NIST SP 800-171 Revision 3 Initial Public Draft

Analysis of Public Comments

August 2023

In late 2023, NIST began the update to Special Publication (SP) 800-171 by leveraging the input from the Pre-Draft Call for Comments on the NIST Controlled Unclassified Information (CUI) series issued in July 2022 and recent updates to SP 800-53r5 (Revision 5) and SP 800-53B. The update represents over one year of data collection, technical analyses, customer interaction, redesign, and development of the security requirements and supporting information for the protection of CUI. Many trade-offs have been made to ensure that the technical and non-technical requirements have been stated clearly and concisely while also recognizing the specific needs of federal and nonfederal organizations.

The initial public draft (ipd) of SP 800-171r3 was issued in May 2023 for a 90-day public comment period. Reviewers were encouraged to provide feedback on all or parts of the draft. In particular, NIST sought comments and recommendations on the recategorization of controls, the inclusion of organization-defined parameters (ODP), and the prototype CUI overlay. Over 80 organizations and individuals submitted comments.

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 all technical publications in the Cybersecurity and Privacy portfolio. 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.

Analysis of Comments Received

Almost 1,700 comments were received from 82 commenters on SP 800-171r3 ipd and its supporting resources (i.e., analysis of changes, FAQ, and CUI Overlay). Over 98% of the comments submitted focused on the draft publication.

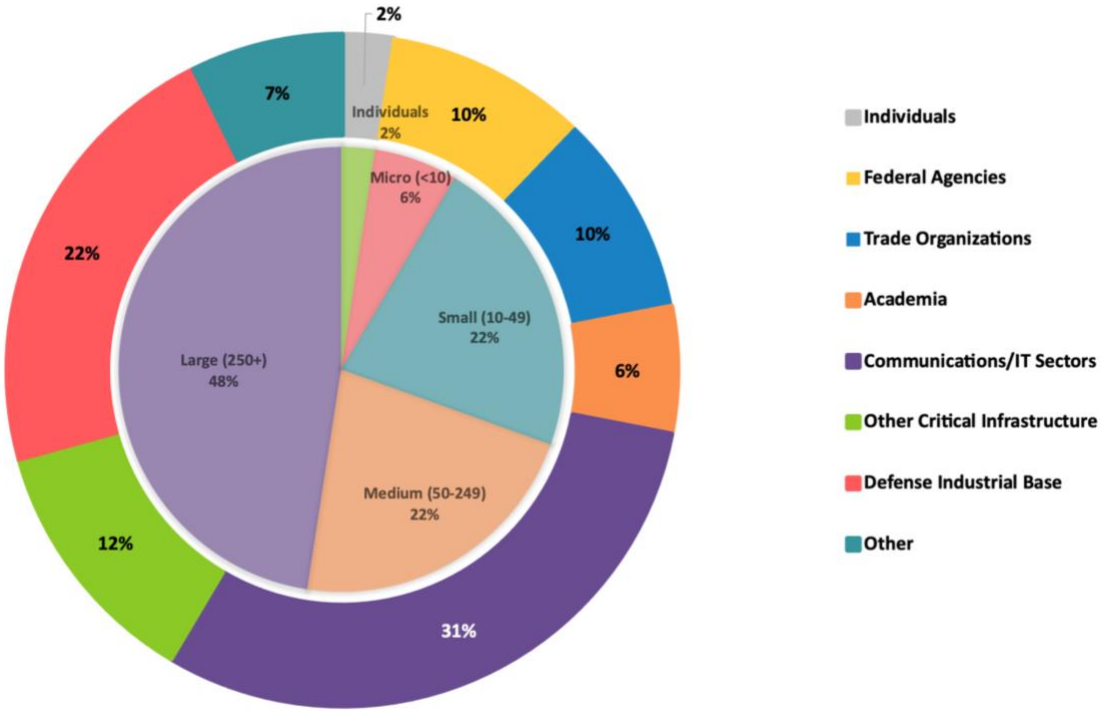

Figure 1. Commenters by Sector and Organization Size

Recategorization of Controls

The IPD included a significant change in how the SP 800-53 controls were categorized and recast many controls from NFO[1] to CUI[2] or NCO[3]. There was limited feedback recommending changes to specific control categorizations (i.e., a control categorized as CUI with a recommendation to recategorize as FED or NCO). Several commenters recommended removing the NFO tailoring category and recategorizing those controls appropriately to provide an unambiguous set of requirements for implementing organizations and assessors.

A few commenters also indicated that some of the new SP 800-171 security requirements based on changes to the SP 800-53r5 controls seemed duplicative of other requirements. Recommendations included combining similar requirements, even if those requirements are derived from different source SP 800-53 controls.

[1] Expected to be implemented by nonfederal organizations without specification.
[2] Directly related to protecting the confidentiality of CUI.
[3] Not directly related to protecting the confidentiality of CUI.

