FutureFeed

Attain. Maintain. **Prove it Anytime.**

NIST SP 800-171 Revision 3

Stuart Itkin

February 27, 2025

A Bit About Me

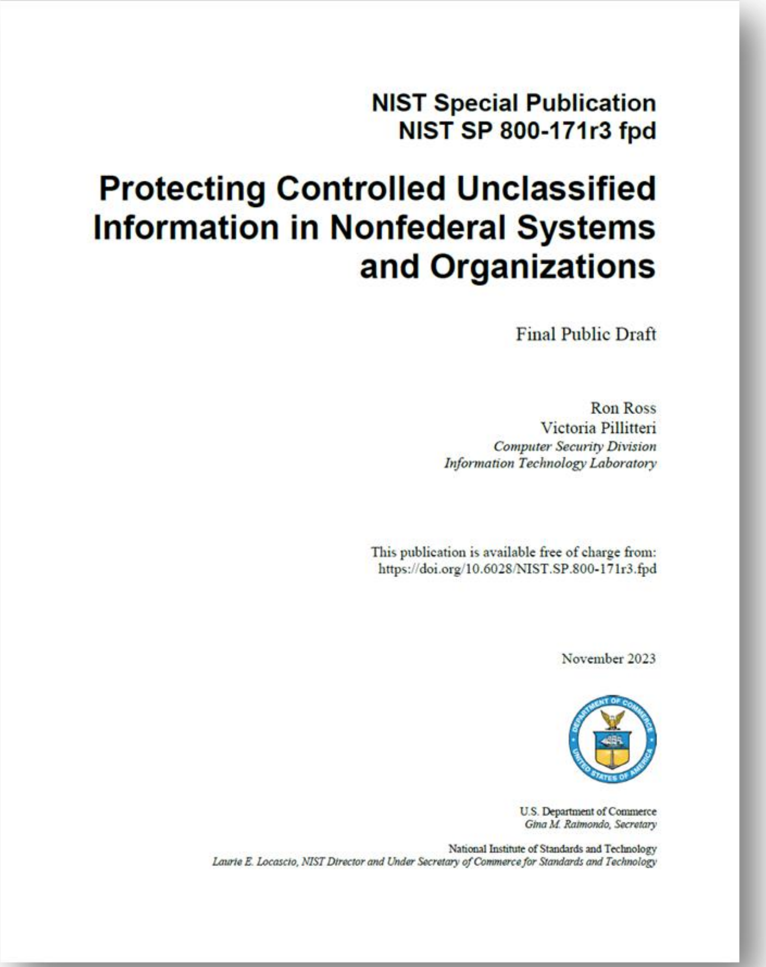
- Started out as a small child in Chicago, IL
- Member of the CMMC Standards Working Group
- Founding Board Director, MSPs for the Protection of Critical Infrastructure
- Director, CMMC Industry Standards Council
- Currently CRO and Security Evangelist at FutureFeed, the leading Cyber-GRC platform for the DIB
- Previously:
    - Senior Vice President at NeoSystems, a CMMC Managed Service Provider and RPO
    - Vice President of CMMC and FedRAMP Assurance at Coalfire Federal, an authorized C3PAO and RPO
    - Vice President of Products and Marketing at Exostar, a Boeing, Lockheed Martin, Raytheon Technologies, BAE Systems, Rolls Royce formed joint venture company
    - Lead mentor at Virginia State Government funded MACH37 cybersecurity product accelerator
- BA, MA, and ABD from the University of Illinois at Urbana-Champaign

BLUF (Bottom Line Up Front)

- NIST 800-171 Revision 3 was published in May 2024 and per NIST supersedes Revision 2
- 38 CFR 170 (the CMMC “Final Rule”), however, establishes Revision 2 as the foundation of the CMMC program (for now)
  - This will change at some point in the future
- Revision 3 gives you a little more work to do
  - But what you’ll need to do will be more clear
  - And nothing you’re doing to satisfy Revision 2 will be wasted
- Satisfying Revision 3 requirements will make you more secure !

What’s NIST 800-171’s Role?

- To provide a uniform set of standards for non-federal entities to ensure they maintain a baseline level of security consistent with federal expectations.
- To enhance the overall security of the federal supply chain to reduce the risk of cyber threats and information breaches.



