# Initial Public Draft (IPD) NIST SP 800-171, Revision 3

*Frequently Asked Questions*

May 10, 2023

On July 19, 2022, NIST announced its intention to update the series of Special Publications dedicated to the protection of Controlled Unclassified Information (CUI). We have recently completed the initial public draft (IPD) of NIST Special Publication (SP) 800-171, Revision 3. The proposed revisions to the publication have been guided and informed by the public comments received and NIST's responsibility to meet the requirements of the Federal Information Security Modernization Act, Executive Order (EO) 13556, CUI federal regulation, and Office of Management and Budget (OMB) Circular A-130.

The following frequently asked questions provide background information and rationale for the changes proposed for NIST SP 800-171, Revision 3:

**What are the significant changes between NIST SP 800-171, Revision 2 and Draft NIST SP 800-171, Revision 3?**

- Streamlined introductory information to improve clarity and customer understanding
- Eliminated the distinction between basic and derived security requirements
- Updated the security requirements and families to reflect updates in the NIST SP 800-53, Revision 5 and NIST SP 800-53B moderate control baseline and updated tailoring criteria
- Increased the specificity of security requirements to remove ambiguity, improve the effectiveness of implementation, and clarify the scope of assessments
- Introduced organization-defined parameters (ODP) in selected security requirements to increase flexibility and to help organizations better manage risk
- Removed outdated and redundant security requirements
- Detailed analysis of the changes between Revision 2 and Revision 3 (linked from the Revision 3 publication details)
- Developed a protype CUI overlay (linked from the Revision 3 publication details)

**Why did NIST eliminate the distinction between basic and derived security requirements?**

The intent of FIPS 200 was to define high-level security requirements that federal agencies satisfy by selecting and tailoring controls from NIST SP 800-53. One of the unintended side effects of using FIPS 200 as an authoritative source for the development of the NIST SP 800-171 security requirements was the lack of specificity in the requirements. Refocusing the security requirements using only NIST SP 800-53 as the single authoritative source significantly increased the specificity and clarity.

**Why did NIST increase the level of detail in security requirement specifications?**

The security requirements in previous versions of NIST SP 800-171 were stated at a high level of abstraction and left detailed specification to the implementers and the assessors. While certain organizations viewed this lack of specificity favorably, others stated that it made the solution space too broad and left the requirements open to interpretation and subjective in their application. The lack of specificity also made assessments more difficult since assessors had different expectations and

interpretations on whether organizations satisfied the requirements. The increased specificity in Revision 3 continues to allow for flexibility in implementation but also aligns security requirement language to the control language in NIST SP 800-53.

**Why did NIST incorporate selected security requirements into other requirements, resulting in multi-part requirements?**

In many cases, security requirements are closely related to other requirements. For efficiency and increased understanding, certain requirements have been withdrawn and incorporated into other requirements when there is a direct relationship or logical association. Such grouping resulted in multi-part requirements but did not add to the total number of requirements. The grouping of requirements is also consistent with the content of the security controls in NIST SP 800-53.

**Why did NIST align the security requirement structure and language to be consistent with NIST SP 800-53?**

The public comments received from the request for information indicated that many organizations are overwhelmed with the number of different security and risk management frameworks in use by the public and private sectors. To better align two widely used NIST resources, a strategy has been initiated to transition the security requirements in NIST SP 800-171 to the control language in NIST SP 800-53. Related to that transition, NIST has developed a protype CUI overlay. The prototype overlay shows how the NIST SP 800-53B moderate control baseline is tailored at the control and control-item levels to express the security requirements necessary for the protection of CUI from unauthorized disclosure.

**Why did NIST introduce organization-defined parameters (ODP) in selected security requirements?**

Organization-defined parameters are used in the NIST SP 800-53 controls to provide flexibility to federal agencies in tailoring controls to support specific organizational missions or business functions and to manage risk. To provide that same flexibility to federal agencies in working with nonfederal organizations to protect CUI, ODPs have been selectively employed in the requirements in NIST SP 800-171, Revision 3, consistent with their use in NIST SP 800-53, Revision 5. Once ODPs have been defined, they become part of the security requirement and can be assessed as such. ODPs also help simplify assessments by providing greater specificity to the requirements being assessed and reducing ambiguity and inconsistent interpretation by assessors. Federal agencies can elect to specify ODPs, provide guidance on selecting ODPs for nonfederal agencies, or allow nonfederal agencies to self-select ODP values.