Prototype CUI Overlay

There were limited comments on the prototype CUI overlay. While the majority of commenters expressed support for the concept and appreciated the traceability and alignment between the SP 800-53 controls and the SP 800-171 security requirements, there is an opportunity for NIST to better educate the community about (SP 800-53) control overlays, including their purpose and benefits.

Use of Organization-Defined Parameters (ODP)

Many of the comments received were related to the introduction of ODPs in the security requirements. While some organizations supported the concept, which provides flexibility to federal agencies and nonfederal organizations, there were concerns about the responsible entity for defining ODPs and the potential for inconsistent expectations and implementations (e.g., different ODP values used by different federal agencies resulting in the need for multiple and costly implementations). Common recommendations included having a single entity define ODPs for all nonfederal organizations, although commenters suggested many different entities, including NIST, a panel of federal agencies, industry coalitions/groups, and nonfederal organizations. Some commenters recommended removing all ODPs from the publication, others provided suggestions for changes to ODPs for specific requirements, and some recommended adding ODPs to security requirements.

Comments on Security Requirements

Over 80% of the comments received addressed one or more SP 800-171 security requirements, and there was at least one comment for almost each one.[4] Many of the comments addressed recommendations for parameter values and concerns about the implementation of ODPs for each requirement. Some commentors provided constructive feedback on how to improve the discussion section of each security requirement to promote understanding of the requirement intent and facilitate better implementation. Interestingly, only 21 comments were received on security requirement 3.13.11 (Cryptographic Protection). Some organizations and individuals elected to submit identical comments. Table 1 identifies the security requirements that received the most comments.

Table 1. Number of comments received on SP 800-171r3 ipd security requirements

Requirement Number and Name	Total Comments	Comments on ODPs
3.1.1 Account Management	42	16
3.12.5 Independent Assessment	39	11
3.5.7 Password Management	37	6
3.1.21 External Systems – Limits and Restrictions on Authorized Use	28	6
3.14.01 Flaw Remediation	27	4
3.16.03 External System Services	27	5

[4] There were no comments received on security requirements 3.4.5 Access Restrictions for Change, 3.5.11 Authenticator Feedback, and 3.14.2 Malicious Code Protection.

A few commenters indicated a preference for the format and text of the SP 800-171r 2 requirements and recommended restoring certain requirements (e.g., 3.7.1 and 3.14.5) that were withdrawn.

Alignment With SP 800-53 and Other Standards/Guidelines

Consistent with the feedback on the Pre-Draft Call for Comments, the majority of the commenters supported the closer alignment between the SP 800-171 security requirements and the SP 800-53r5 controls. A small number of commenters did not support the alignment between the security requirements and controls nor the additional specificity produced by the alignment. One commenter suggested that SP 800-171 should be aligned with a different control framework rather than SP 800-53, indicating an opportunity for NIST to provide additional informative resources in our portfolio of cybersecurity risk management guidance. Many commenters requested additional mappings and encouraged coordination and alignment with the Cybersecurity Maturity Model Certification (CMMC) program.

Additional Implementation Guidance

Many commenters representing organizations of all sizes requested additional implementation guidance and resources. Even with the updated discussion sections, commenters requested additional clarity to assist with interpreting the requirements, especially for small-to-mid-size organizations. Some commenters requested a smaller subset of requirements for small-to-mid-size businesses and cost-effective implementation examples and case studies.

Less than 5% of the comments received were not in scope for NIST. However, NIST appreciates the candid feedback and suggestions. While NIST may be unable to directly address the comments, a better understanding of the perspectives of the CUI user community — including the challenges faced by implementers and opportunities for improvement across the federal cybersecurity ecosystem — helps improve our guidelines and resources. Examples of feedback that were out of scope for NIST include:

- *Current and planned requirements related to the Cybersecurity Maturity Model Certification (CMMC), the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 Clause, and CMMC/DFARS compliance*
- *Defining the parameter values for ODPs for all federal agencies*
- *Identification and marking of CUI*
- *Identification of "flow down requirements"*
- *Identification of specific solutions and implementations for "compliance"*
- *Cost of implementation*

Next Steps

NIST is adjudicating the comments and preparing the final public draft (fpd) of SP 800-171r3. Concurrently, the team is developing the initial public draft of SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*, which will provide assessment procedures for the SP 800-171r3 security requirements. NIST anticipates releasing SP 800-171r3 fpd and SP 800-171A ipd for public comment in Q1 of FY 2024 (October – December 2023) and looks forward to ongoing engagement with users during the comment period.

Based on a preliminary review and analysis of the comments received, NIST plans to make the following changes in SP 800-171r3 fpd:

- Reduce the number of ODPs
- Reevaluate the tailoring categories and tailoring decisions to eliminate the NFO category, and tailor out controls that may be adequately addressed by other related controls
- Restructure and streamline the discussion sections to only address the security requirement and sequence the text to correspond with specific requirement items

Please provide send questions and comments to the authors at 800-171comments@list.nist.gov.