Pre-Draft Call for Comments: NIST CUI Series

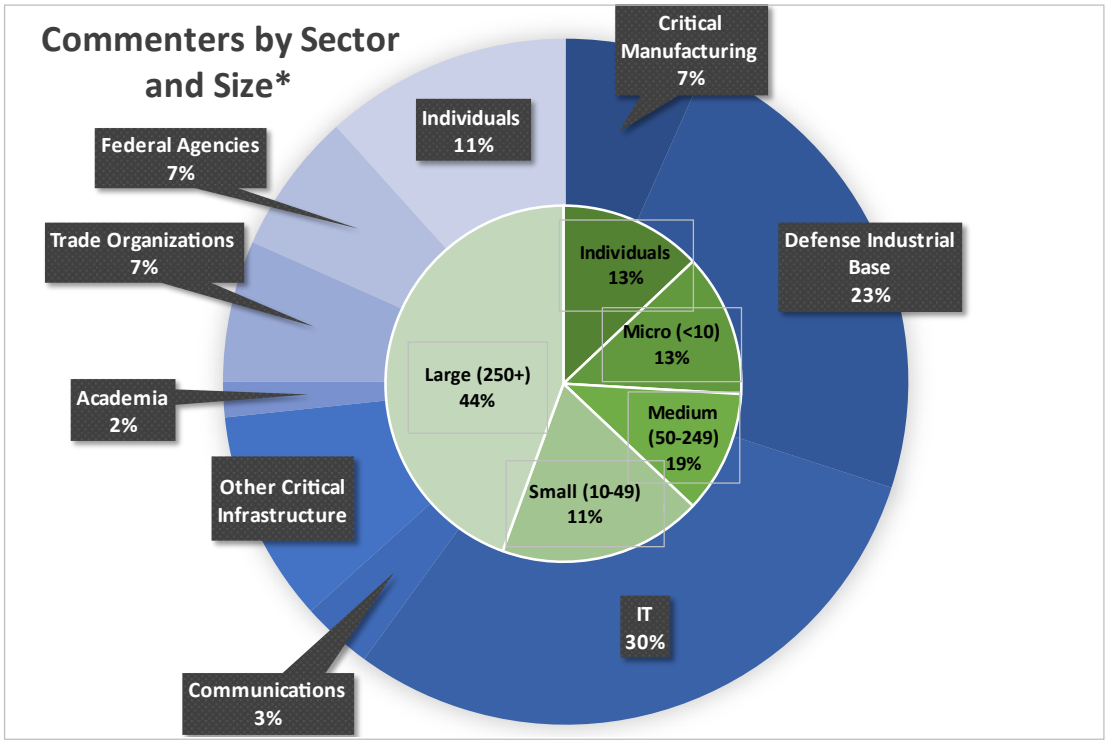
Analysis of Public Comments

November 1, 2022

NIST issued a Pre-Draft Call for Comments on the Controlled Unclassified Information (CUI) series of publications in July 2022. The purpose of the call was to solicit feedback from interested parties to improve NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and its supporting publications SP 800-171A, SP 800-172, and SP 800-172A. During the 90-day public comment period, more than 60 individuals and organizations submitted comments describing how they use the CUI series and provided feedback on potential updates for consistency with SP 800-53, Revision 5, and SP 800-53B. The comments also addressed implementation and usability issues and provided other suggestions to improve the publication. The comments have been posted on the Protecting CUI Project page, and the graph below provides a breakdown of the sector/organization type and organization size of the commenters.

Overview of NIST's Standards and Guidelines Engagement and Update Process

NIST believes that robust, widely understood, and participatory development processes produce the strongest, most effective, most trusted, and broadly accepted standards and guidelines. To that end, NIST conducts at least one public comment period for SPs and IRs open to all interested stakeholders. The public comment period is announced via GovDelivery and other mechanisms, and the authors engage in ongoing stakeholder outreach throughout the development process. Ultimately, the final decision about what to include in the standard or guideline rests with NIST; not all comments received are implemented.



*Note: Organization size is based on the number of people employed

Analysis of Comments Received

Current Use of the CUI Series (Topics 1, 2, 4, and 5), Benefits, and Challenges (Topics 4 and 5)

Responding organizations that primarily represent members of the defense industrial base use the CUI series to meet contractual and/or solicitation requirements for the Defense Federal Acquisition Regulation Supplement (DFARS) and to prepare for the Department of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC). SP 800-171 provides a comprehensive set of requirements to protect CUI, and SP 800-171A provides procedures for the assessment of the CUI security requirement implementation. In many cases, organizations did not use the CUI series alone and referenced the relationships between the series and other NIST guidelines, as well as sector-specific and international cybersecurity standards and requirements (e.g., SP 800-53, NIST Risk Management Framework, Cybersecurity Framework, CMMC, FedRAMP, HiTRUST, ISO 27001, ISO 27002).

