From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Pre-Draft Call for Comments: SP 800-171 Rev. 3 (Draft)
Date: Friday, September 16, 2022 8:20:06 PM

NIST,

We'd like to commend the team for authoring and maintaining the CUI series. The series provides much needed guidance for this category of information. The opportunity to provide feedback about use and effectiveness of the CUI series is also appreciated. Below are our comments:

- Use of the CUI Series
    - Loss of aggregated CUI is a significant risk to national security. In many cases multiple frameworks may be applicable. Adding a table with some suggesting mappings to how the controls overlap would help to reduce a duplication of effort.

- Updates for consistency with SP 800-53 Revision 5 and SP 800-53B
    - The 800-53 rev 4 Supply Chain controls were not previously mapped to the 800-171 controls; however, the supply chain is mentioned multiple times in the 800-171. Ensure that the new 800-53 supply controls are mapped accordingly.
    - The 800-171 identifies SI-7 Software, Firmware, and Information Integrity as NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI (NCU). Given that Firmware is a fast-growing attack vector, these security controls should be mapped as CUI

- Updates to improve usability and implementation
    - The series as a whole outlines the security controls for the organization, but oftentimes the controls span across different disciplines within the organization. A control that is addressed by one group is often considered met by the organization, when in reality the control is often only partially satisfied. For example, although firmware is software, software developers are usually not responsible for the firmware updates on devices. Both the developers and IT operations would need to do their parts. Separating the control into distinct areas of operation would remove the ambiguity (i.e., Perform maintenance on organizational systems for applications, Perform maintenance on organizational systems for firmware, etc....)
    - Add the requirement for automated scanning tools where applicable (i.e., such as device integrity and maintenance). Most organizations that deal with CUI already have some access to scanning tools. Scanning tools would provide repeatable, reliable and up to date results.

- Firmware attacks have become a popular attack vector for nation state actors. Firmware related exploits are one of the more popular themes across CISA's KEV list. Unfortunately, most organizations don't understand their exposure to these types of attacks. A device integrity category of controls might be beneficial to helping organizations understand their exposure.
- Although the security controls can be satisfied in many different ways, and should not be dependent upon a particular architecture. Identifying how an associated architecture would be applicable to satisfying the requirements in the 800-171 would be useful in a supplemental document.

Please let me know if there are any questions.

Thanks

Jeffrey Hsiao | Federal Solutions Engineer | [redacted] | +[redacted]| **Eclypsium**