NIST Special Publication
NIST SP 800-171r3 fpd

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Final Public Draft

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3.fpd

November 2023

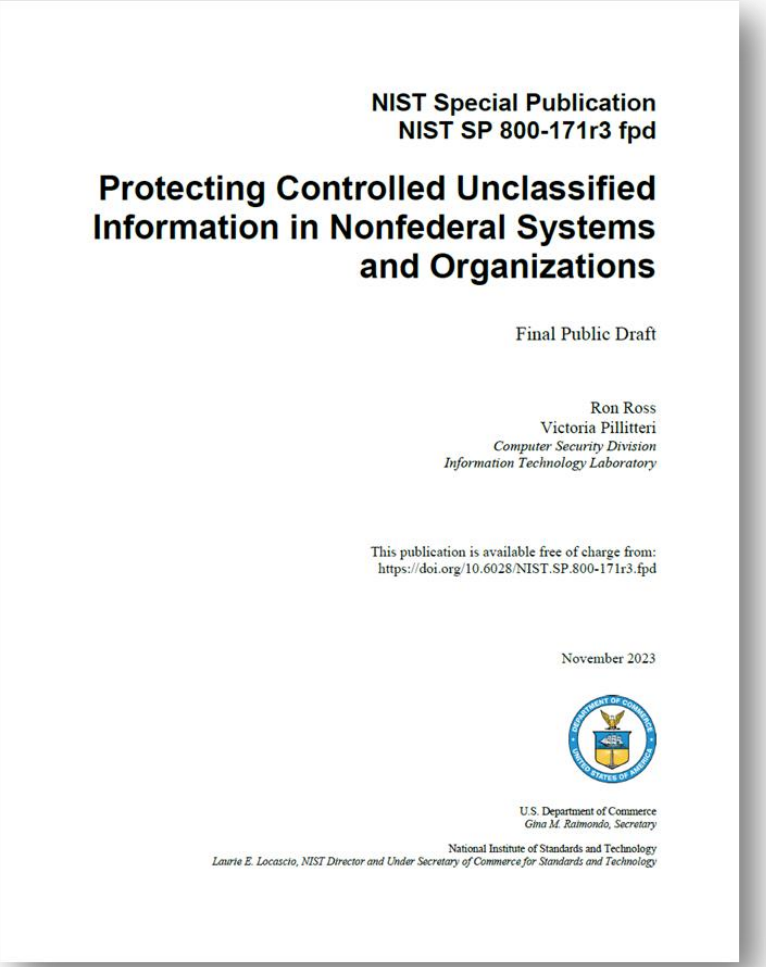
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Where did NIST 800-171 come from?

Executive Order 13556, November 4, 2010

- Established a governmentwide Controlled Unclassified Information (CUI) Program to standardize the way unclassified information that requires protection should be handled
- Designated the National Archive and Records Administration (NARA) as the Executive Agent to implement the program
- Tasked the Secretary of Commerce, through the Director of the National Institute of Standards and Technology (NIST), to develop and issue standardized guidelines for the protection of CUI on nonfederal information systems



NIST Special Publication
NIST SP 800-171r3 fpd

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Final Public Draft

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3.fpd

November 2023

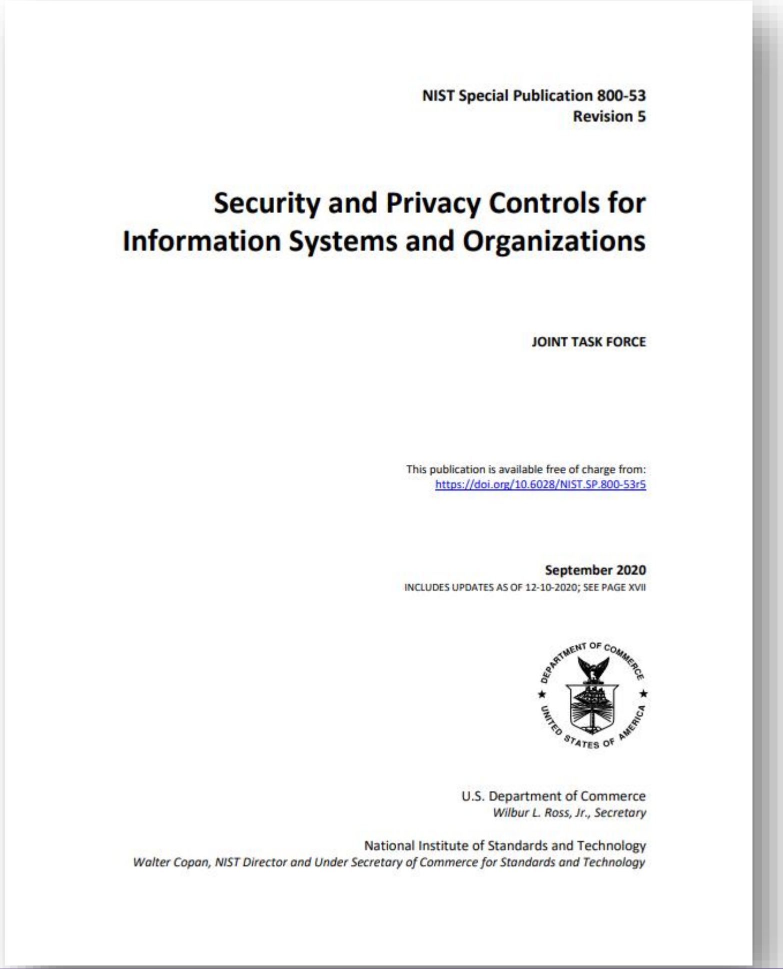
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

More specifically, Where did it come from?

NIST 800-53, "Security and Privacy Controls for Information Systems and Organizations."

- NARA had already established the Moderate Baseline for the protection of CUI in Government Systems
- Selected controls from the NIST 800-53 catalog that were relevant to protecting CUI in non-Federal systems where it was stored, processed, or transmitted
- 800-171 Rev 2
  - 110 Controls
  - `14 families



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Why did NIST create 800-171Rev 3?

