SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-172 (2020)

NIST SP 800-172 provides enhanced security requirements to protect Controlled Unclassified Information against advanced threats.

What it is

NIST SP 800-172 is a cybersecurity framework that helps organizations implement enhanced security requirements to protect Controlled Unclassified Information (CUI) in nonfederal systems and environments. The framework focuses on strengthening the confidentiality and integrity of sensitive information, particularly when facing advanced persistent threats.

Published by the National Institute of Standards and Technology (NIST), NIST SP 800-172 supplements the baseline controls in NIST SP 800-171 and is primarily used by federal contractors, subcontractors, and organizations handling CUI. Its requirements focus on advanced cybersecurity controls, continuous monitoring, incident response, and risk management to ensure robust safeguards for federal information assets.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION Rev. 1
EFFECTIVE February 2021	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Very High		

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

Why it matters

- **Strengthen advanced threat defense** Improve the ability to detect and counter sophisticated cyberattacks targeting CUI within federal contractor systems.
- **Enhance data protection practices** Reduce the likelihood of unauthorized access, exfiltration, or compromise of sensitive information critical to national interests.
- **Improve compliance with federal requirements** Support fulfillment of stringent U.S. government mandates for CUI protection to maintain eligibility for federal contracts.
- **Increase incident response effectiveness** Enable earlier detection, analysis, and containment of security incidents through enhanced monitoring and response capabilities.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-172

Enhanced CUI Control Library

Organize NIST SP 800-172 enhanced security requirements mapped to existing NIST SP 800-171 control families.

Enhanced Safeguard Implementation Tracking

Track implementation of safeguards designed to defend against advanced persistent threats targeting CUI.

Security Architecture and System Hardening

Manage configuration baselines, system hardening practices, and architectural safeguards protecting sensitive systems.

Continuous Monitoring and Incident Response

Coordinate monitoring, detection, and response activities across systems handling Controlled Unclassified Information.

CUI Third-Party and Environment Monitoring

Monitor third-party access and dependencies affecting the protection of CUI environments.

Federal Cybersecurity Review Readiness Reporting

Provide dashboards showing control coverage, open risks, and readiness for federal cybersecurity reviews.

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 Enhanced Security Requirements

Defines enhanced security requirements for protecting Controlled Unclassified Information in nonfederal systems.

csrc.nist.gov/publications/detail/sp/800-172/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

What is NIST SP 800-172 used for?

NIST SP 800-172 provides enhanced security requirements to protect Controlled Unclassified Information (CUI) in non-federal systems and organizations, particularly from advanced persistent threats (APTs). It is designed to supplement NIST SP 800-171 by raising the security baseline for organizations handling CUI that may be targeted by sophisticated adversaries.

Is NIST SP 800-172 mandatory or certifiable?

NIST SP 800-172 is not a certifiable standard, nor is it universally mandatory. Its application is determined by specific contract clauses, federal agency requirements, or regulatory actions within supply chains, commonly those associated with the Department of Defense or federal contractors.

What types of organizations must comply with NIST SP 800-172?

Organizations that process, store, or transmit CUI on behalf of U.S. federal agencies and are deemed at increased risk from advanced persistent threats may be required to implement NIST SP 800-172. Applicability is typically driven by contract requirements or organizational risk analysis.

What are the key concepts or requirements of NIST SP 800-172?

Key concepts in NIST SP 800-172 include enhanced security controls across areas such as asset management, privileged operations, incident response, and continuous monitoring. The requirements expand on existing controls from SP 800-171 by introducing advanced techniques like deception, isolation, and robust auditing to counter advanced threats.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How should organizations implement NIST SP 800-172 controls?

Implementation should begin with a gap assessment against current NIST SP 800-171 compliance, followed by integration of the additional controls specified in SP 800-172. Organizations should use a risk-based approach, document their implementation status, and ensure that enhanced security controls are operational and effective.

How does NIST SP 800-172 relate to other NIST frameworks?

NIST SP 800-172 is intended as a supplement to NIST SP 800-171, specifically addressing increased threats to CUI. It does not replace SP 800-171 but builds upon it, and can complement other frameworks such as the NIST Cybersecurity Framework when managing broader security programs.

What are ongoing compliance requirements for NIST SP 800-172?

Ongoing compliance requires regular reassessment of enhanced controls, continuous monitoring for emerging threats, and updating documentation and evidence to demonstrate sustained alignment with NIST SP 800-172 requirements. Audits and internal reviews are key to ensuring continued effectiveness.

How would SmartSuite support NIST SP 800-172?

SmartSuite helps organizations manage NIST SP 800-172 by enabling risk tracking, mapping and management of enhanced controls, and organizing evidence collections to support compliance activities. The platform facilitates audit readiness with robust documentation, workflow automation, and real-time reporting to support continuous monitoring and regulatory oversight.

License included / downloadable: Yes NIST SP 800-172 is publicly available for free from NIST's publications website. License included with platform

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