Protecting Controlled Unclassified Information: What’s New in Draft SP 800-171 Revision 3

Victoria Yan Pillitteri
victoria.yan@nist.gov
Agenda

NIST Special Publication (SP) 800-171 at a Glance

Change Overview: Draft SP 800-171 Revision 3

Looking Ahead for the CUI Series

Contact Information and Q&A
SP 800-171 at a Glance

SECURITY REQUIREMENTS FOR PROTECTING CONFIDENTIALITY OF CUI

NONFEDERAL SYSTEMS & ORGANIZATIONS

PROCESS, STORE, OR TRANSMIT CUI, OR PROVIDE PROTECTION FOR SUCH COMPONENTS

DRAFT REV 3 RELEASED 10 MAY COMMENT THRU 14 JULY

INTERNATIONAL USE AND IMPACT

NEW & IMPROVED SUPPLEMENTAL RESOURCES

ASSESSMENT PROCEDURES SP 800-171A

ENHANCED SECURITY REQUIREMENTS SP 800-172

ENHANCED SECURITY REQ'S ASSESSMENT PROCEDURES 800-172A
Change Overview: Draft SP 800-171 Rev 3

**Improved Readability**
- streamlined “Introduction” and “The Fundamentals”

**Updated Security Requirements**
- to reflect controls & families in SP 800-53 Rev 5 and SP 800-53B Moderate Baseline
- eliminated distinction between basic & derived requirements
- increased specificity & grouped requirements
- introduced organization-defined parameters (ODPs)
- removed outdated & redundant requirements

**Updated Tailoring Criteria**
- added new tailoring category, NA
- recategorized selected controls from SP 800-53B Moderate Baseline

**Added Supplemental Resources**
- *prototype* CUI Overlay using tailored controls in SP 800-53 Rev 5
- transition mapping tables & analysis of changes between SP 800-171 Rev 2 and draft Rev 3
- FAQ
### Draft SP 800-171 Rev 3 Security Requirement Families

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Maintenance</th>
<th>Security Assessment &amp; Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Added: 1, Withdrawn: 5)</td>
<td>(Added: 0, Withdrawn: 3)</td>
<td>(Added: 3, Withdrawn: 1)</td>
</tr>
<tr>
<td>Awareness &amp; Training</td>
<td>Media Protection</td>
<td>System &amp; Communications Protection</td>
</tr>
<tr>
<td>(Added: 0, Withdrawn: 0)</td>
<td>(Added: 0, Withdrawn: 2)</td>
<td>(Added: 2, Withdrawn: 4)</td>
</tr>
<tr>
<td>Audit &amp; Accountability</td>
<td>Personnel Security</td>
<td>System &amp; Information Integrity</td>
</tr>
<tr>
<td>(Added: 0, Withdrawn: 0)</td>
<td>(Added: 0, Withdrawn: 0)</td>
<td>(Added: 1, Withdrawn: 3)</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Physical Protection</td>
<td></td>
</tr>
<tr>
<td>(Added: 0, Withdrawn: 1)</td>
<td>(Added: 2, Withdrawn: 3)</td>
<td></td>
</tr>
<tr>
<td>Identification &amp; Authentication</td>
<td>Risk Assessment</td>
<td>New Families</td>
</tr>
<tr>
<td>(Added: 1, Withdrawn: 4)</td>
<td>(Added: 1, Withdrawn: 1)</td>
<td>Planning</td>
</tr>
<tr>
<td>(Added: 4)</td>
<td></td>
<td>(Added: 4)</td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
<td>System &amp; Services Acquisition</td>
</tr>
<tr>
<td>(Added: 0, Withdrawn: 0)</td>
<td></td>
<td>(Added: 2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Added: 4)</td>
</tr>
</tbody>
</table>

- ✔️ Aligned with **SP 800-53 Rev 5** and **SP 800-53B Moderate Baseline**
- ✔️ No change in **total number** of requirements (still 110)
Updated Security Requirements

✓ Updated security requirement structure
✓ Organization-defined parameters (ODP) included in some requirements
  • ODP include assignment & selection operations
✓ Direct link to source SP 800-53 control(s)

3.15.3. Rules of Behavior
a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for handling CUI and system usage.
b. Review and update the rules of behavior [Assignment: organization-defined frequency].

