SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information (June 2018)

NIST SP 800-171A (June 2018) is the withdrawn edition of the CUI assessment procedures, superseded by Rev. 3 in May 2024 but still the edition CMMC and DFARS assessments incorporate.



What it is

NIST SP 800-171A (June 2018) is the withdrawn first edition of NIST's assessment procedures for the Controlled Unclassified Information (CUI) security requirements in SP 800-171: NIST withdrew it on May 14, 2024 and superseded it with SP 800-171A Rev. 3 . It is still the edition the Department of Defense incorporates by reference. 32 CFR 170.14(d) prescribes NIST SP 800-171A Jun2018 for assessing the CMMC security requirements, 32 CFR 170.16 and 170.17 require Level 2 self-assessments and C3PAO certification assessments to follow it, 32 CFR 170.18 applies it to Level 3 assessments by DCMA DIBCAC, and DFARS 252.204-7020 defines a High Assessment as one conducted by Government personnel using NIST SP 800-171A.

The National Institute of Standards and Technology (NIST) published the edition on June 13, 2018; its authors are Ron Ross, Kelley Dempsey and Victoria Pillitteri. The abstract describes assessment procedures and a methodology that federal and nonfederal organizations can use to assess the CUI security requirements in SP 800-171.

At a glance

PUBLISHER
National Institute of Standards and Technology (NIST)

TYPE
Assessment / Maturity Model

VERSION
June 2018 edition; withdrawn May 14, 2024

EFFECTIVE
June 13, 2018

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/800/171/a/final

Why it matters

- **Traceable determinations** Every assessment objective is a set of determination statements tied to the requirement text, so findings trace to the requirement and the evidence that supports them (Section 2.1).
- **Three methods, four kinds of object** Examine, interview and test are applied to specifications, mechanisms, activities and individuals, which lets an organization pick the mix that gives sufficient confidence at the lowest cost (Section 2.1).
- **Adjustable rigor** Depth and coverage attributes run from basic to focused to comprehensive, each value building on the one before, so the same procedure serves a light self-check or a full certification assessment (Appendix D).
- **An assurance case, not a checklist** Evidence from self-assessments, third-party product testing and life cycle artifacts is organized into an argument that the requirements are met (Section 2.2).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-171A (2018)

Determination Statement Register

Record each requirement with its determination statements, for example 3.1.1[a] through 3.1.1[f], as linked records in Compliance Management so a finding is made per statement (Section 2.1).

Methods and Objects per Procedure

Capture which examine, interview and test methods and which specifications, mechanisms, activities and individuals were selected for each procedure, with the depth and coverage value chosen (Appendix D).

Evidence for the Assurance Case

Attach policies, system security plan extracts, configuration records and test results to the statements they support so the Section 2.2 assurance case is assembled from the records themselves.

Assessment Plans and Reviews

Use Internal Audit Management to schedule self-assessments, C3PAO certification assessments and DIBCAC High Assessments, assign assessors and track fieldwork to completion.

Open Findings and POA&M Items

Track each determination not yet met in Cyber & IT Risk with an owner and due date, and record the POA&M closeout self-assessment that 32 CFR 170.16 requires within 180 days.

SPRS Score Record

Keep the summary level score, the assessment date and the SP 800-171 version assessed, the three items DFARS 252.204-7020 posts to SPRS, with each submission as a record for reporting.

Common framework mappings

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

Official resources

NIST SP 800-171A Document

Provides assessment procedures for security requirements of Controlled Unclassified Information.

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

NIST SP 800-171 Revision 2

Outlines the requirements for protecting Controlled Unclassified Information in non-federal systems.

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

Frequently asked questions

Why does NIST SP 800-171A (2018) still matter after NIST withdrew it?

NIST withdrew the June 2018 edition on May 14, 2024, when SP 800-171A Rev. 3 superseded it, but the DoD rules still name it. 32 CFR 170.14(d) says assessment of the CMMC security requirements is prescribed by NIST SP 800-171A Jun2018, 32 CFR 170.16 and 170.17 require Level 2 self-assessments and C3PAO certification assessments to follow it, 32 CFR 170.18 applies it with SP 800-172A Mar2022 at Level 3, and DFARS 252.204-7020 defines a High Assessment as one conducted by Government personnel using NIST SP 800-171A.

What is inside an SP 800-171A assessment procedure?

Each procedure quotes the security requirement, states an assessment objective as a list of determination statements, and lists potential assessment methods and objects (Section 2.1). For requirement 3.1.1 the objective runs from 3.1.1[a] authorized users are identified to 3.1.1[f] system access is limited to authorized devices, followed by Examine, Interview and Test lists that name the documents, roles and mechanisms an assessor can select from.

What do examine, interview and test mean, and what are depth and coverage?

Examine is reviewing, inspecting, observing, studying or analyzing assessment objects; interview is holding discussions with individuals or groups; test is exercising activities or mechanisms under specified conditions to compare actual with expected behavior (Section 2.1). Depth sets the rigor and level of detail and coverage sets the scope, each with the values basic, focused and comprehensive, and Appendix D Tables D-1 through D-3 describe what each value adds.

 © 2026 SmartSuite Inc. All rights reserved.

Who can conduct an assessment under SP 800-171A?

The abstract allows self-assessments, independent third-party assessments and government-sponsored assessments, and Section 2.2 says assessments can be conducted by system developers, system integrators, auditors, system owners or the organization's security staff. Under DFARS 252.204-7020 a Basic Assessment is a contractor self-assessment, while Medium and High Assessments are conducted by the Government, the High Assessment using SP 800-171A.

Which revision of SP 800-171 do the 2018 procedures assess?

Appendix A cites SP 800-171 Revision 1 of December 2016, the edition in force when the procedures were written, and the same fourteen-family structure carried into Revision 2 (February 2020), which 32 CFR 170.14 incorporates for CMMC Level 2. The 97 requirements of SP 800-171 Rev. 3 use a different numbering with organization-defined parameters and are assessed with SP 800-171A Rev. 3, not this edition.

License included / downloadable: Yes NIST SP 800-171A is free of charge from NIST; the PDF is the authoritative text, and the CSRC record also offers the procedures as CSV and XLSX files.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-171a-assessing-security-requirements-controlled

 © 2026 SmartSuite Inc. All rights reserved.