential for noncompliance due to possible misinterpretation of the requirements. Providing a few more details or requirements for each control, such as those found within SP 800-53, would provide more clarity while maintaining the ability for organizations to meet requirements with different approaches and technologies.

   Suggested Change: Incorporate changes to the SP 800-171 to make it more closely resemble the SP 800-53 controls included in the SP 800-53B's Moderate Baseline.

2. **Comment Type:** General

   Comment: Control 3.1.18, "Control connection of mobile devices," does not describe which "connection" is being referenced. Does is refer to mobile devices remotely connecting to organizational resources (such as email), which would be more accurately covered by control 3.1.12, or does it refer to physical USB connection of mobile devices to other CUI (or out-of-scope) assets? As written, it is unclear. The discussion, which is derived from NIST SP 800-53 AC-19 and talks about basic security guidance for mobile

devices, does not follow the control's name (and possibly not its intent), and would be better matched to a control that matches that of AC-19.

Suggested Change: Change control 3.1.18 to more closely match SP 800-53's AC-19, which requires "configuration requirements, connection requirements, and implementation guidance" for mobile devices and requires connections of mobile devices to organizational systems be authorized.

3. **Comment Type:** General

   Comment: The Awareness and Training section requires organizational training programs, but has no requirement to maintain a record of training. Without training records, organizations will have little evidence of compliance with controls 3.2.1 and 3.2.2, other than procedural or policy requirements.

   Suggested Change: Incorporate SP 800-53's AT-4 into the SP 800-171 to require training records be maintained by the organization.

4. **Comment Type:** General

   Comment: Control 3.3.4 requires an alert in the event of an audit log failure, but does not require actions to fix the failure be taken or defined. The SP 800-53's AU-5 has the requirement to alert and take action (and define these actions) on event log failure, which ensures organizations are prepared for such a failure, should one occur.

   Suggested Change: Incorporate SP 800-53's AU-5(b) into the 800-171 to require organizations to define and take actions on audit logging failures.

5. **Comment Type:** General

   Comment: Control 3.4.1 includes requirements for both baseline configurations and inventories, which are not related enough to be included in one control. Separating them into two separate controls, similar to the way they are separated in SP 800-53, makes more sense from an assessment and tracking standpoint.

   Suggested Change: Separate control 3.4.1's baseline configuration and inventory requirements into two separate controls, similar to the SP 800-53.

6. **Comment Type:** General

   Comment: The discussion on the different accesses and MFA for control 3.5.3, located within Q80-Q85 of the DoD's *Frequently Asked Questions (FAQs) regarding the*

implementation of DFARS Subpart 204.73 and PGI Subpart 204.73, DFARS Subpart 239.76 and PGI Subpart 239.76 revision 3[1], are easier to understand than that within SP 800-171. While specifically a DoD interpretation of the NIST control, making the control easier to understand eliminates the potential for confusion within industry and the need for additional clarification from any agency in the future.

Suggested Change: Incorporate the discussion language of Q80-Q85 of the DoD's *Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 DFARS Subpart 239.76 and PGI Subpart 239.76 revision 3*, or something similar, within control 3.5.3, to clarify its intentions.

7. **Comment Type:** General

Comment: Controls 3.12.1 and 3.12.3 are too similar in wording. One requires periodic assessment to determine if controls are being effective, while the other requires ongoing monitoring to determine if controls are being effective. These two are derivations of SP 800-53's CA-2 and CA-7. CA-2 requires periodic assessments of all controls to be planned and performed to determine if controls are "implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements." This would be satisfied by an annual self-assessment of the organization's compliance with the SP 800-171. CA-7 is the continuous monitoring requirement that determines the effectiveness of the controls on an organizationally defined schedule. While CA-7 requires that assessments are scheduled and performed in accordance with the continuous monitoring strategy, it does distinguish that assessments and monitoring are separate tasks. Having these two controls with similar wording might convince some organizations that both can be satisfied by the same task, when they actually have different levels of scheduling and tasking for each.

Suggested Change: Change the wording of control 3.12.1 to better match that of the SP 800-53's CA-2 to ensure it is distinguished from 3.12.3, as these have two separate intents.

8. **Comment Type:** General

Comment: Control 3.13.12 requires indication that collaborative devices are in use. Not every device has an indicator light, so this control could be interpreted to require a physical slider or cover to disable devices such as webcams or microphones when not in use. Including language to allow indication that the device cannot be used would allow organizations to reach this conclusion earlier.

[1] located at https://dodprocurementtoolbox.com/faqs/cybersecurity

Suggested Change: Add language into control 3.13.12 to allow use of "usage prevention" devices or solutions, such as webcam sliders or microphone disable buttons, in lieu of indicators of use.

Thank you for your consideration of the above feedback.

These comments were authored by Ronald Creech of the Office for Research Security.

Should you desire to follow up with us, please do not hesitate to contact Blaze Baker at Blaze.Baker@udri.udayton.edu.

Respectfully,

Sukh Sidhu, Ph.D.
Executive Director
University of Dayton Research Institute