SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (withdrawn May 14, 2024)

NIST SP 800-171 Rev. 2: 110 CUI security requirements in 14 families, withdrawn by NIST on May 14, 2024 but still the...



What it is

NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, was withdrawn by NIST on May 14, 2024 and superseded by NIST SP 800-171 Revision 3 . Yet it is still the edition the Department of Defense cites: 32 CFR 170.14 makes the CMMC Level 2 security requirements identical to those of SP 800-171 R2. DFARS 252.204-7012 binds covered contractor information systems to the SP 800-171 in effect when a solicitation is issued or as authorized by the contracting officer. NIST published Rev. 2 on February 21, 2020 and issued an errata update on January 28, 2021. It sets out 110 security requirements in 14 families for protecting the confidentiality of CUI.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Revision 2 (February 2020; updated January 28, 2021); withdrawn May 14, 2024
EFFECTIVE February 21, 2020	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

Why it matters

- **A defined scope** Sec. 1.1 limits the requirements to system components that process, store or transmit CUI or protect such components, and lets an organization isolate those components in a separate CUI security domain by physical or logical separation.
- **A fixed, numbered set** 110 requirements numbered 3.1.1 to 3.14.7 across 14 families, each with an informative discussion section drawn from SP 800-53 that does not extend the requirement (Chapter 2).
- **Traceable origins** Basic requirements come from FIPS 200 and derived requirements from the SP 800-53 moderate baseline; Appendix D maps every requirement to SP 800-53 and ISO/IEC 27001 controls and Appendix E records each tailoring decision (Sec. 2.2).
- **Two documents that decide contracts** The system security plan (3.12.4) and the plan of action (3.12.2); Sec. 3.12.2 notes that agencies may treat both as critical inputs to the decision to process CUI on a nonfederal system or to award a contract.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-171 Rev.2

Requirement Library

Load the 110 requirements in their 14 families with the basic or derived flag, the Appendix D mapping to SP 800-53 and ISO/IEC 27001, an owner and an implementation status for each.

System Security Plan

Maintain the 3.12.4 content as records: system boundary, environment of operation, how each requirement is implemented and connections to other systems, with the review date each update requires.

Plan of Action

Track each unimplemented requirement as a 3.12.2 plan of action item with the planned mitigation, owner, milestone date and closure evidence, linked to the requirement it corrects.

Assessment and SPRS Record

Record 3.12.1 assessments, the DoD Assessment Methodology score, the version of SP 800-171 assessed and the SPRS posting date required by DFARS 252.204-7020.

CUI Scope and Security Domain

Document the components designated for CUI and the separation that isolates them under Sec. 1.1, so the requirement set applies only where CUI is processed, stored or transmitted.

Edition Tracking by Contract

Note for each contract whether its solicitation cites Rev. 2 or Rev. 3 under DFARS 252.204-7012(b)(2)(i), and keep the 3.12.3 continuous monitoring evidence for both.

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · FedRAMP Rev. 5 · ISO 27001:2022 · ISO 27002:2022 · NIST CSF 2.0 · NIST 800-53 Rev.5 · PCI DSS 4.0.1 · SOC 2

Official resources

NIST SP 800-171 Rev. 2

Defines requirements for protecting Controlled Unclassified Information in nonfederal systems.

csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST SP 800-171A Assessment Guide

Provides procedures for assessing CUI security requirements in organizations.

csrc.nist.gov/publications/detail/sp/800-171a/final

NIST SP 800-53 Controls Catalog

Outlines security and privacy controls supporting compliance with SP 800-171.

csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST Protecting CUI Overview

Offers an overview of the NIST framework for safeguarding Controlled Unclassified Information.

csrc.nist.gov/projects/protecting-controlled-unclassified-information

Frequently asked questions

Is NIST SP 800-171 Rev. 2 still in use after its withdrawal?

Yes. NIST withdrew Rev. 2 on May 14, 2024 and superseded it with Rev. 3, but 32 CFR 170.14 defines CMMC Level 2 as identical to the requirements in NIST SP 800-171 R2, and DFARS 252.204-7012 applies the SP 800-171 in effect at the time the solicitation is issued or as authorized by the contracting officer. DFARS 252.204-7020 assessments also record the version of SP 800-171 against which the assessment was conducted.

How many requirements does Rev. 2 contain and how are basic and derived requirements different?

Rev. 2 contains 110 security requirements in 14 families (Table 1). Sec. 2.2 explains that basic security requirements come from FIPS 200, the minimum security requirements for federal information and systems, and derived security requirements come from the security controls in the SP 800-53 moderate baseline, tailored to drop what is uniquely federal, not about confidentiality or routinely satisfied without specification. Media Protection shows the pattern: 3.8.1 to 3.8.3 are basic, 3.8.4 to 3.8.9 derived.

 © 2026 SmartSuite Inc. All rights reserved.

What must a system security plan and plan of action contain under Rev. 2?

Requirement 3.12.4 asks organizations to develop, document and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems; footnote 28 says there is no prescribed format. Requirement 3.12.2 asks for plans of action that describe how unimplemented requirements will be met and how planned mitigations will be implemented, which may be combined with the system security plan.

How does CMMC use Rev. 2?

32 CFR 170.14 builds the CMMC Model on this edition: Level 1 uses the 15 requirements of 48 CFR 52.204-21, Level 2 is identical to NIST SP 800-171 R2, and Level 3 adds 24 selected requirements from NIST SP 800-172 of February 2021 with DoD-assigned parameters. Assessment follows SP 800-171A of June 2018. DFARS 252.204-7021 defines the Conditional and Final Level 2 (Self), Level 2 (C3PAO) and Level 3 (DIBCAC) statuses, and the DFARS CMMC rule is effective November 10, 2025 with a three-year phased rollout.

What did the January 28, 2021 errata update change?

NIST describes it as an errata update that includes corrections that do not alter existing or introduce new technical information or requirements. The errata table shows editorial changes in Chapter One: an existing paragraph on the applicability of the requirements and on isolating CUI components in a separate security domain was moved to an earlier section, and the wording of the front matter and Sec. 1.1 was adjusted. The 110 requirements were unchanged.

License included / downloadable: Yes NIST SP 800-171 Rev. 2 is free of charge from NIST, which still hosts the withdrawn PDF, the requirements in CSV and XLSX form and the CUI system security plan and plan of action templates.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-171-rev-2

 © 2026 SmartSuite Inc. All rights reserved.