SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-172 Rev. 3

NIST SP 800-172 Rev. 3 (May 13, 2026) sets 103 enhanced requirements in 17 families to protect CUI tied to critical programs or high value assets; CMMC Level 3 uses 24 from the 2021 edition.



What it is

NIST SP 800-172 Revision 3 is the current edition of NIST's enhanced security requirements for protecting Controlled Unclassified Information (CUI) that is associated with a critical program or high value asset. The requirements are aimed at the advanced persistent threat (APT) to that information. The National Institute of Standards and Technology (NIST) published it on May 13, 2026 and withdrew the February 2, 2021 edition the same day; the jump from a first edition to Revision 3 is a one-time change made so the numbering matches SP 800-171 Rev. 3 (Appendix F). Federal agencies select its requirements for contracts and agreements with nonfederal organizations that handle such CUI, as a supplement to SP 800-171 .

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION Revision 3 (May 13, 2026); supersedes the February 2021 edition
EFFECTIVE May 13, 2026	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: csrc.nist.gov/pubs/sp/800/172/r3/final

Why it matters

- **Built for the APT, not for everyone** Requirements apply only to components that process, store or transmit CUI associated with a critical program or high value asset, or that protect such components, and only when an agency selects them (Section 1.1 and 2.3).
- **Three protection strategies** Penetration-resistant architecture, damage-limiting operations and cyber resiliency run through the requirement set, and Appendix D relates them to five effects on an adversary: redirect, preclude, impede, limit and expose.
- **Every requirement has a source** Appendix C Table 2 gives each requirement a type, E, T or S, and the SP 800-171 requirement or SP 800-53 control it comes from, for example 03.01.01E Dual Authorization from 03.01.02 and AC-03(02).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-172

Enhanced Requirement Register

Record each 03.xx.yyE requirement with its title, type (E, T or S) and source from Appendix C Table 2, and keep the 2021 identifiers beside them for the 24 CMMC Level 3 requirements.

Organization-Defined Parameters

Store the parameter values an agency assigns from Appendix E Table 4, or the DoD values in 32 CFR 170.14(c)(4) Table 1, as fields on the requirement so implementation and assessment read the same value.

Critical Program and Asset Scope

Use Cyber & IT Risk to list the components that process, store, transmit or protect the CUI in scope, and the trust relationships that give a direct attack path, as Section 2.3 asks.

Selection Rationale

Document for each requirement whether it was selected comprehensively or selectively, the dependency that drove it and the risk assessment it rests on, so the Section 2.3 decision is auditable.

Assessment Evidence

Attach evidence to each requirement for SP 800-172A Rev. 3 or, for CMMC Level 3, for the DIBCAC assessment under 32 CFR 170.18, and track findings to closure.

Supplier Flow-Down

Use Third Party Risk Management to record which suppliers receive the selected enhanced requirements by agreement and the status of their implementation.

Common framework mappings

CIS Controls v8.1 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-37 Rev.2 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

NIST SP 800-172 Rev. 3 — Enhanced Security Requirements for Protecting CUI

The May 2026 revision, numbered to match SP 800-171 Rev. 3; supersedes SP 800-172 of February 2021.

csrc.nist.gov/pubs/sp/800/172/r3/final

NIST Special Publication 800-53

Provides a catalog of security and privacy controls for federal information systems and organizations.

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

Frequently asked questions

Which edition of NIST SP 800-172 does CMMC Level 3 use?

The February 2021 edition. 32 CFR 170.14(c)(4) states that the CMMC Level 3 security requirements are selected from NIST SP 800-172 Feb2021, lists the 24 requirements with DoD-assigned organization-defined parameters in Table 1, and 32 CFR 170.18 has DCMA DIBCAC assess them against SP 800-172A Mar2022. NIST withdrew that edition on May 13, 2026 when Revision 3 was published, but the regulation incorporates the 2021 text by reference until it is amended.

How many enhanced security requirements are in Revision 3 and how are they numbered?

Section 3 holds 115 numbered identifiers in the 17 families of Table 1, written as 03.xx.yyE, and 12 of them are marked Withdrawn, which leaves 103 active requirements summarized in Appendix C Table 2. The publication cautions that the sequential numbering does not mean an enhanced requirement such as 03.01.01E enhances the similarly numbered SP 800-171 requirement; the source column in Table 2 shows the real relationship.

What are the three types of enhanced requirement?

Appendix C defines them. Type E enhances a specific SP 800-171 requirement and names it, such as 03.01.01E Dual Authorization from 03.01.02. Type T is sourced to a control tailored out of the SP 800-53B moderate baseline when SP 800-171 was built. Type S does not enhance a specific requirement but strengthens the protection of CUI associated with critical programs or high value assets, and cites its SP 800-53 control, such as 03.01.04E Concurrent Session Control from AC-10.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What changed from the February 2021 edition?

Appendix F lists the changes: introductory material streamlined, requirements made more specific and grouped where possible, outdated and redundant requirements removed, new requirements added from threat intelligence, empirical attack data and the expansion of the security objectives to integrity and availability, titles added, discussion sections restructured, wording aligned with SP 800-53, a new Appendix C summary and Appendix E list of parameters, the old mapping appendix folded into the requirements, and the one-time revision number change to match SP 800-171 Rev. 3.

Does an organization have to implement every enhanced requirement?

No. The abstract says there is no expectation that all of the enhanced security requirements will be selected by federal agencies, and Section 2.3 allows selection comprehensively or selectively, guided by mission and business needs and ongoing risk assessments. An agency can also scope application to the components that handle the critical CUI, protect them or offer a direct attack path to them, and the selected set is then written into the agreement.

License included / downloadable: Yes NIST SP 800-172 Rev. 3 is free of charge from NIST; the PDF is the authoritative text, and the requirements are also issued in the CPRT and OSCAL formats.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-172-enhanced-security-requirements-cui