NIST SP 800-171 Revision 3 (Final Public Draft) and SP 800-171A Revision 3 (Initial Public Draft)

Analysis of Public Comments

February 2024

NIST concurrently issued Special Publication (SP) 800-171r3 (Revision 3) (final public draft) and SP 800-171Ar3 (initial public draft) for public comment in November 2023. During the comment period, NIST received over 750 comments from over 40 individuals.

> ***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 the 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.*

Overview of Significant Changes

This update to SP 800-171r3 includes changes made in response to the public comments received on the initial public draft (ipd). Significant changes include:

- Elimination of the NFO control tailoring category
- Introduction of a new tailoring category for controls that are addressed by other related controls (ORC)
- Reduction of the number of organization-defined parameters (ODPs) achieved by removing ODPs that did not significantly impact the security requirement
- Clarification of responsibility for assigning ODP values
- Consolidation of security requirements for better consistency with SP 800-53
- Refinement of discussion sections for better understanding and usability
- Addition of leading zeros to security requirements to support automated tool usage

For a detailed requirement-by-requirement analysis of the changes between SP 800-171r3 (fpd) and SP 800-171r2, refer to the change analysis (Rev. 2 to Rev. 3 [fpd]) spreadsheet available on the publication details page.

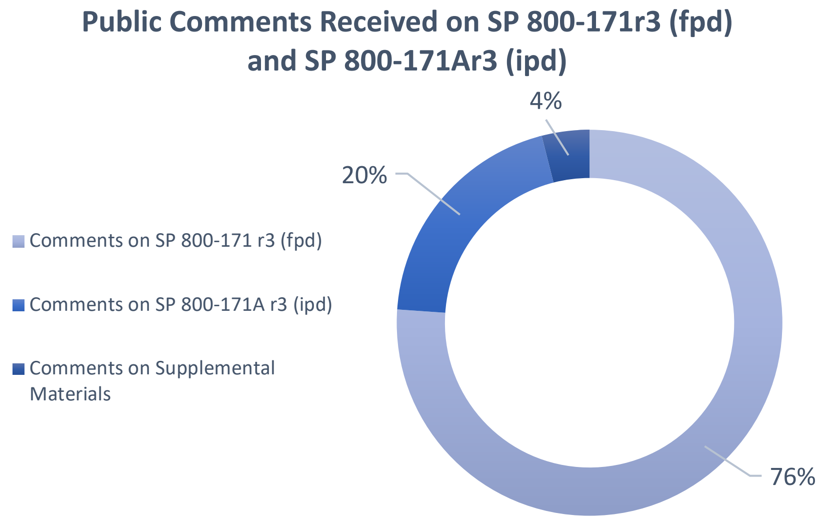
The SP 800-171Ar3 (ipd) reflects the security requirements in SP 800-171r3 (fpd) and includes the following significant changes:

- Assessment procedure syntax restructured to align with SP 800-53Ar5

- References section added to provide source assessment procedures from SP 800-53A
- A one-time change made to the publication version number (skipping "Revision 2") to align with SP 800-171r3

Analysis of Comments Received

The number of public comments and number of individuals and organizations submitting comments decreased compared to those received in response to SP 800-171r3 (ipd).[1] The majority of comments received during this public comment period addressed the SP 800-171r3 (fpd) security requirements, though many comments were associated with more than one topic (e.g., comments addressed use of organization-defined parameters and the discussion).



SP 800-171: Use of Organization-Defined Parameters (ODP) and the Term "Periodically"

The use of ODPs and the term "periodically" in the requirements received the most comments at 115. Fewer than 8% of those comments suggested adding ODPs to the requirements. Six commenters suggested that NIST clarify the entity responsible for assigning ODP values and provided suggestions for potential entities to define ODPs, although these issues are explicitly addressed in the publication and FAQ. There were over 70 comments on defining ODPs and the term "*periodically*" in specific requirements as well as suggestions for values/ranges of values to use. Twenty-six comments recommended removing specific ODPs.

SP 800-171: Content and Structure of the Source SP 800-53 Control and Control Enhancement

NIST made the design decision to have the SP 800-171 security requirement structure and content mirror the SP 800-53 source controls. Over 25 comments provided feedback that could benefit from *first* being applied to a future revision of SP 800-53 and then included in future revisions of SP 800-171. Many of the suggestions to the [SP 800-171] security requirements and discussion sections were helpful to

[1] Approximately 1,700 comments were received on SP 800-171r3 (ipd).

clarify scope and intent. NIST requests that commenters use the NIST SP 800-53 Public Comment Website to provide feedback on improving the [SP 800-53] controls.

