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

June 6, 2023 || 1:00 PM -2:00 PM Eastern

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Ron Ross
ron.ross@nist.gov

Victoria Yan Pillitteri
victoria.yan@nist.gov

Etiquette & Reminders

Due to the number of attendees, all participant microphones and cameras are **automatically muted**.

Please enter questions and comments for presenters in the WebEx Q&A.

Do not send questions via direct message to the host/panelists.

Q&A is NOT moderated.

Chat has been disabled for this event.

Please be kind and courteous to others.

For technical issues with WebEx, send a **PRIVATE Q&A via WebEx** to the Panelist "WEBEX Help" or email: 800-171comments@list.nist.gov

FAQ

Will this webinar be recorded?

Yes. The event will be recorded and posted at the event site within 10 business days.

When will slides be posted?

The slides will be posted by close of business on **June 6, 2023** on the event site**.**

Does NIST issue CE/CPE credits?

No. NIST does not provide specific information regarding CE/CPE credits. Attendees are welcome to use their registration confirmation email to self-report to their certification bodies.

Where is the event site?

https://csrc.nist.gov/Events/2023/protecting-cui-draft-sp800171-rev3

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

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Ron Ross
ron.ross@nist.gov

Victoria Yan Pillitteri
victoria.yan@nist.gov

Agenda

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

- Special Publication (SP) 800-171 at a Glance
- 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 THE CONFIDENTIALITY OF CUI

NONFEDERAL
SYSTEMS & ORGANIZATIONS

PROCESSING, STORING, OR TRANSMITTING
CUI

DRAFT REV 3
RELEASED MAY 10
COMMENT THRU JULY 14

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

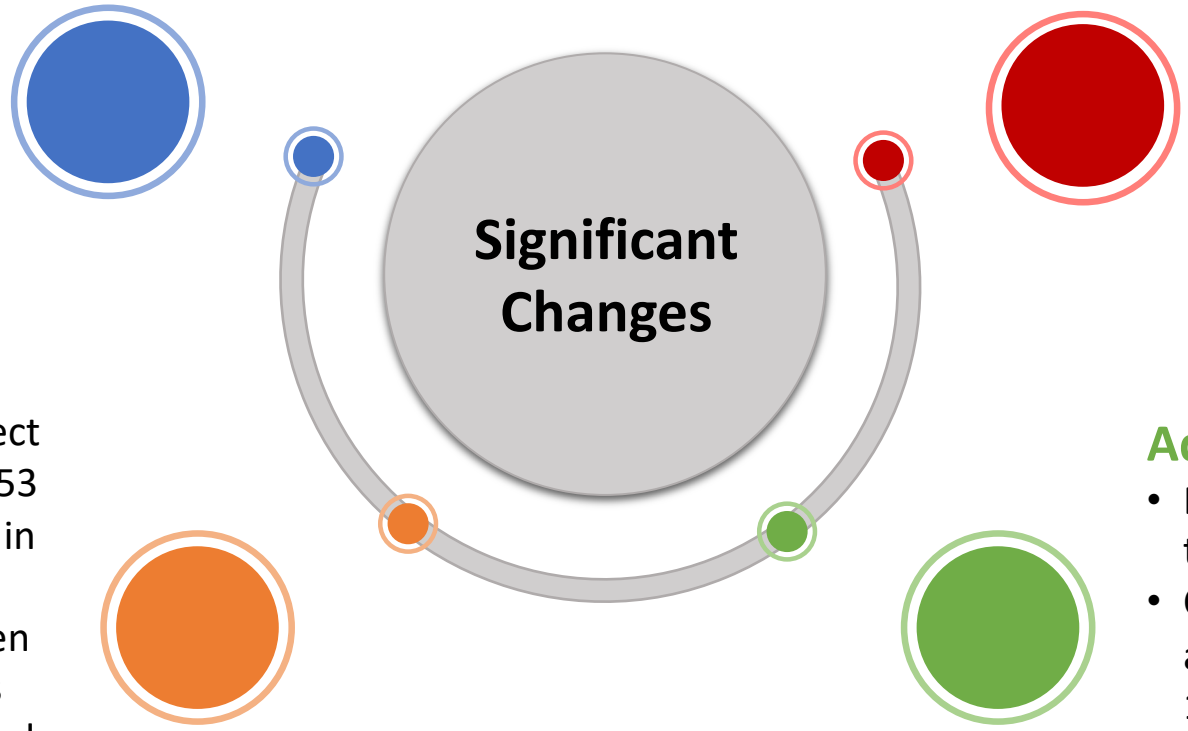
Overview: Draft SP 800-171 Rev 3

Improved Readability

Streamlined “Introduction” and “The Fundamentals” sections

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 & 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