- NIST 800-171Rev 2 based on NIST 800-53 Rev 4
- NIST 800-53 was update from Rev 4 to Rev 5 in 2020
  - Address evolving security and privacy challenges
  - Incorporate lessons learned
  - Reflects changes in technology and threat landscapes
- NIST 800-171Rev 3 (May 2024) establishes alignment with 800-53 Rev 5

NOTE, the following are all affected:

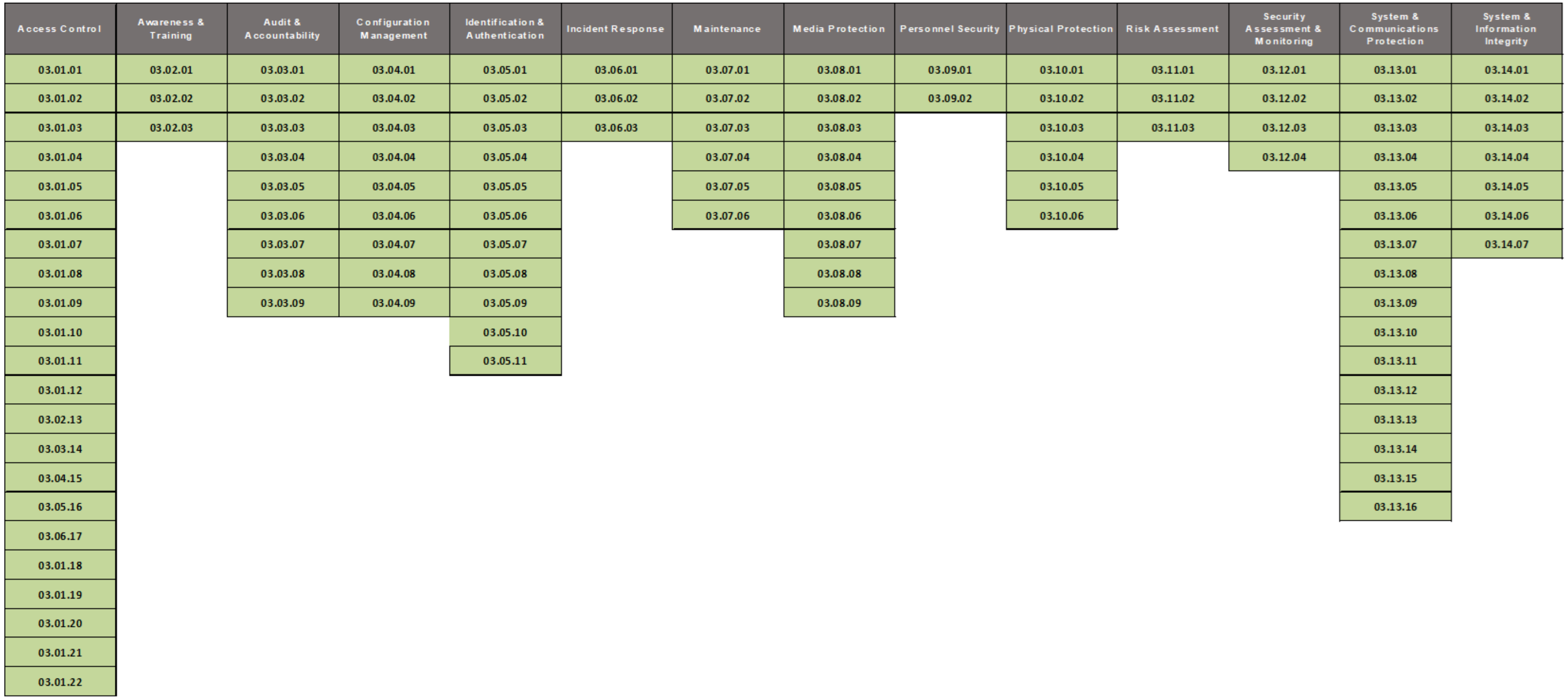
- NIST SP 800-171 Rev 3
- NIST SP 800-171A Rev 3
- NIST SP 800-172 Rev 3
- NIST SP 800-172A Rev 3

So, what has changed in 800-171Rev 3?

Alignment with NIST 800-53 Rev 5

- Improved readability
- Updated Security Requirements
  - Added, deleted, and changed security requirements to reflect controls and 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 & redundant requirements
- Updated Tailoring Criteria
  - Recategorized selected controls from SP 800-53B moderate baseline
- Added Supplemental Resources

