

Protecting Controlled Unclassified Information

Project Update

Agenda

<https://csrc.nist.gov/projects/protecting-CUI>



Protecting CUI Series at a Glance

Change Overview: SP 800-171 Rev 3 and SP 800-171A Rev 3

Looking Ahead for the CUI Series

Contact Information and Q&A

Protecting CUI Series at a Glance



**SECURITY
REQUIREMENTS**
FOR PROTECTING THE
CONFIDENTIALITY OF CUI



**NONFEDERAL
SYSTEMS &
ORGANIZATIONS**



PROCESSING, STORING,
OR TRANSMITTING
CUI



TAILORED FROM THE
SP 800-53B
MODERATE
BASELINE



**INTERNATIONAL
USE & IMPACT**



NEW & IMPROVED
**SUPPLEMENTAL
RESOURCES**



ASSESSMENT
PROCEDURES
SP 800-171A



ENHANCED SECURITY
REQUIREMENTS
SP 800-172

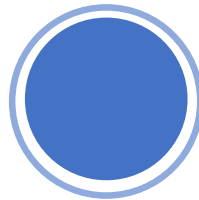


ASSESSMENT PROCEDURES
FOR ENHANCED SECURITY
REQUIREMENTS
SP 800-172A

Change Overview: SP 800-171 Rev 3

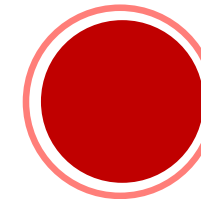
Improved Readability

- Streamlined “Introduction” and “The Fundamentals” sections
- Added Appendix for ODPs



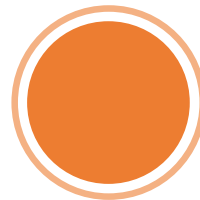
Updated Tailoring Criteria

- Added new tailoring categories: NA and ORC
- Eliminated NFO tailoring category
- Recategorized selected controls from SP 800-53B moderate baseline



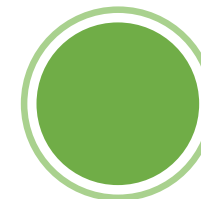
Updated Security Requirements

- Added, deleted, or changed security requirements to reflect controls & families in SP 800-53 Rev 5 and moderate baseline in 800-53B
- Eliminated distinction between basic and derived requirements
- Increased specificity and grouped requirements
- Introduced organization-defined parameters (ODPs)
- Removed outdated and redundant requirements
- Further tailored discussions to focus on CUI

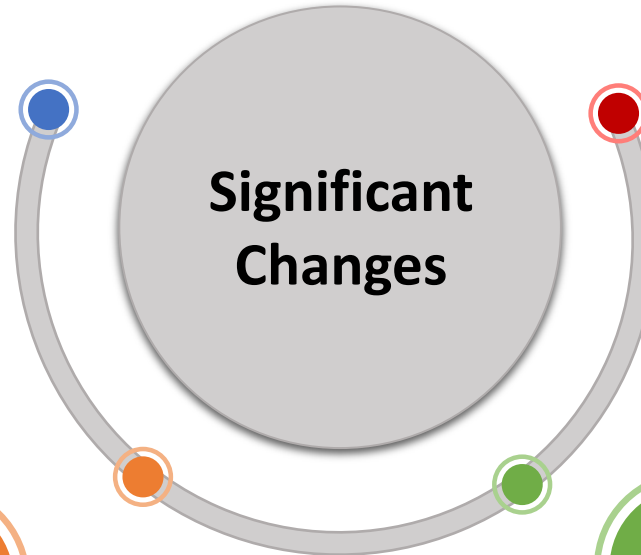


Added Supplemental Resources

- Developed CUI Overlay using tailored controls in SP 800-53 Rev 5
- Created transition mapping tables and analysis of changes between SP 800-171 Rev 2 and SP 800-171 Rev 3
- Developed updated FAQ
- Concurrently issued updated security requirements through Cybersecurity and Privacy Reference Tool



Significant Changes



SP 800-171 Rev 2 withdrawn: May 14, 2024

Updated Security Requirements

- ✓ Updated security requirement **structure**; added leading 0s to requirements
- ✓ Included **organization-defined parameters** (ODP) in certain requirements
 - ODPs can use assignment and/or selection operations
- ✓ Updated **discussion sections** to focus on CUI
- ✓ Included direct link to **source** SP 800-53 controls

New requirement structure

03.13.11 Cryptographic Protection

Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].