- Developed *prototype* CUI Overlay using tailored controls in SP 800-53 Rev 5
- Created transition mapping tables & analysis of changes between SP 800-171 Revision 2 and Revision 3
- Developed an FAQ

Updated Security Requirements

Draft SP 800-171 Rev 3 Security Requirement Families			
Access Control (Added: 1, Withdrawn: 5)	**Maintenance** (Added: 0, Withdrawn: 3)	**Security Assessment & Monitoring** (Added: 3, Withdrawn: 1)	
Awareness & Training (Added: 0, Withdrawn: 0)	**Media Protection** (Added: 0, Withdrawn: 2)	**System & Communications Protection** (Added: 2, Withdrawn: 4)	
Audit & Accountability (Added: 0, Withdrawn: 0)	**Personnel Security** (Added: 0, Withdrawn: 0)	**System & Information Integrity** (Added: 1, Withdrawn: 3)	
Configuration Management (Added: 0, Withdrawn: 1)	**Physical Protection** (Added: 2, Withdrawn: 3)	**New Families**	**Planning** (Added: 4)
Identification & Authentication (Added: 1, Withdrawn: 4)	**Risk Assessment** (Added: 1, Withdrawn: 1)		**System & Services Acquisition** (Added: 2)
Incident Response (Added: 0, Withdrawn: 0)			**Supply Chain Risk Management** (Added: 4)

- ✓ 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
  - ODPs include assignment & selection operations
- ✓ Direct link to **source** SP 800-53 controls

New requirement structure

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*]**.

New ODP

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

SP 800-53 Source

Supporting Publications: SP 800-18 [67]

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 → IPD SP 800-171 Rev 3
NCO	Not directly related to protecting the confidentiality of CUI	58	81
NFO	Expected to be implemented by nonfederal organizations without specification	61	17
FED	Primarily the responsibility of the Federal Government	18	21
CUI	Directly related to protecting the confidentiality of CUI	125	168
NA	Not Applicable	New in IDP SP 800-171 Rev 3	50
	Moderate Baseline Security Controls by SP 800-53 Revision	**262**	**287**

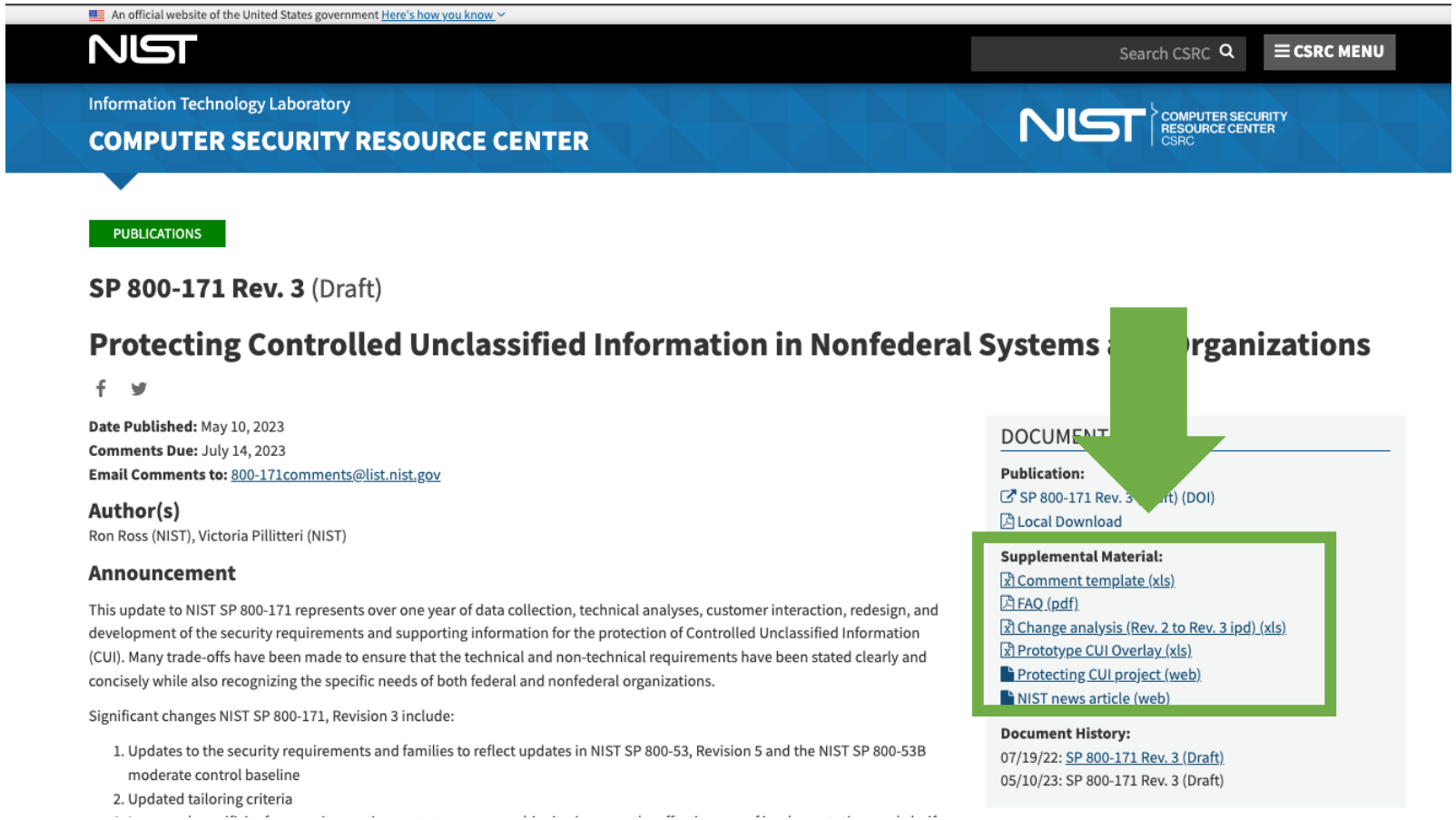
- ✓ New tailoring category, NA
- ✓ Recategorized selected controls from **SP 800-53B moderate baseline**