DISCUSSION
Rules of behavior represent a type of access agreement for system users. Organizations consider rules of behavior for the handling of CUI based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users.

REFERENCES
Source Controls: PL-4
Supporting Publications: SP 800-18 [67]
# Updated Tailoring Criteria

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NCO</td>
<td>Not directly related to protecting the confidentiality of CUI</td>
<td>58</td>
<td>81</td>
</tr>
<tr>
<td>NFO</td>
<td>Expected to be implemented by nonfederal organizations without specification</td>
<td>61</td>
<td>17</td>
</tr>
<tr>
<td>FED</td>
<td>Primarily the responsibility of the Federal Government</td>
<td>18</td>
<td>21</td>
</tr>
<tr>
<td>CUI</td>
<td>Directly related to protecting the confidentiality of CUI</td>
<td>125</td>
<td>168</td>
</tr>
<tr>
<td>NA</td>
<td>Not Applicable</td>
<td>New in IDP SP 800-171 Rev 3</td>
<td>50</td>
</tr>
</tbody>
</table>

**Moderate Baseline Security Controls by SP 800-53 Revision**

- New tailoring category, NA
- Recategorized selected controls from SP 800-53B moderate baseline
<table>
<thead>
<tr>
<th>Unique Sort ID</th>
<th>SP 800-53 Rev 5 Control &amp; Control Enhancement</th>
<th>Tailoring Decision</th>
<th>Unique Sort ID</th>
<th>SP 800-171 Rev 3 Security Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-01-00-00</td>
<td>AC-1 Policy and Procedures</td>
<td>CUI</td>
<td>3.15-01</td>
<td>3.15.1 Policy and Procedures</td>
</tr>
<tr>
<td>AC-01-00-01</td>
<td>a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:</td>
<td>CUI</td>
<td>3.15-01a.</td>
<td>3.15.1a Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements.</td>
</tr>
<tr>
<td>AC-01-00-02</td>
<td>1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that:</td>
<td>CUI</td>
<td>3.15-01a.</td>
<td>3.15.1a Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements.</td>
</tr>
<tr>
<td>AC-01-00-03</td>
<td>(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and</td>
<td>NCO</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>AC-01-00-04</td>
<td>(b) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and</td>
<td>NCO</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>AC-01-00-05</td>
<td>2. Procedures to facilitate the implementation of the access control policy and the associated access controls;</td>
<td>CUI</td>
<td>3.15-01a.</td>
<td>3.15.1a Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements.</td>
</tr>
<tr>
<td>AC-01-00-06</td>
<td>b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and</td>
<td>NCO</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>AC-01-00-07</td>
<td>c. Review and update the current access control policy</td>
<td>CUI</td>
<td>3.15-01b.</td>
<td>3.15.1b Review and update policies and procedures [Assignment: organization-defined frequency].</td>
</tr>
<tr>
<td>AC-01-00-08</td>
<td>1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and</td>
<td>CUI</td>
<td>3.15-01b.</td>
<td>3.15.1b Review and update policies and procedures [Assignment: organization-defined frequency].</td>
</tr>
<tr>
<td>AC-01-00-09</td>
<td>2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].</td>
<td>CUI</td>
<td>3.15-01b.</td>
<td>3.15.1b Review and update policies and procedures [Assignment: organization-defined frequency].</td>
</tr>
</tbody>
</table>
Added Supplemental Resources

