FREQUENTLY ASKED QUESTIONS

NIST SP 800-171r3 and NIST SP 800-171Ar3

On July 19, 2022, NIST announced its intention to update the series of Special Publications dedicated to the protection of Controlled Unclassified Information (CUI). NIST Special Publication (SP) 800-171r3 (Revision 3) and SP 800-171Ar3 have been guided and informed by:

- The public comments received during the pre-draft call for comments, initial public draft comment period for SP 800-171r3, the final public draft comment period for SP 800-171r3, and the initial public draft comment period for SP 800-171Ar3
- NIST's responsibility to meet the requirements of the Federal Information Security Modernization Act (FISMA), Executive Order (EO) 13556, CUI federal regulations, and Office of Management and Budget (OMB) Circular A-130

The following frequently asked questions provide background information and rationale for the changes in SP 800-171r3 and SP 800-171Ar3:

What is the scope and applicability of SP 800-171r3?

The security requirements in SP 800-171r3 are only applicable to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components.

What are the significant differences between SP 800-171r2 and SP 800-171r3?

- Streamlined introductory information to improve clarity and customer understanding
- Eliminated the distinction between basic and derived security requirements
- Updated security requirements and families to reflect changes in the SP 800-53r5 control catalog, SP 800-53B moderate control baseline, and tailoring criteria
- Increased the specificity of security requirements to remove ambiguity, improve the effectiveness of implementation, and clarify the scope of assessments
- Eliminated the NFO control tailoring category
- Introduced a new control tailoring category for controls that are addressed by other related controls (ORC)
- Introduced organization-defined parameters (ODP) in select security requirements to increase flexibility and to help organizations better manage risk
- Clarified the responsibility for assigning ODP values
- Removed outdated and redundant security requirements
- Combined security requirements (or parts of requirements) with other requirements for consistency and ease of use
- Added security requirements due to control categorization changes
- Sequenced the content in the discussion sections to align with the individual parts of the requirements
- Modified the tailoring categories of selected controls and control items (subparts of controls)

- Updated tailoring and mapping tables and developed transition mapping tables that outline changes between Revision 2 and Revision 3
- Added an Appendix to consolidate ODPs in a single location for easy reference
- Developed a CUI overlay that is available as a separate document on the NIST publication details website with SP 800-171r3
- Added leading zeros to security requirement numbers to achieve greater consistency with SP 800-171Ar3 numbering formats and to support automated tool usage

What enhancements were made to increase the usability of the publication?

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:

- Titles for each security requirement
- Internal hyperlinks to help readers quickly navigate sections and tables
- Hyperlinks to the SP 800-53 security controls in the NIST Cybersecurity and Privacy Reference Tool (CPRT)
- Updated content in the security requirement discussion sections
- A references section for each requirement that provides direct links to the authoritative source controls in SP 800-53 and other NIST technical publications
- Transition mapping tables to help organizations understand the changes in Revision 3
- An appendix that consolidates ODPs in a single location to facilitate ease of reference and use
- A CUI overlay that describes how each control and control item in the SP 800-53B moderate baseline is tailored for SP 800-171

Why were the security requirement structure and language aligned to be consistent with SP 800-53?

The public comments received from the request for information indicated that many organizations are overwhelmed by the number of different security and risk management frameworks in use by public and private sectors. To better align two widely used NIST resources, a strategy has been initiated to transition the security requirements in SP 800-171 to the control language in SP 800-53. NIST has also developed a CUI overlay that shows how the 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 was the distinction between basic and derived security requirements eliminated?

The intent of FIPS 200 was to define high-level security requirements that federal agencies satisfy by selecting and tailoring controls from SP 800-53. Recasting the security requirements using only SP 800-53 as the single authoritative source significantly increased the specificity and clarity of the requirements.

Why was the level of detail in security requirement specifications increased?

The security requirements in previous versions of SP 800-171 were stated at a high level of abstraction and left detailed specification to implementers and 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 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 with the control language in SP 800-53.

Why were selected security requirements incorporated 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 has resulted in multi-part requirements but does not add to the total number of requirements. The grouping of requirements is also consistent with the content of the security controls in SP 800-53.