New ODP

DISCUSSION

Cryptography is implemented in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. FIPS-validated cryptography is recommended for the protection of CUI.

REFERENCES

Source Control: [SC-13](#)

SP 800-53 Source

Supporting Publications: FIPS 140-3 [38]

Updated Tailoring Criteria



Tailoring Symbol	Tailoring Criteria	SP 800-53 Rev 4 Moderate Baseline → SP 800-171 Rev 2	SP 800-53 Rev 5 / 800-53B Moderate Baseline → SP 800-171 Rev 3
NCO	Not directly related to protecting the confidentiality of CUI	58	96
NFO	Expected to be implemented by nonfederal organizations without specification	61	0
FED	Primarily the responsibility of the Federal Government	18	22
CUI	Directly related to protecting the confidentiality of CUI	125	156
ORC	The outcome of the control relating to the protection of confidentiality of CUI is adequately covered by other related controls.	New in FPD SP 800-171 Rev 3	13
NA	Not Applicable	New in IDP SP 800-171 Rev 3	50
[SP 800-53] Moderate Baseline Security Controls		262	287

- ✓ New tailoring categories: NA and ORC
- ✓ Recategorized selected controls from SP 800-53B moderate baseline
- ✓ Removed tailoring category: NFO
- ✓ Overall, fewer security requirements

Added Supplemental Resources



- ✓ FAQ
- ✓ Transition Mapping Tables / Change Analysis
- ✓ Prototype CUI Overlay
- ✓ Link to CPRT Dataset



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

An official website of the United States government [Here's how you know](#)

NIST Information Technology Laboratory **COMPUTER SECURITY RESOURCE CENTER** Search CSRC CSRC MENU

PUBLICATIONS

NIST SP 800-171 Rev. 3

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

f t in ✉

Date Published: May 2024

Supersedes: [SP 800-171 Rev. 2 \(01/28/2021\)](#)

Author(s)
Ron Ross (NIST), Victoria Pillitteri (NIST)

Abstract
The protection of Controlled Unclassified Information (CUI) is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides federal agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations. The requirements apply to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This publication can be used in

DOCUMENT

Publication:
<https://doi.org/10.6028/NIST.SP.800-171r3>
Download URL

Supplemental Material:
[Change analysis \(Rev. 2 to Rev. 3\) \(xlsx\)](#)
[CUI Overlay \(xlsx\)](#)
[FAQ \(pdf\)](#)
[800-171r3 Dataset on CPRT](#)
[Protecting CUI in Nonfederal Systems and Organizations](#)
[NIST news article](#)

Publication Parts:
[SP 800-171A Rev. 3](#)