NIST 800-171 Revision 2



Access Control	Awareness & Training	Audit & Accountability	Configuration Management	Identification & Authentication	Incident Response	Maintenance	Media Protection	Personnel Security	Physical Protection	Risk Assessment	Security Assessment & Monitoring	System & Communications Protection	System & Information Integrity
03.01.01	03.02.01	03.03.01	03.04.01	03.05.01	03.06.01	03.07.01	03.08.01	03.09.01	03.10.01	03.11.01	03.12.01	03.13.01	03.14.01
03.01.02	03.02.02	03.03.02	03.04.02	03.05.02	03.06.02	03.07.02	03.08.02	03.09.02	03.10.02	03.11.02	03.12.02	03.13.02	03.14.02
03.01.03	03.02.03	03.03.03	03.04.03	03.05.03	03.06.03	03.07.03	03.08.03		03.10.03	03.11.03	03.12.03	03.13.03	03.14.03
03.01.04		03.03.04	03.04.04	03.05.04		03.07.04	03.08.04		03.10.04		03.12.04	03.13.04	03.14.04
03.01.05		03.03.05	03.04.05	03.05.05		03.07.05	03.08.05		03.10.05			03.13.05	03.14.05
03.01.06		03.03.06	03.04.06	03.05.06		03.07.06	03.08.06		03.10.06			03.13.06	03.14.06
03.01.07		03.03.07	03.04.07	03.05.07			03.08.07					03.13.07	03.14.07
03.01.08		03.03.08	03.04.08	03.05.08			03.08.08					03.13.08	
03.01.09		03.03.09	03.04.09	03.05.09			03.08.09					03.13.09	
03.01.10				03.05.10								03.13.10	
03.01.11				03.05.11								03.13.11	
03.01.12												03.13.12	
03.02.13												03.13.13	
03.03.14												03.13.14	
03.04.15												03.13.15	
03.05.16												03.13.16	
03.06.17													
03.01.18													
03.01.19													
03.01.20													
03.01.21													
03.01.22													

FutureFeed

Attain. Maintain. **Prove it Anytime.**

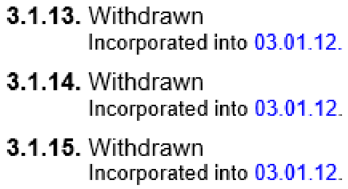
From 14 to 17 Control Families

Access Control (AC) - Policies and procedures for limiting access to systems and information to authorized users.	**Maintenance (MA)** - Performing periodic maintenance on systems and providing effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	**System and Communications Protection (SC)** - Protecting the confidentiality, integrity, and availability of information being transmitted or received.
Awareness and Training (AT) - Ensuring that all users are aware of the security risks associated with their activities and the applicable policies, standards, and procedures related to the security of the system.	**Media Protection (MP)** - Protecting digital and non-digital media containing CUI, including limiting access to authorized users and sanitizing or destroying media before disposal or reuse.	**System and Information Integrity (SI)** - Ensuring that systems and information are protected against malicious code, unauthorized changes, and other integrity violations.
Audit and Accountability (AU) - Implementing mechanisms to record and examine activity in information systems.	**Physical Protection (PE)** - Limiting physical access to systems, equipment, and the respective operating environments to authorized individuals	**Planning (PL) -** Having a System Security Plan (SSP), document organizational roles and responsibilities, and policies and procedure needed to implement security requirements.
Configuration Management (CM) - Establishing and maintaining the integrity of software and hardware through control of processes for initializing, changing, and monitoring configurations.	**Personnel Security (PS)** - Ensuring that individuals occupying positions of responsibility within an organization (including third-party service providers) are trustworthy and meet established security criteria for those positions.	**System and Services Acquisition (SA)** Establish requirements for system, system components, and external service providers and for their acquisition.
Identification and Authentication (IA) - Ensuring that only authorized individuals can access the system by verifying the identity of users, processes, or devices as a prerequisite to allowing access.	**Risk Assessment (RA)** - Assessing the security risks associated with the operation and use of organizational systems.	**Supply Chain Risk Management (SR)** Have a plan for managing supply chain risk, implement acquisition strategies to protect against and mitigate supply chain risk, and establish processes for identifying and addressing weaknesses and deficiencies.
Incident Response (IR) - Establishing an operational incident-handling capability for organizational systems, including preparation, detection, analysis, containment, recovery, and user response activities.	**Security Assessment (CA)** - Assessing the security controls in organizational systems to determine if the controls are effective in their application.	

From 110 to 97 CUI Controls: -12%

Type of Change	Change Description	Number of Controls
No significant change	Editorial changes to requirement; no change in outcome.	18
Significant Change	Additional detail in requirement, including more comprehensive detail on and foundational tasks for achieving the outcome of the requirement.	46
Minor Change	Editorial changes. Limited changes in level of detail and outcome of requirement.	15
New Requirement	Newly added requirement in FPD SP 800-171 Rev 3.	19
Withdrawn Requirement	Requirement withdrawn.	33
New Organization-defined Parameter (ODP)	*Note: New ODPs can apply to all change types with the exception of withdrawn requirements. Each requirement includes one or more new ODPs.*	49
	Total Number of Security Requirements in SP 800-171 Rev 3	**97**

But some "Withdrawn Requirements" have been Consolidated

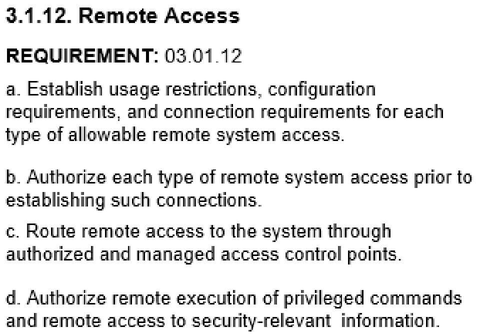


3.1.13. Withdrawn
Incorporated into 03.01.12.

3.1.14. Withdrawn
Incorporated into 03.01.12.

3.1.15. Withdrawn
Incorporated into 03.01.12.

So, some CUI Controls now have multiple Control Items



3.1.12. Remote Access

REQUIREMENT: 03.01.12

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.

b. Authorize each type of remote system access prior to establishing such connections.

c. Route remote access to the system through authorized and managed access control points.

d. Authorize remote execution of privileged commands and remote access to security-relevant information.

