SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-171 Rev. 3

NIST SP 800-171 specifies security requirements to protect Controlled Unclassified Information (CUI) in nonfederal systems and organizations.

What it is

NIST SP 800-171 Revision 3 is a cybersecurity and data protection framework that provides requirements for safeguarding Controlled Unclassified Information (CUI) in nonfederal systems and organizations. Its primary purpose is to ensure organizations implement security controls that reduce the risk of unauthorized access, disclosure, or loss of sensitive federal information outside government agencies.

Developed and published by the National Institute of Standards and Technology (NIST), this framework is widely adopted by federal contractors, subcontractors, and other entities handling CUI on behalf of the U.S. government. NIST SP 800-171 covers focus areas such as access control, incident response, audit and accountability, risk management, and physical and system security, aligning closely with other NIST standards and federal compliance requirements.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION NIST SP 800-171 Revision 3
EFFECTIVE December 2023	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: https://csrc.nist.gov/pubs/sp/800/171/r3/final

Why it matters

- **Strengthen data protection practices** Implement proven controls that reduce the risk of unauthorized access and disclosure of sensitive government information.
- **Enhance regulatory alignment** Facilitate compliance with federal contracting requirements by aligning cybersecurity practices with government standards and expectations.
- **Increase audit readiness** Establish systematic documentation and monitoring, enabling organizations to demonstrate control effectiveness during audits or assessments.
- **Improve security oversight** Provide clearer roles, responsibilities, and processes for safeguarding CUI, supporting mature cybersecurity management.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-171 Rev. 3

CUI Scope and System Boundary

Define where CUI lives and flows, and maintain a clear, auditable system boundary.

800-171 Requirement Library

Organize requirements by family with owners, procedures, and implementation notes.

SSP and POA&M Management

Maintain SSP content, track gaps in POA&Ms, and manage remediation through closure.

Evidence and Assessment Readiness

Centralize evidence tied to each requirement with timestamps, reviewers, and version history.

Continuous Compliance Cadence

Schedule recurring access reviews, patching, logging, and vulnerability activities with proof.

Executive and Auditor Reporting

Report readiness, open gaps, and remediation progress by system, family, and owner.

Common framework mappings

CIS Controls v8.1 | CMMC 2.0 | DFARS 252.204-7012 | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST SP 800-172 | NIST 800-53 Rev.5

Official resources

NIST SP 800-171 Revision 3

Defines requirements for protecting Controlled Unclassified Information (CUI) in nonfederal systems.

csrc.nist.gov/pubs/sp/800/171/r3/final

NIST Special Publication 800-171 Appendix E

Provides detailed implementation guidance correlated with security controls.

csrc.nist.gov/pubs/sp/800/171/r3/final

NIST SP 800-171A Assessment Procedures

Outlines assessment methods to evaluate the effectiveness of implemented security requirements.

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

NIST Risk Management Framework (RMF)

Outlines the process for risk management in federal information systems.

csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Frequently asked questions

What is NIST SP 800-171 Rev. 3 used for?

NIST SP 800-171 Rev. 3 is used to define security requirements for protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations. It helps ensure that federal contractors, subcontractors, and other entities reduce the risk of unauthorized access, disclosure, or loss of sensitive information when handling CUI on behalf of the U.S. government.

Is NIST SP 800-171 required or mandatory?

NIST SP 800-171 is mandatory for organizations that process, store, or transmit CUI in accordance with federal contracts or regulations, such as the DFARS clause for Department of Defense contractors. While NIST does not provide independent certification, compliance is typically assessed through customer audits, self-assessments, or third-party validation based on contract requirements.

Who does NIST SP 800-171 apply to?

NIST SP 800-171 applies to any nonfederal organization—including contractors, subcontractors, and service providers—that handles CUI received from U.S. federal agencies. This includes organizations supporting government projects where CUI must be protected outside federal information systems.

What are the key control families in NIST SP 800-171 Rev. 3?

NIST SP 800-171 Rev. 3 includes 14 control families, such as Access Control, Audit and Accountability, Incident Response, Media Protection, Physical Protection, Risk Assessment, Security Assessment, System and Communications Protection, and System and Information Integrity. Each family contains specific requirements that collectively secure CUI against common threats.

 - © 2026 SmartSuite Inc. All rights reserved.

How should organizations implement NIST SP 800-171 controls?

Organizations should begin by conducting a gap analysis to assess current security controls against the requirements of NIST SP 800-171. They must then create a System Security Plan (SSP), remediate identified gaps, develop a Plan of Action & Milestones (POA&M), and document evidence of implementation and monitoring for compliance verification.

How does NIST SP 800-171 relate to other NIST frameworks?

NIST SP 800-171 is closely aligned with other frameworks such as NIST SP 800-53 and the NIST Risk Management Framework (RMF). While NIST SP 800-53 is broader and intended for federal systems, SP 800-171 tailors its requirements specifically for nonfederal entities handling CUI and is often used as a minimum standard in federal contracting.

What are the ongoing compliance requirements for NIST SP 800-171?

Organizations must maintain and update their System Security Plan and continuously monitor the effectiveness of implemented controls. They are required to regularly reassess risk, address deficiencies through POA&Ms, retain records of corrective actions, and be prepared for audits or assessments as stipulated by contract terms.

How would SmartSuite support NIST SP 800-171 Rev. 3?

SmartSuite streamlines NIST SP 800-171 compliance by enabling organizations to map and manage control implementation, track remediation tasks, and maintain comprehensive risk and evidence registers. It supports ongoing compliance through real-time dashboards, robust documentation management, and workflow automation for audit readiness and regulatory reporting.

License included / downloadable: Yes NIST SP 800-171 is publicly available through official NIST publications.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-171-rev-3

 © 2026 SmartSuite Inc. All rights reserved.