Why were organization-defined parameters (ODP) introduced in selected security requirements?

Organization-defined parameters are used in the 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 working with nonfederal organizations to protect CUI, ODPs have been selectively employed in the requirements in SP 800-171r3, consistent with their use in SP 800-53r5. 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 specify ODPs, provide guidance to nonfederal organizations on selecting ODPs, or allow nonfederal organizations to select ODP values.

Who is responsible for defining organization-defined parameters?

The determination of ODP values can be guided and informed by laws, Executive Orders, directives, regulations, policies, standards, guidance, or mission and business needs. If a federal agency or consortium of agencies do not specify a particular value or range of values for an ODP, nonfederal organizations must assign those values to complete the security requirement.

What is meant by “the organization”?

In a security requirement with an ODP, an organization can refer to either the federal agency or the nonfederal organization establishing the parameter values for the requirement.

Why were new security requirements added to the catalog and other requirements removed?

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, NIST 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 SP 800-53B was updated to reflect the security controls in SP 800-53r5, it automatically triggered an update to the security requirements in SP 800-171. That update resulted in the addition of new security requirements and the removal of certain requirements in Revision 3.

Why were new security requirement families added to the catalog?

Three new security requirement families have been added to Revision 3 to maintain consistency with the SP 800-53B moderate control baseline: 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 (CA) family.

Why were some of the security control tailoring criteria assignments changed?

Selected tailoring criteria changes have been made based on the public comments received and lessons learned during the seven years that organizations used SP 800-171. 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 in nonfederal organizations. The tailoring criteria reassignments that were made during the transition from Revision 2 to Revision 3 resulted in the elimination of the NFO tailoring criterion (and assigned controls) and an increase in the number of NCO, FED, and CUI controls.

Why were new tailoring criteria added?

A new tailoring criterion called Not Applicable (NA) has been added to ensure completeness in the tailoring analyses applied to the SP 800-53B moderate control baseline. This tailoring criterion is used for the Program Management (PM) and Personally Identifiable Information (PII) Processing and Transparency families. The controls in those families are not allocated to any SP 800-53B control baseline (i.e., Low, Moderate, High). In addition, a new tailoring criterion called Other Related Control (ORC) was created. The ORC criterion means that the protection capability provided by the control is also provided by another control in the same or different control family. Using this tailoring option helps eliminate potential redundancy in requirements without affecting the protection of CUI in nonfederal systems and organizations.

Will the security requirements in the publication be available in different data formats?

SP 800-171r3 and SP 800-171Ar3 are available in CPRT and include spreadsheet and JSON files. The CUI overlay is available in spreadsheet format on the publication details page under "Supplemental Materials."

Why was the mapping of the SP 800-53 security controls to the ISO 27001 security controls removed?

The mapping table in SP 800-171r3 focus exclusively on the SP 800-53 security controls, which is the authoritative source for the security requirements. NIST also recently updated the mapping of the SP 800-53r5 controls to the ISO/IEC 27001:2022 controls.

What are the significant changes between NIST SP 800-171A and NIST SP 800-171Ar3?

- SP 800-171Ar3 assessment procedures reflect corresponding updates to the security requirements in SP 800-171r3.

- Assessment procedure syntax was restructured to align with SP 800-53A.
- A references section was added to provide source assessment procedures from SP 800-53A.
- Additional guidance was included on the fundamentals of conducting security requirement assessments.
- A one-time change to the publication version number was made to align with SP 800-171r3.

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 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.

What other NIST resources are available?

- Security & Privacy Controls and Assessing Security & Privacy Controls Introductory Courses: NIST offers a series of free, on-demand, online courses between 45-60 minutes long that provide a high-level introduction to and overview of the foundational publications SP 800-53 and SP 800-53A.
- NIST is committed to providing additional resources for implementers by Q1 FY25, including mappings/crosswalks between SP 800-171r3 and SP 800-171r2, SP 800-53r5, and the Cybersecurity Framework 2.0, as well as a SP 800-171r3 and SP 800-171Ar3 quick start guide for small and medium enterprises.