From 110 to 156 Control Items: +42%

NIST 800-171 Revision 3

Access Control	Awareness & Training	Audit & Accountability	Configuration Management	Identification & Authentication	Incident Response	Maintenance	Media Protection	Personnel Security	Physical Protection	Risk Assessment	Security Assessment & Monitoring	System & Communications Protection	System & Information Integrity	Planning	System & Services Acquisition	Supply Chain Risk Management
03.01.01	03.02.01	03.03.01	03.04.01	03.05.01	03.06.01		03.08.01	03.09.01	03.10.01	03.11.01	03.12.01	03.13.01	03.14.01	03.15.01	03.16.01	03.17.01
03.01.02	03.02.02	03.03.02	03.04.02	03.05.02	03.06.02		03.08.02	03.09.02	03.10.02	03.11.02	03.12.02		03.14.02	03.15.02	03.16.02	03.17.02
03.01.03		03.03.03	03.04.03	03.05.03	03.06.03		03.08.03				03.12.03		03.14.03	03.15.03	03.16.03	03.17.03
03.01.04		03.03.04	03.04.04	03.05.04	03.06.04	03.07.04	03.08.04			03.11.04		03.13.04				
03.01.05		03.03.05	03.04.05	03.05.05	03.06.05	03.07.05	03.08.05				03.12.05					
03.01.06		03.03.06	03.04.06			03.07.06			03.10.06			03.13.06	03.14.06			
03.01.07		03.03.07		03.05.07			03.08.07		03.10.07							
03.01.08		03.03.08	03.04.08				03.08.08		03.10.08			03.13.08	03.14.08			
03.01.09												03.13.09				
03.01.10			03.04.10									03.13.10				
03.01.11			03.04.11	03.05.11								03.13.11				
03.01.12			03.04.12	03.05.12								03.13.12				
												03.13.13				
												03.13.15				
03.05.16																
03.01.18																
03.01.20																
03.01.22																