Updated Tailoring Criteria

Unique Sort ID (800-53r5)	SP 800-53 Rev 5 Control & Control Enhancement	Tailoring Decision	Unique Sort ID IPD 800-171r3	SP 800-171 Rev 3 Security Requirement
AC-01-00-00	**AC-1 Policy and Procedures**	**CUI**	**03-15-01:**	**3.15.1 Policy and Procedures**
AC-01-00-01	a. Develop, document, and disseminate to [Assignment: organization-defined personnel o 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.
AC-01-00-02	1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that:	CUI	03-15-01a.	3.15.1a. Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements.
AC-01-00-03	(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	NCO		—
AC-01-00-04	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	NCO		—
AC-01-00-05	2. Procedures to facilitate the implementation of the access control policy and the associated access controls;	CUI	03-15-01a.	3.15.1a. Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements.
AC-01-00-06	b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and	NCO		—
AC-01-00-07	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].
AC-01-00-08	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].
AC-01-00-09	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].

Added Supplemental Resources

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



https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft

Added Supplemental Resources

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

Family	SP 800-171 R2 SORT-ID	SP 800-171 R2 Identifier	SP 800-171 R2 Security Requirement	SP 800-171 R2 Basic or Derived Security Requirement	IPD SP 800-171 R3 SORT-ID	IPD SP 800-171 R3 Identifier	Initial Public Draft (IPD) SP 800-171 R3 Security Requirement	No Significant Change	Significant Change	Minor Change	New ODP	New Requirement	Withdrawn Requirement	Summary of Change(s)
Access Control	R2-03-01-01	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Basic	R3-03-01-01	3.1.1	**Account Management** a. Define and document the types of system accounts allowed and prohibited. b. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]. c. Specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges). d. Authorize access to the system based on a valid access authorization and intended system usage. e. Monitor the use of accounts. f. Disable accounts of individuals within [Assignment: organization-defined time period] when the accounts: 1. Have expired; 2. Are no longer associated with a user or individual; 3.Are in violation of organizational policy; or 4. Have been inactive for [Assignment: organization-defined time period]. g. Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks]. h. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When system usage or need-to-know changes for an		X		X			New security requirement title Aligned with SP 800-53, Rev 5 to provide more comprehensive detail on and foundational tasks for account management Added new ODP: policy, procedures and criteria for account management Added new ODP: time period to disable accounts Added new ODP: time period to disable inactive accounts Added new ODP: time period to disable accounts after significant risks Added new ODP: significant risks roles (with account management to notify personnel or roles (with account
Access Control	R2-03-01-02	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Basic	R3-03-01-02	3.1.2	**Access Enforcement** Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.	X						New security requirement title Aligned with SP 800-53, Rev 5 Rephrased for clarity; outcome remains unchanged
Access Control	R2-03-01-03	3.1.3	Control the flow of CUI in accordance with approved authorizations.	Derived	R3-03-01-03	3.1.3	**Flow Enforcement** Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.	X						New security requirement title Aligned with SP 800-53, Rev 5 Rephrased for clarity; outcome remains unchanged
Access Control	R2-03-01-04	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Derived	R3-03-01-04	3.1.4	**Separation of Duties** a. Identify the duties of individuals requiring separation. b. Define system access authorizations to support separation of duties.	X						New security requirement title Aligned with SP 800-53, Rev 5 Separated into two parts (a, b) needed for achieve outcome, rephrased for clarity; outcome remains unchanged