Added Supplemental Resources



Prototype CUI Overlay

Unique Sort ID (800-53r5)	SP 800-53 Rev 5 Control & Control Enhancement	Tailoring Decision	Unique Sort ID (800-171r3)	SP 800-171 Rev 3 Security Requirement	Additional Tailoring
IA-12-03-00	IA-12(03) Identity Proofing Identity Evidence Validation and Verification	FED		—	
IA-12-03-01	Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].	FED		—	
IA-12-05-00	IA-12(05) Identity Proofing Address Confirmation	FED		—	
IA-12-05-01	Require that a [Selection: registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.	FED		—	
IR-01-00-02	IR-01 Policy and Procedures	CUI	03-15-01:	03.15.01 Policy and Procedures	
IR-01-00-03	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:	CUI	03-15-01a.	03.15.01.a. Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.	Addresses all policy (instead of only incident response policy) Removed ODP to assign "personnel or roles"
IR-01-00-04	1. [Selection (one or more): organization-level; mission/business process-level; system-level] incident response policy that:	CUI	03-15-01a.	03.15.01.a. D	select one or more "organization-business process-level; system level"
IR-01-00-05	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	NCO		—	
IR-01-00-06	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	NCO		—	
IR-01-00-07	2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;	CUI	03-15-01a.	03.15.01.a. Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.	Addresses all procedures (instead of only incident response procedures)
IR-01-00-08	b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and	NCO		—	
IR-01-00-09	c. Review and update the current incident response:	CUI	03-15-01b.	03.15.01b. Review and update policies and procedures periodically.	Addresses update of all policy and procedures (instead of only incident response)
IR-01-00-10	1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and	CUI	03-15-01b.	03.15.01b. Review and update policies and procedures periodically.	Removed ODPs to assign "frequency" and "events"
IR-01-00-11	2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	CUI	03-15-01b.	03.15.01b. Review and update policies and procedures periodically.	Removed ODPs to assign "frequency" and "events"

✓ Filter and Sort by Column

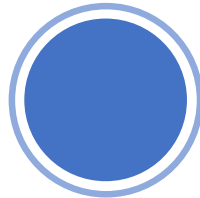
✓ Tailoring decisions at control- and requirement—item level

Change Overview: SP 800-171A Rev 3



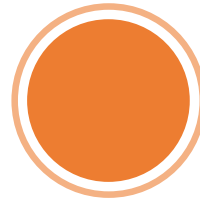
Improved Readability

- Updated “Introduction” and “The Fundamentals” sections
- Made version number update to align with SP 800-171 Rev 3
- Added Appendix for ODPs



Updated Assessment Procedures

- Restructured assessment procedure syntax to align with SP 800-53A Rev 5
- Included ODPs (consistent with SP 800-171 security requirements)
- Provided additional guidance on assessment methodology



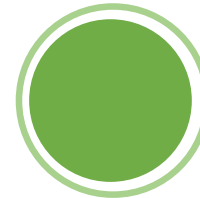
Significant Changes



SP 800-171A withdrawn: May 14, 2024

Added Supplemental Resources

- Delivered SP 800-171A assessment procedures in spreadsheet format
- Concurrently issued updated assessment procedures through Cybersecurity and Privacy Reference Tool



Updated Assessment Procedures

SP 800-171

03.01.10 Device Lock

- a. Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended].
- b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.
- c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

DISCUSSION

Device locks are temporary actions taken to prevent access to the system when users depart from the immediate vicinity of the system but do not want to log out due to the temporary nature of their absences. Device locks can be implemented at the operating system level or application level. User-initiated device locking is behavior- or policy-based and requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of the system (e.g., when organizations require users to log out at the end of workdays). Publicly viewable images can include static or dynamic images, such as patterns used with screen savers, solid colors, photographic images, a clock, a battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

REFERENCES

Source Controls: [AC-11](#), [AC-11\(01\)](#)

Supporting Publications: None

03.01.10 Device Lock

SP 800-171A

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.10.ODP[01]: one or more of the following PARAMETER VALUES are selected: {a device lock is initiated after <A.03.01.10.ODP[02]: time period> of inactivity; the user is required to initiate a device lock before leaving the system unattended}.

A.03.01.10.ODP[02]: the time period of inactivity after which a device lock is initiated is defined (if selected).

A.03.01.10.a: access to the system is prevented by <A.03.01.10.ODP[01]: SELECTED PARAMETER VALUES>.

A.03.01.10.b: the device lock is retained until the user reestablishes access using established identification and authentication procedures.

