SmartSuite

Framework / Supply Chain Security / NIST Special Publications

NIST SP 800-171 Rev. 2

NIST SP 800-171 defines security requirements for protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations.

What it is

NIST SP 800-171 Rev. 2 is a cybersecurity framework that helps organizations protect Controlled Unclassified Information (CUI) in nonfederal information systems and environments. Its primary goal is to ensure that organizations handling CUI apply consistent safeguards to reduce the risk of unauthorized access, disclosure, or loss.

Developed and published by the National Institute of Standards and Technology (NIST), the framework is mandated for federal contractors, suppliers, and other nonfederal entities that process or store CUI. NIST SP 800-171 outlines a set of security requirements across 14 control families, including access control, incident response, risk assessment, and system integrity, providing structured guidance for compliance and security oversight.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Guidance	VERSION Rev. 2
EFFECTIVE February 2020	DOMAIN Supply Chain Security	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

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

Why it matters

- **Strengthen cybersecurity governance** Establish structured, repeatable security practices and roles, enabling organizations to manage and oversee CUI protections more effectively.
- **Enhance regulatory alignment** Support compliance with federal acquisition and supply chain requirements, aligning internal security programs with key government regulations and standards.
- **Increase audit readiness** Facilitate thorough documentation and monitoring, allowing organizations to demonstrate control effectiveness and respond efficiently to compliance audits.
- **Support incident response capabilities** Require defined processes for incident detection, reporting, and management, leading to faster and more coordinated responses to security events.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-171 Rev.2

CUI Security Control Library

Organize the 14 NIST 800-171 control families with ownership, scope, and implementation guidance.

System Security Plan Management

Maintain System Security Plans (SSPs) documenting control implementation and system boundaries.

Gap Identification and Remediation Tracking

Identify control gaps, track remediation tasks, and document risk mitigation decisions.

Evidence and Assessment Documentation

Capture assessment artifacts, control test results, and supporting documentation for compliance reviews.

CUI Third-Party Access Monitoring

Monitor third-party access to CUI and ensure vendor compliance with security requirements.

Federal Assessment Readiness Reporting

Provide dashboards showing control coverage, open findings, and readiness for federal assessments.

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

What is NIST SP 800-171 Rev. 2 used for?

NIST SP 800-171 Rev. 2 provides guidelines for protecting Controlled Unclassified Information (CUI) in nonfederal information systems and organizations. It is designed to help federal contractors and other organizations handling CUI ensure adequate security. The framework ensures sensitive data is protected from unauthorized access and disclosure.

Is NIST SP 800-171 Rev. 2 mandatory for organizations?

NIST SP 800-171 Rev. 2 is a requirement for nonfederal organizations that process, store, or transmit CUI on behalf of U.S. federal agencies. It is not a certifiable framework, but compliance is mandatory for organizations subject to federal contracts containing CUI clauses, such as DFARS 252.204-7012.

What types of organizations does NIST SP 800-171 Rev. 2 apply to?

The framework applies to contractors, subcontractors, and other entities outside the federal government that access, process, or store CUI provided by or for federal agencies. This includes organizations within the Defense Industrial Base (DIB) and others working with federal data under relevant contracts.

 © 2026 SmartSuite Inc. All rights reserved.

What are Control Families in NIST SP 800-171 Rev. 2?

NIST SP 800-171 Rev. 2 is structured around 14 control families, such as Access Control, Incident Response, and Physical Protection. Each family includes specific requirements and safeguards to ensure the confidentiality of CUI. Organizations must implement these controls to achieve compliance.

How should organizations approach implementing NIST SP 800-171 Rev. 2?

Implementation begins with scoping CUI environments, conducting a gap analysis, and developing a System Security Plan (SSP) and Plan of Action and Milestones (POA&M). Organizations should prioritize controls based on risk and ensure all requirements are addressed, documenting their compliance efforts and remediation steps.

How does NIST SP 800-171 Rev. 2 relate to other frameworks like CMMC?

NIST SP 800-171 Rev. 2 forms the foundational security requirements for CMMC (Cybersecurity Maturity Model Certification) Level 2. While NIST SP 800-171 Rev. 2 provides the requirements, CMMC adds an assessment and certification layer. Compliance with NIST SP 800-171 Rev. 2 often supports broader regulatory obligations, such as those under DFARS.

What are the ongoing compliance requirements for NIST SP 800-171 Rev. 2?

Organizations must maintain up-to-date System Security Plans, remediate deficiencies via POA&Ms, and continually monitor for risks and control effectiveness. Annual or as-needed self-assessments are crucial to ensure controls remain in place and effective as the threat landscape and systems change.

How would SmartSuite support NIST SP 800-171 Rev. 2?

SmartSuite helps organizations manage NIST SP 800-171 Rev. 2 compliance through centralized risk tracking, control management, and automated evidence collection. The platform supports audit readiness with real-time reporting, streamlined documentation, and workflow tools that enable teams to monitor implementation status, track remediation actions, and demonstrate compliance to auditors.

License included / downloadable: Yes NIST SP 800-171 Rev. 2 is publicly available for free from NIST's website. License included with platform

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

 © 2026 SmartSuite Inc. All rights reserved.