Changes Between Revisions 2 and 3

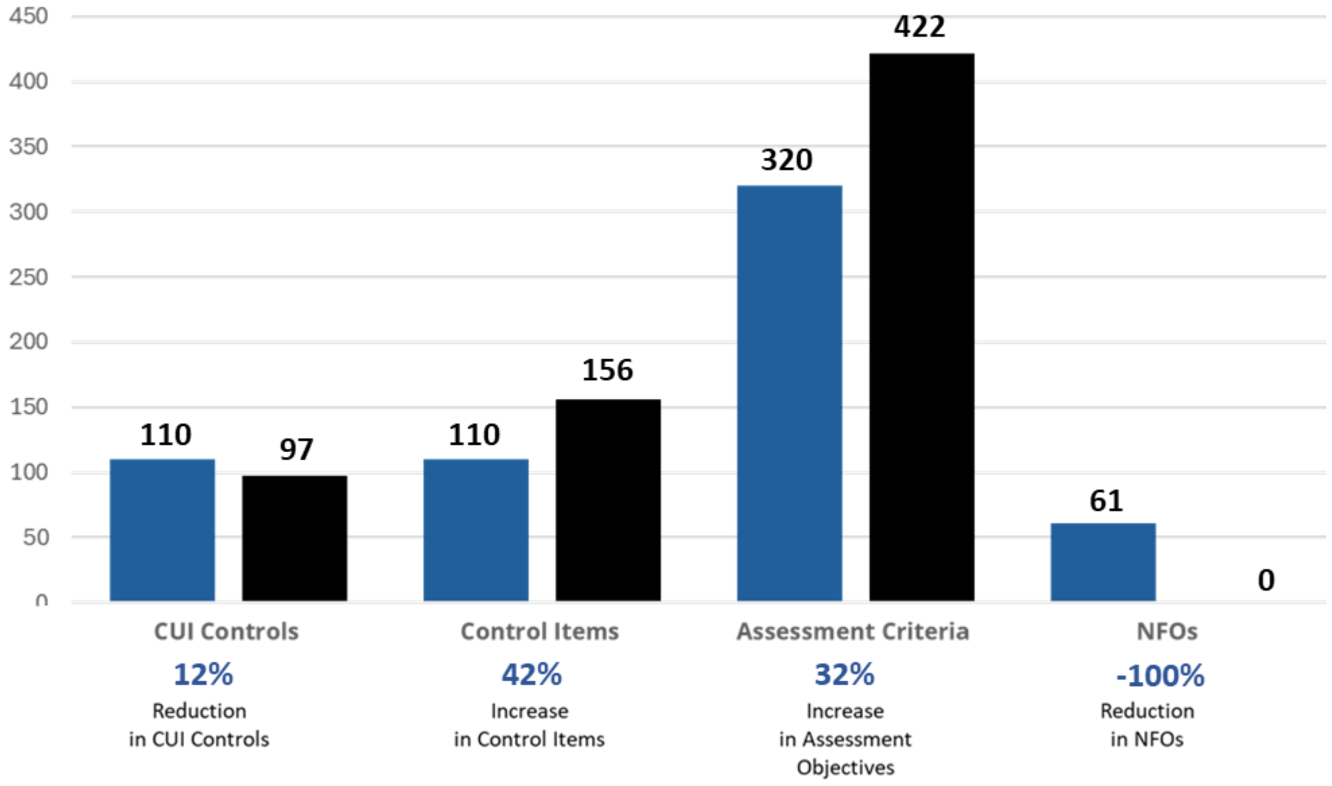
Access Control	Awareness & Training	Audit & Accountability	Configuration Management	Identification & Authentication	Incident Response	Maintenance	Media Protection	Personnel Security	Physical Protection	Risk Assessment	Security Assessment & Monitoring	System & Communications Protection	System & Information Integrity	Planning	System & Services Acquisition	Supply Chain Risk Management
03.01.01	03.02.01	03.03.01	03.04.01	03.05.01	03.06.01	▨	03.08.01	03.09.01	03.10.01	03.11.01	03.12.01	03.13.01	03.14.01	03.15.01	03.16.01	03.17.01
03.01.02	03.02.02	03.03.02	03.04.02	03.05.02	03.06.02	▨	03.08.02	03.09.02	03.10.02	03.11.02	03.12.02	▨	03.14.02	03.15.02	03.16.02	03.17.02
03.01.03	▨	03.03.03	03.04.03	03.05.03	03.06.03	▨	03.08.03		▨	▨	03.12.03	▨	03.14.03	03.15.03	03.16.03	03.17.03
03.01.04		03.03.04	03.04.04	03.05.04	03.06.04	03.07.04	03.08.04		▨	03.11.04	▨	03.13.04	▨			
03.01.05		03.03.05	03.04.05	03.05.05	03.06.05	03.07.05	03.08.05		▨		03.12.05	▨	▨			
03.01.06		03.03.06	03.04.06	▨		03.07.06	▨		03.10.06			03.13.06	03.14.06			
03.01.07		03.03.07	▨	03.05.07			03.08.07		03.10.07			▨	▨			
03.01.08		03.03.08	03.04.08	▨			03.08.08		03.10.08			03.13.08	03.14.08			
03.01.09		▨	▨	▨			▨					03.13.09				
03.01.10			03.04.10	▨								03.13.10				
03.01.11			03.04.11	03.05.11								03.13.11				
03.01.12			03.04.12	03.05.12								03.13.12				
▨												03.13.13				
▨												▨				
▨												03.13.15				
03.05.16												▨				
▨																
03.01.18																
▨																
03.01.20																
▨																
03.01.22																

FutureFeed

Attain. Maintain. **Prove it Anytime.**

Net Impact of Control Slight of Hand

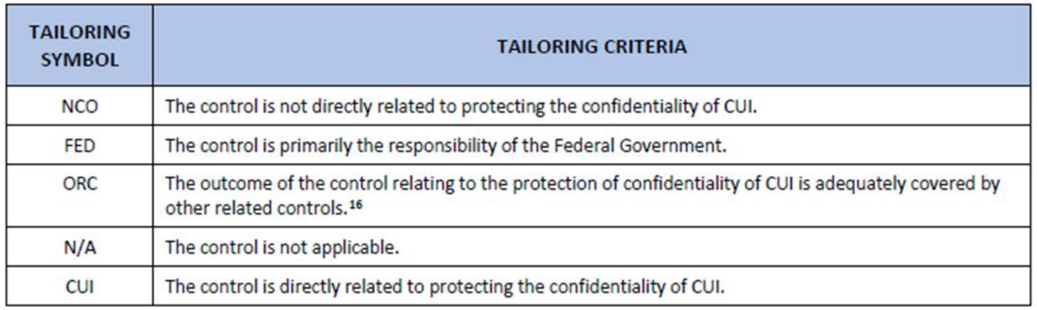
	Assessment Objectives	
NIST 800-171 Rev2	320	
NIST 800-171 Rev3	510	+59%
Aos that are ODPs	(88)	
Net Assessment Objectives	422	+32%