A.03.01.10.c: information previously visible on the display is concealed via device lock with a publicly viewable image.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for session lock... other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for cryptographic key establishment and/or management; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for implementing the access control policy for session lock; session lock mechanisms]

REFERENCES

Source Assessment Procedures: [AC-11](#), [AC-11\(01\)](#)

SP 800-171 and SP 800-171A Datasets



An official website of the United States government [Here's how you know](#)

NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Search CSRC **CSRC MENU**

PROJECTS CYBERSECURITY AND PRIVACY REFERENCE TOOL

Cybersecurity and Privacy Reference Tool CPRT



CPRT Catalog

The Cybersecurity and Privacy Reference Tool (CPRT) highlights the reference data from NIST publications without the search, and export the data in a structured format that is human- and machine-consumable. For example, you can use the reference data for each publication in MS Excel or JSON.

We will be adding more NIST datasets to this catalog. See the [CPRT Roadmap](#) for future planned functionalities.

Reference Dataset	Publication Title
SP 800-171 Rev 3	Protecting Controlled Unclassified Information in Nonfederal Systems
SP 800-171A Rev 3	Assessing Enhanced Security Requirements for Controlled Unclassified

An official website of the United States government [Here's how you know](#)

NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Search CSRC **CSRC MENU**

PROJECTS CYBERSECURITY AND PRIVACY REFERENCE TOOL

Cybersecurity and Privacy Reference Tool CPRT



Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, 3.0.0

CPRT / SP 800-171

Families

- [03.01](#) Access Control
- [03.02](#) Awareness and Training
- [03.03](#) Audit and Accountability
- [03.04](#) Configuration Management
- [03.05](#) Identification and Authentication
- [03.06](#) Incident Response
- [03.07](#) Maintenance
- [03.08](#) Media Protection
- [03.09](#) Personnel Security
- [03.10](#) Physical Protection

An official website of the United States government [Here's how you know](#)

NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Search CSRC **CSRC MENU**

PROJECTS CYBERSECURITY AND PRIVACY REFERENCE TOOL

Cybersecurity and Privacy Reference Tool CPRT



Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, 3.0.0

CPRT / SP 800-171 / 03.08 / 03.08.01

Export - ⓘ

Media Protection (03.08)

03.08.01: Media Storage

[Show all 03.08.01 References](#) ⓘ

[SP 800-171 Security Requirement](#) [SP 800-171A Assessment Procedure](#) [Both](#)

Physically control and securely store system media that contain CUI.

Discussion

System media include digital and non-digital media. Digital media include diskettes, flash drives, magnetic tapes, external or removable solid state or magnetic drives, compact discs, and digital versatile discs. Non-digital media include paper and microfilm. Physically controlling stored media includes conducting inventories, establishing procedures to allow individuals to check out and return media to libraries, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. Controlled areas provide physical and procedural controls to meet the requirements established for protecting information and systems. Sanitization techniques (e.g., destroying, cryptographically erasing, clearing, and purging) prevent the disclosure of CUI to unauthorized individuals. The sanitization process removes CUI from media such that the information cannot be retrieved or reconstructed.

References

Source Controls: [3.8.1 MP-04](#)

Supporting Publications: [SP 800-111](#) [SP 800-88](#)



<https://csrc.nist.gov/Projects/cprt/catalog#/cprt/home>

Looking Ahead for the CUI Series

- ✓ **Revise SP 800-172 and SP 800-172A**
- ✓ **Follow the same development strategy as SP 800-171, Revision 3**
- ✓ **Projected development schedule**
 - NISTSP 800-172, R1 (Initial Public Draft) – CY2024
 - NISTSP 800-172, R1 (Final Public Draft) – CY2025
 - NISTSP 800-172A, R1 (Initial Public Draft) – CY2025
 - NISTSP 800-172, R1 (Final) – CY2025
 - NISTSP 800-172A, R1 (Final) – CY2025



STAY IN TOUCH

CONTACT US



<https://csrc.nist.gov/Projects/protecting-CUI>



sec-cert@nist.gov



[@NISTcyber](https://twitter.com/NISTcyber)