The comments refer to the benefit of a uniform set of security requirements to protect CUI and meet contractual and regulatory requirements. Some comments mentioned the use of the series as a source of cybersecurity requirements that support "good cyber hygiene" and "best practices." There have also been challenges in using the CUI series, including implementation issues with specific CUI requirements, difficulties for non-technical and non-cybersecurity stakeholders, and the challenge of implementing multiple sets of requirements and controls (e.g., SP 800-171, SP 800-53, and ISO 27001/27002). While out of scope for NIST, some of the comments addressed the applicable scope of the publication as well as the cost of implementation and compliance with different contractual and regulatory requirements.

Alignment, Opportunities, and Features to Change, Add, and/or Remove (Topics 3, 6, 7, and 8)

Many commenters shared that the CUI series is not the only set of requirements used in their organizations, and there is a need for alignment across the cybersecurity requirements landscape. Suggestions included using the SP 800-53 controls in lieu of the SP 800-171 and 800-172 security requirements, creating an "enhanced overlay" of the SP 800-53 controls to include additional context focused on CUI (similar to the enhanced overlay in SP 800-161), rescinding the CUI series and tailoring the Cybersecurity Framework to meet specific requirements, and developing additional mappings and resources to support implementors. Commenters requested mappings to ISO, HiTRUST, and the NICE Framework.

There was broad support for the update to SP 800-171 to address changes to the controls in the moderate impact baseline (SP 800-53B) and the new inclusive language guidance in NIST Internal Report 8366, *Guidance for NIST Staff on Using Inclusive Language for Documentary Standards*. Commenters supported the inclusion of the NFO controls that are currently tailored out. This would result in a more comprehensive set of security requirements in a single source and provide needed foundational context and guidance for the CUI requirements. Similarly, a few commenters suggested combining the security requirements with the assessment guidance for a consolidated resource. Finally, there was significant feedback requesting closer connection and traceability to the source SP 800-53 controls.

Comments on SP 800-171 Security Requirements and SP 800-172 Enhanced Security Requirements

Many commenters provided specific comments and edits on the security requirements. NIST appreciates the feedback related to implementation challenges. Feedback was provided on 53 different security requirements in SP 800-171 and 9 enhanced security requirements in SP 800-172. The most commented on security requirement was 3.13.11, "*Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.*"

NIST will research and propose options in the forthcoming draft on how best to address feedback on the specific CUI security requirements to balance stakeholder concerns with appropriate countermeasures to protect the confidentiality of CUI.

Many comments and suggestions received were not in scope for the NIST CUI series. However, NIST appreciates the feedback and will share those comments with the appropriate entities. While NIST may not be able to address these suggestions, understanding the perspectives of the organizations that implement the CUI requirements and the many dependencies between NIST guidance and the cybersecurity ecosystem helps improve the overall quality of the CUI series.

Comments and suggestions that were out of scope for the NIST CUI series included:

- Addressing the integrity and availability of CUI
- Ensuring reciprocity between the CUI requirements with other federal cybersecurity requirements (e.g., FedRAMP)
- Current and planned requirements related to the CMMC program implementation
- DFARS compliance, including SPRS 800-171 assessment and scoring
- Identifying CUI
- Addressing technology-specific implementations (e.g., cloud-based systems, zero trust architectures, applicability to operational technology and the Internet of Things)
- Contractual requirements of federal agencies
- Software bill of materials (SBOM)

Next Steps

An initial public draft of SP 800-171, Revision 3, is planned for late spring 2023. Based on the feedback from the pre-draft call for comments and ongoing NIST research efforts, the following updates are planned in the forthcoming draft:

- Update the security requirements for consistency and alignment with SP 800-53, Revision 5 (including inclusive language updates), and the SP 800-53B moderate-impact baseline
- Develop a CUI overlay (Supplementary Appendix to the existing security requirement catalog) to better link the CUI security requirements to the SP 800-53 controls for stakeholder feedback
- Consider and propose options on how best to address stakeholder feedback on the NFO control tailoring

The above list of proposed updates is not exhaustive, and additional changes may be considered to improve the quality and useability of the publication. Throughout the update process, NIST will continue with ongoing outreach and stakeholder engagement, including holding a webinar during the public comment period of draft SP 800-171, Revision 3. NIST acknowledges and appreciates the organizations and individuals who contributed their time, knowledge, and feedback to the update process. Such

participation helps to ensure that the CUI series addresses the security needs of organizations charged with protecting controlled unclassified information.