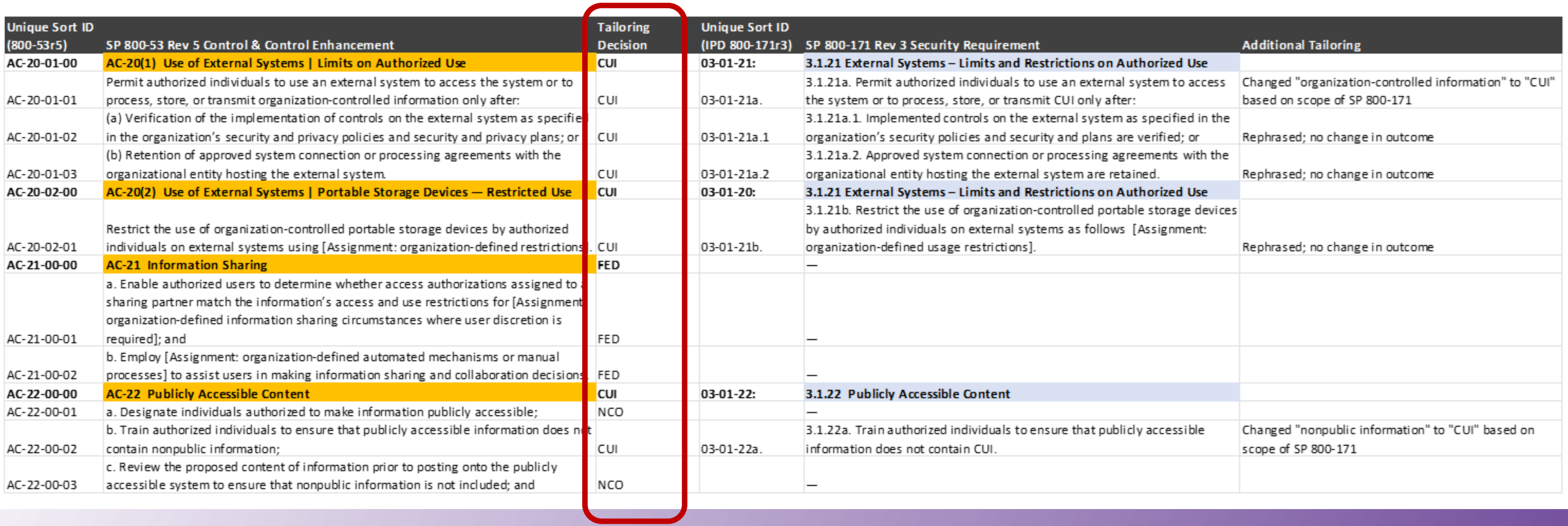
Establishing NIST 800-171 Rev 3 Controls

How NIST decided which 800-53 controls went into 800-171 Rev 3

Security control tailoring criteria



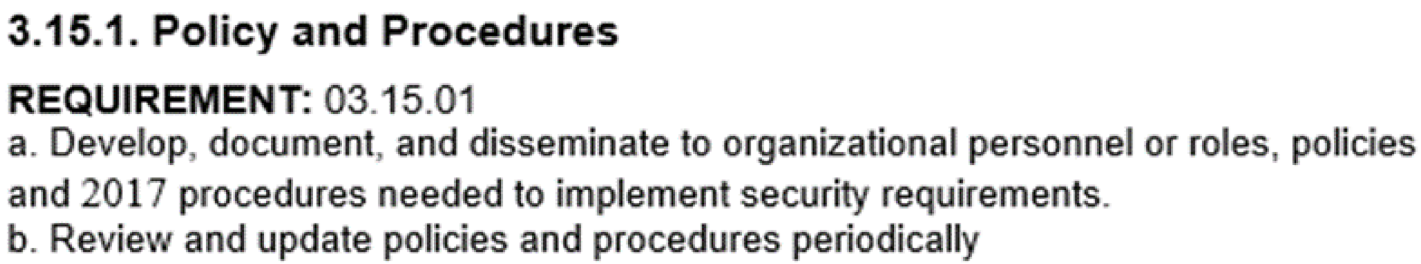
TAILORING SYMBOL	TAILORING CRITERIA
NCO	The control is not directly related to protecting the confidentiality of CUI.
FED	The control is primarily the responsibility of the Federal Government.
ORC	The outcome of the control relating to the protection of confidentiality of CUI is adequately covered by other related controls.[16]
N/A	The control is not applicable.
CUI	The control is directly related to protecting the confidentiality of CUI.



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-20-01-00	**AC-20(1) Use of External Systems | Limits on Authorized Use**	**CUI**	**03-01-21:**	**3.1.21 External Systems – Limits and Restrictions on Authorized Use**	
AC-20-01-01	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:	CUI	03-01-21a.	3.1.21a. Permit authorized individuals to use an external system to access the system or to process, store, or transmit CUI only after:	Changed "organization-controlled information" to "CUI" based on scope of SP 800-171
AC-20-01-02	(a) Verification of the implementation of controls on the external system as specifie in the organization's security and privacy policies and security and privacy plans; or	CUI	03-01-21a.1	3.1.21a.1. Implemented controls on the external system as specified in the organization's security policies and security and plans are verified; or	Rephrased; no change in outcome
AC-20-01-03	(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.	CUI	03-01-21a.2	3.1.21a.2. Approved system connection or processing agreements with the organizational entity hosting the external system are retained.	Rephrased; no change in outcome
AC-20-02-00	**AC-20(2) Use of External Systems | Portable Storage Devices — Restricted Use**	**CUI**	**03-01-20:**	**3.1.21 External Systems – Limits and Restrictions on Authorized Use**	
AC-20-02-01	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].	CUI	03-01-21b.	3.1.21b. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems as follows [Assignment: organization-defined usage restrictions].	Rephrased; no change in outcome
AC-21-00-00	**AC-21 Information Sharing**	**FED**		—	
AC-21-00-01	a. Enable authorized users to determine whether access authorizations assigned to sharing partner match the information's access and use restrictions for [Assignment organization-defined information sharing circumstances where user discretion is required]; and	FED		—	
AC-21-00-02	b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.	FED		—	
AC-22-00-00	**AC-22 Publicly Accessible Content**	**CUI**	**03-01-22:**	**3.1.22 Publicly Accessible Content**	
AC-22-00-01	a. Designate individuals authorized to make information publicly accessible;	NCO		—	
AC-22-00-02	b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;	CUI	03-01-22a.	3.1.22a. Train authorized individuals to ensure that publicly accessible information does not contain CUI.	Changed "nonpublic information" to "CUI" based on scope of SP 800-171
AC-22-00-03	c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and	NCO		—	

Also, noteworthy while we talk about controls

Policy and Procedures are now explicitly required !