✓ Filter and Sort by Column

Added Supplemental Resources

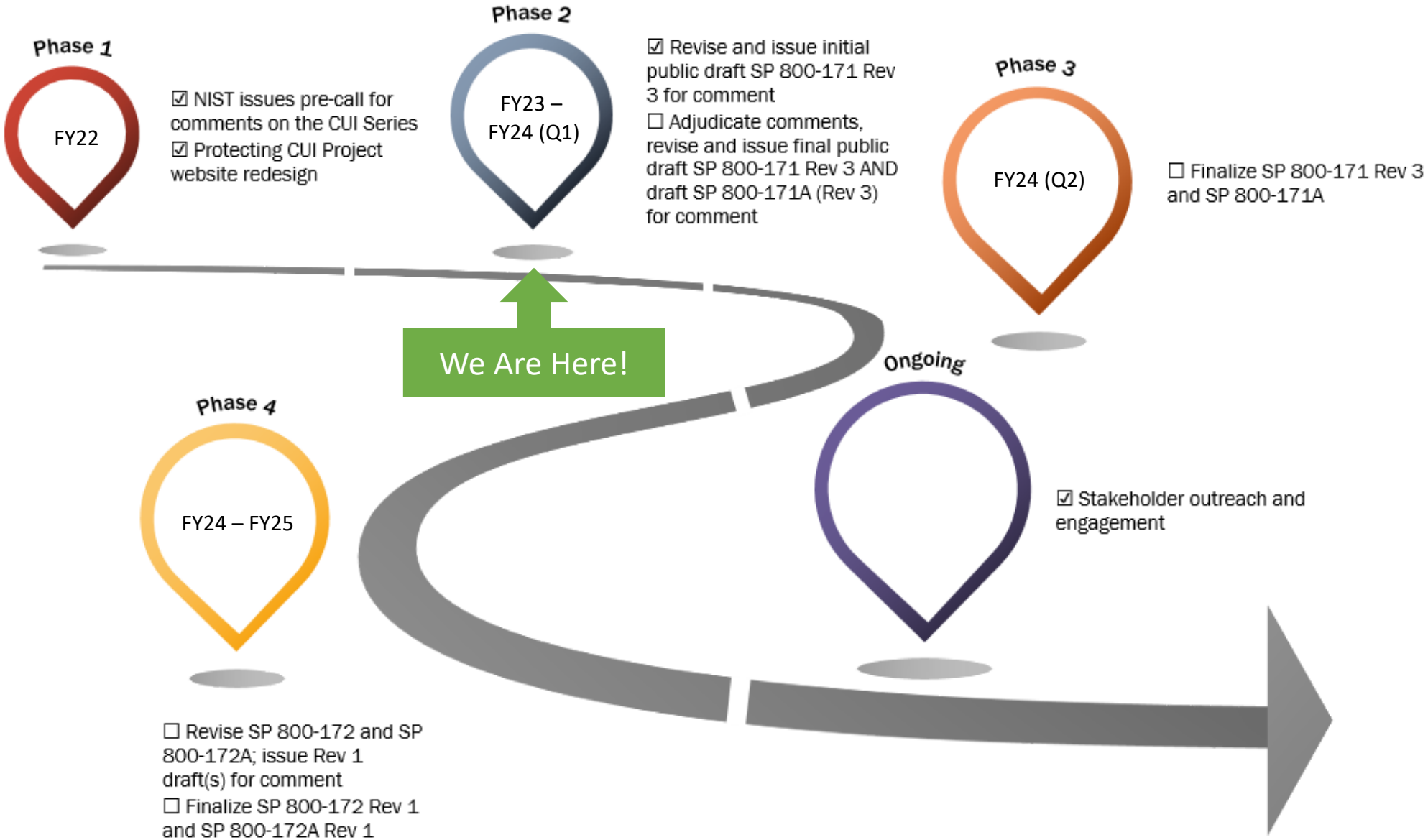
Prototype CUI Overlay

Unique Sort ID (800-53r5)	SP 800-53 Rev 5 Control & Control Enhancement	Tailoring Decision	Unique Sort ID (IPD 800-171r3	SP 800-171 Rev 3 Security Requirement	Additional Tailoring
AC-01-00-00	**AC-1 Policy and Procedures**	**CUI**	**03-15-01:**	**3.15.1 Policy and Procedures**	
AC-01-00-01	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.	Addresses all policy (instead of only access control policy) Removed ODP to assign "personnel or roles"
AC-01-00-02	1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that:			3.15.1a. Develop, document, and disseminate to organizational personnel or and procedures needed to implement security requirements.	Removed ODP to select one or more "organization-level; mission/business process-level; system level"
AC-01-00-03	(a) Addresses purpose, scope, roles, responsibilities, management commi coordination among organizational entities, and compliance; and				
AC-01-00-04	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	NCO		—	
AC-01-00-05	2. Procedures to facilitate the implementation of the access control policy and the associated access controls;	CUI	03-15-01a.	3.15.1a. Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements.	Addresses all procedures (instead of only access control procedures)