**Why did NIST add new security requirements to the catalog and remove other requirements from the catalog?**

NIST is required by federal law, regulation, and policy to develop, make available, and maintain a variety of security standards and guidelines. As part of this ongoing responsibility, the publications are routinely updated with state-of-the-practice safeguards and countermeasures to help organizations protect CUI from unauthorized disclosure. When the moderate control baseline in NIST SP 800-53B was updated to reflect the security controls in NIST SP 800-53, Revision 5, it automatically triggered an update to the security requirements in NIST SP 800-171. That update resulted in the addition of new security requirements in Revision 3. It also resulted in the removal of certain requirements from the catalog. Information regarding the transition of security requirements from NIST SP 800-171, Revision 2 to Revision 3 can be found on the publication details web page.

**Why did NIST add new security requirement families to the catalog?**

Three new security requirement families have been added to Revision 3 to maintain consistency with the NIST SP 800-53B moderate control baseline. The families include the *Planning (PL)* family, the *System and Services Acquisition (SA)* family, and the *Supply Chain Risk Management (SR)* family. In addition, the *Security Assessment* family has been renamed the *Security Assessment and Monitoring (SA)* family.

**Why did NIST change some of the security control tailoring criteria assignments?**

Based on the public comments received and lessons learned during the seven years of NIST SP 800-171, selected tailoring criteria changes have been made. Feedback from the pre-draft call for comments indicated that certain NFO controls, including foundational ones such as the XX-1 controls from each family (e.g., AC-1, Policy and Procedures), were not being implemented or assessed. Appendix E (Table 41) in NIST SP 800-171 describes the tailoring criteria reassignments that were made during the transition from Revision 2 to Revision 3. The reassignments resulted in a significant reduction in the number of NFO controls and an increase in the number of NCO, FED, and CUI controls.

**Why did NIST add a new tailoring criterion?**

To ensure completeness in the tailoring analyses applied to the NIST SP 800-53B moderate control baseline, a new tailoring criterion of *Not Applicable (NA)* has been added. This tailoring criterion is used for the *Program Management (PM)* and *Personally Identifiable Information (PII) Processing and Transparency* families, as both control families are not allocated to any NIST SP 800-53B security control baseline (i.e., Low, Moderate, High).

**What enhancements did NIST make to increase the usability of the catalog?**

Many enhancements have been made to the publication to increase its usability, help facilitate the implementation and assessment of the requirements, and improve the overall customer experience. These include:

- Adding titles to each security requirement
- Implementing internal hyperlinks to help readers quickly navigate through the sections and tables contained in the publication
- Implementing hyperlinks to the NIST SP 800-53 security controls in the NIST Cybersecurity and Privacy Reference Tool (CPRT)
- Refreshing the content of the discussion section for each security requirement
- Adding a references section for each requirement to provide direct linkages to the authoritative source control(s) in NIST SP 800-53 and other NIST technical publications to help facilitate the implementation and assessment of the requirement
- Adding transition mapping tables to help organizations understand the changes in Revision 3
- Developing a CUI *overlay* that describes how each control and control item in the NIST SP 800-53B moderate baseline is tailored for NIST SP 800-171

**Will the security requirements in the catalog be available in different data formats?**

After NIST SP 800-171, Revision 3 is issued as a final publication, NIST will update the security requirements in CPRT and include CSV and JSON files that can be derived from CPRT. The CUI overlay will be published in Excel format.

**Why did NIST remove the mapping of the NIST SP 800-53 security controls to the ISO 27001 security controls?**

The mapping table in NIST SP 800-171, Revision 3 will focus exclusively on the NIST SP 800-53 security controls, which is the authoritative source for the security requirements. NIST is currently updating the mapping of the NIST SP 800-53, Revision 5 controls to the ISO/IEC 27001:2022 controls and will issue the update by fall 2023.

**Are there special provisions for small and mid-size organizations that are required to implement the security requirements?**

The CUI federal regulation requires federal agencies that use federal information systems to process, store, or transmit CUI to comply with NIST standards and guidelines. The responsibility of federal agencies to protect CUI does not change when the information is shared with nonfederal organizations. Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems, irrespective of the organization's size. NIST is responsible for developing and publishing the security requirements for the protection of CUI. The application and implementation of the requirements and any compliance issues related to the content of NIST SP 800-171 are the responsibility of the federal agency that has a relationship with a nonfederal organization, as expressed in a specific contract or agreement.