- FAQ
- Transition Mapping Tables & Change Analysis
- Prototype CUI Overlay

## Added Supplemental Resources

### Change Analysis SP 800-171 Rev 2 to IPD Rev 3

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>R2-03-01-01</td>
<td>3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).</td>
<td>Basic</td>
<td>R3-03-01-01</td>
<td>3.1.1</td>
<td>Account Management</td>
<td>a. Define and document the types of system accounts allowed and prohibited.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>R2-03-01-02</td>
<td>3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.</td>
<td>Basic</td>
<td>R3-03-01-02</td>
<td>3.1.2</td>
<td>Access Enforcement</td>
<td>Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>R2-03-01-03</td>
<td>3.1.3 Control the flow of CUI in accordance with approved authorizations.</td>
<td>Derived</td>
<td>R3-03-01-03</td>
<td>3.1.3</td>
<td>Flow Enforcement</td>
<td>Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>R2-03-01-04</td>
<td>3.1.4 Separate the duties of individuals to reduce the risk of malfeasance activity without collusion.</td>
<td>Derived</td>
<td>R3-03-01-04</td>
<td>3.1.4</td>
<td>Separation of Duties</td>
<td>a. Identify the duties of individuals requiring separation. b. Define system access authorizations to support separation of duties.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Prototype CUI Overlay

### Unique Sort ID (800-53r5) | Tailoring Decision | Unique Sort ID (IPD 800-17r) | Additional Tailoring
--- | --- | --- | ---
AC-01-00-00 | **AC-1 Policy and Procedures** | CUI | **03-15-01:** 3.15.1 Policy and Procedures

**a.** Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

- **CUI** 03-15-01a. 3.15.1a. Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements.
- **NCO**

**b.** Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

- **CUI** 03-15-01a. 3.15.1a. Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements.
- **NCO**

**c.** Review and update the current access control:

- **CUI** 03-15-01b. 3.15.1b. Review and update policies and procedures [Assignment: organization-defined frequency].
- **NCO**

**1.** Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

- **CUI** 03-15-01b. 3.15.1b. Review and update policies and procedures [Assignment: organization-defined frequency].
- **NCO**

**2.** Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events];

- **CUI** 03-15-01b. 3.15.1b. Review and update policies and procedures [Assignment: organization-defined frequency].
- **NCO**

**AC-02-00-00 | **AC-2 Account Management** | CUI | **03-01-01:** 3.1.1 Account Management

**a.** Define and document the types of accounts allowed and specifically prohibited for use within the system; and

- **CUI** 03-01-01a. 3.1.1a. Define and document the types of system accounts allowed and prohibited.
- **NFO**

**b.** Assign account managers;

- **NFO**

**c.** Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;

- **NFO**

---

**Filter and Sort by Column**

**Tailoring decisions at control- and requirement—item level**
Looking Ahead for the CUI Series

Phase 1
- NIST issues pre-call for comments on the CUI Series
- Begin NIST Protecting CUI Project website redesign

Phase 2
- Revise SP 800-171; issue draft(s) for public comment
- Finalize SP 800-171 Rev 3

Phase 3
- Revise SP 800-171A; issue draft(s) for public comment
- Finalize SP 800-171A Rev 1

Phase 4
- Revise SP 800-172 and SP 800-172A; issue draft(s) for public comment
- Finalize SP 800-172 Rev 1 and SP 800-172A Rev 1

Ongoing
- Stakeholder outreach and engagement for awareness and continuous improvement to the CUI Series

We Are Here!

July 2022
The public comment period is open now through July 14, 2023

NIST is specifically interested in comments, feedback, and recommendations for the following topics:

- Re-categorized controls (e.g., controls formerly categorized as NFO)
- Inclusion of organization-defined parameters (ODP)
- Prototype CUI overlay

Questions or comments? Email: 800-171comments@list.nist.gov.

Comments received in response to this request will be posted on the Protecting CUI project site after the due date. Submitters’ names and affiliations (when provided) will be included, while contact information will be removed.
Webinar: What’s New in Draft NIST SP 800-171, Revision 3
June 6, 2023  |  1:00 – 2:00 PM ET

Space is limited, join the waitlist at
STAY IN TOUCH

CONTACT US

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

800-171comments@list.nist.gov

@NISTcyber