AC-01-00-06	b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and	NCO		—	
AC-01-00-07	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].	Addresses update of all policy and procedures (instead of only access control)
AC-01-00-08	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].	Removed ODP to assign "events"
AC-01-00-09	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].	Removed ODP to assign "events"
AC-02-00-00	**AC-2 Account Management**	**CUI**	**03-01-01:**	**3.1.1 Account Management**	
AC-02-00-01	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;	CUI	03-01-01a.	3.1.1a. Define and document the types of system accounts allowed and prohibited.	
AC-02-00-02	b. Assign account managers;	NFO		—	
AC-02-00-03	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



We need your feedback!

The public comment period is open through July 14, 2023

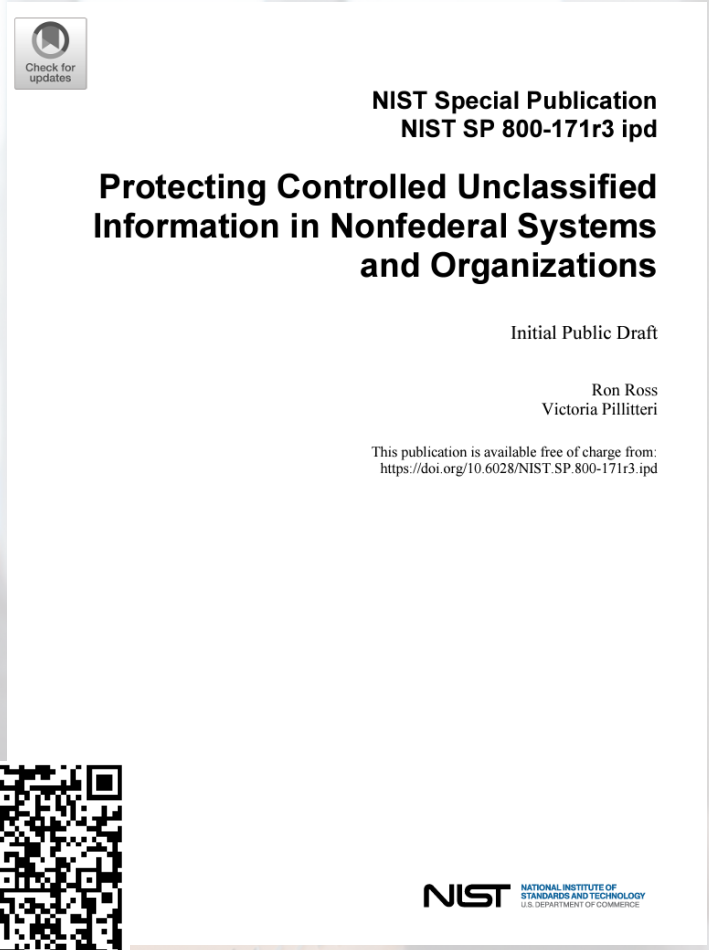
NIST is specifically interested in comments, feedback, and recommendations for the following topics:

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

Questions and to submit comments:
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.

https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

STAY IN TOUCH

CONTACT US

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

800-171comments@list.nist.gov

@NISTcyber