While the [SP 800-171] security requirements and discussion sections are designed to mirror the [SP 800-53] controls to the maximum extent possible, there are differences due to tailoring decisions for protecting the confidentiality of controlled unclassified information (CUI).

SP 800-171: Tailoring Decisions

Over 40 comments addressed tailoring decisions, including specific decisions for other related controls (ORCs), the decision to tailor at the control item level, suggestions for tailoring in additional [SP 800-53] controls and control enhancements, and recommendations for further tailoring of [SP 800-171] requirements and discussion sections to better support the protection of CIU confidentiality.

SP 800-171: Scope and Applicability

There were continued questions and comments about the scope and applicability of the SP 800-171 security requirements, both broadly and specific to individual requirements. Approximately 40 comments addressed CMMC, DFARS, FedRAMP, the identification and marking of CUI, flow-down requirements, and the cost of implementation — all topics deemed out of scope for NIST to address. However, NIST appreciates the candid feedback, suggestions that help provide a better understanding of the perspectives of and challenges faced by the CUI user community, and the opportunity to work across the federal cybersecurity ecosystem to improve all resources.

SP 800-171A: Assessment Procedures

NIST received fewer than 150 comments on SP 800-171Ar3 (ipd). Many commenters were not as familiar with the purpose, scope, and structure of the [SP 800-171A] assessment procedures or the source [SP 800-53A] assessment methodology and terminology. Approximately 25 comments requested clarification on specific terminology related to the assessment methodology and specific security requirement assessment procedures. Over 20 comments suggested the addition of specific assessment procedures for security requirements to further define portions of the source security requirement (e.g., to determine “applicable CUI rules” in security requirement 3.1.9). Other comments identified errors, omissions, and opportunities for improving consistency and usability in the assessment procedures.

Supplemental Resources: FAQ, CUI Overlay, and Analysis of Changes

There were approximately 25 comments on the FAQ, CUI Overlay, and Analysis of Changes between [SP 800-171] Revision 2 and Revision 3 (fpd). Most of these comments identified minor errors and omissions in the CUI overlay tailoring decisions and analysis of changes.

Next Steps

NIST appreciates the thoughtful and detailed comments that were submitted. After comment adjudication, NIST plans to publish SP 800-171r3 and SP 800-171Ar3 in FY24 Q3 (i.e., Spring 2024). NIST will continue to engage with the CUI community to share information and receive feedback to ensure that our portfolio of resources reflects the needs of users and provides adequate safeguards to protect CUI.

Based on the initial adjudication of comments, some of the changes to SP 800-171, SP 800-171A, and the supplemental resources will include:

- Corrections for errors, omissions, and typos
- Better alignment and consistency with the source publications, SP 800-53 and SP 800-53A
- Review of ODPs and use of the term "periodically" to identify the best balance between requiring explicit definition of parameters and providing flexibility to implementers
- Review of all [SP 800-171] discussion sections to better tailor the guidance for protecting the confidentiality of CUI without adding specific examples
- Additional background information about the source [SP 800-53A] assessment methodology and terminology[2]
- Changes to the [SP 800-171A] assessment procedures based on changes to the [SP 800-171] security requirements
- Updates to the FAQ to include additional information on the:
    - Scope and applicability of SP 800-171 and SP 800-171A
    - History and evolution of the CUI security requirements and associated assessment procedures
    - Responsibility for defining ODPs

NIST will not introduce security requirements in SP 800-171 that cannot be sourced to SP 800-53. Commenters are welcome to use the NIST SP 800-53 Public Comment Website to provide feedback on improving the [SP 800-53] controls, and NIST will incorporate accepted SP 800-53 content into future revisions of SP 800-171.

Following the publication of SP 800-171r3 and SP 800-171Ar3, NIST will begin revising SP 800-172 and SP 800-172A. Similar to the process for SP 800-171r3 (ipd), the enhanced security requirements will be issued first, followed by a concurrent release of the final public draft of the [SP 800-172] enhanced security requirements and initial public draft of the [SP 800-172A] assessment procedures.

In addition to continuing to issue this suite of publications in PDF format, future revisions of SP 800-171, SP 800-171A, SP 800-172, and SP 800-172A will be available concurrently via the Cybersecurity and Privacy Reference Tool (CPRT)[3] as they are finalized.

Please send questions and comments to 800-171comments@list.nist.gov.

[2] In FY24 Q3, NIST will release free, on-demand introductory courses on SP 800-53, SP 800-53A, and SP 800-53B. See https://nist.gov/RMF

[3] SP 800-171 Revision 2, SP 800-172 and SP 800-172A (current final versions) are now available on CPRT. SP 800-171A (current final version) will be available in CPRT by end of Q2 FY24.