3.15.1. Policy and Procedures

REQUIREMENT: 03.15.01
a. Develop, document, and disseminate to organizational personnel or roles, policies and 2017 procedures needed to implement security requirements.
b. Review and update policies and procedures periodically

Beware of “Ghost Controls”

- Removed legacy control still reasonably required to demonstrate compliance

  NFO AT-4 (Training Records) was removed.

  The ability to demonstrate that training was performed requires evidence of individual training records.

  AT-4 technically exists as a ghost control

Enhanced Clarity and Specificity

Eliminating the distinction between “Basic” and “Derived” requirements

- FIPS 200 “Basic Requirements”
- 800-53 “Derived Requirements”

} Both had to be satisfied

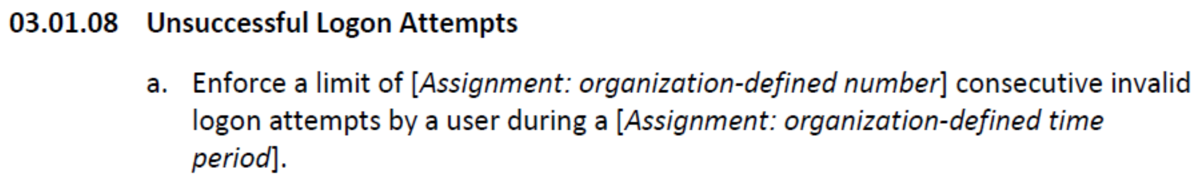
- NIST decided to rely on 800-53 controls to enhance specificity
- Many “Derived” requirements folded into existing requirements to enhance clarity

This removes subjectivity to the benefit of OSCs and Assessors

Organization Defined Parameters (ODP)

NIST 800-171 introduces ODPs (there are 88)

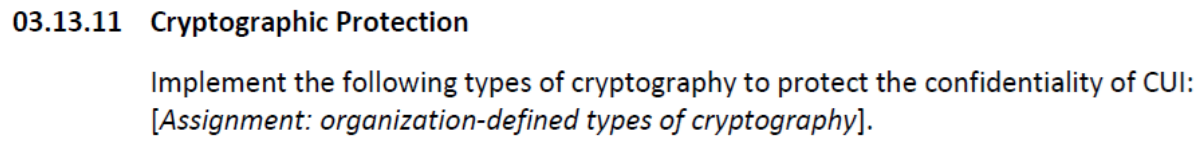
- Provide specificity
- Provide flexibility to align requirements with mission and effectively manage risk
- Support consistent security assessments



03.01.08 Unsuccessful Logon Attempts

a. Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*].

- ODPs set by government (federal agency or a group of federal agencies)
- Where not prescribed, r3 requires contractor to assign the value
- Encryption is now an ODP



03.13.11 Cryptographic Protection

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

NOTE: NIST SP 800-171A Rev 3 contains more ODPs than NIST SP 800-171 Rev 3 You must follow the Assessment Guide.

FutureFeed

Attain. Maintain. **Prove it Anytime.**

What about CMMC?

- NIST 800-171 Rev 3 was published May 2024
- DFARS 252.204-7012(b)(2)(i) states:

  > Except as provided in paragraph (b)(2)(ii) of this clause, **the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171**, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) **in effect at the time the solicitation is issued or as authorized by the Contracting Officer**.

- But 32 CFR 170 (CMMC Final Rule) establishes NIST 800-171 Rev 2 as the basis for CMMC
  - This will change at some point in the future, but will require a rule change
- The proposed Part 48 CUI FAR rule similarly specifies Rev 2 (although NIST says Rev 2 is superseded)

When will NIST 800-171 Rev 3 go into effect?

- A lot must happen to transition from Revision 2 to Revision 3
  - A change to 32 CFR 170
  - Changes to SPRS and eMASS
  - Updated CCP and CCA training materials and curriculum
  - Updated CMMC Assessment Process
  - CCP and CCA re-training and re-certification
  - Template updates
- Remember
  - DoD initially (2015) provided contractors 2 years to implement NIST 800-171
  - It took FedRAMP 32 months to move from NIST 800-53 Rev 4 to Rev 5
- So, when? 2027 is a reasonable guess

Takeaways

- Rev 3 gives you a little more work to do
- What you'll need to do will be more clear
- Nothing you're doing to satisfy Revision 2 will be wasted
- Rev 3 doesn't derail the CMMC 2.11 rollout

- Satisfying Rev 3 requirements will make you more secure

Thank You

THANK YOU!