NDIA

CMMC Update:
Review of NIST 800-171 Rev3
Part 2

Current As Of: July 2023

Sponsored by:

C3 INTEGRATED SOLUTIONS

TODAY'S SPEAKERS

Amira Armond

President

Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Jacob Horne

Chief Security Evangelist

Summit 7

Director of Policy & Standards

MSPs for the Protection of Critical Infrastructure

Vince Scott

CEO

Defense Cybersecurity Group

INFRAGARD National SME Cyberwarfare

Scott Whitehouse

Director of Compliance Services

C3Integrated Solutions

Sponsored by:

C3 INTEGRATED SOLUTIONS

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2
  - Companies not complying sufficiently under current regulation
  - Does not negate obligation to meet the contractual requirements
- CMMC announced Jul ’19 -- 3rd Party Assessments to ensure 800-171 implementation in the future
  - CMMC 2.0 announced Nov ’21
- **DRAFT NIST 800-171Rev3 released 10 May 23**

Sponsored by:

C3 INTEGRATED SOLUTIONS

Supply Chain Risk Management (SCRM) Domain

- **Supply Chain Risk Management (SCRM)**
  - “**Develop a plan** for managing supply chain risks associated with the development, manufacturing, acquisition, delivery, operations, maintenance, and disposal of the system, system components, or system services. “
- **Goals:**
  - Prevent purchase of pre-compromised materials (backdoor chips added to motherboards)
  - Avoid counterfeit parts (Cisco)
  - Reduce risk of product/service becoming compromised (Solarwinds)
  - Reduce risk of risk of product/service not performing its purpose (MSSPs that fail to perform incident monitoring)
- **Different from contractual SCRM which focuses on not passing-through compromised / counterfeit parts to US Government**

Sponsored by:

C3 INTEGRATED SOLUTIONS

Non-Federal Organization (NFO) Controls

- **Most NFO controls/requirements (see Appendix E of 171Rev2… these are assumed to be in place) were incorporated into the main body although a few remain**
- **Policies and Procedures now explicitly required as part of the new Planning Domain**
  - They did not break this down for each domain and do ***not*** require a procedure for each requirement
  - “Procedures can be documented in system security plans or in one or more separate documents.”
- **System Security Plan (SSP) and Incident Response Plan (IRP)**
  - Don’t wait—clear, concise documentation of processes
  - Include update procedures and track updates

System Security Plan – What do I document?

- SSP: primary source of cybersecurity policies
- NIST 800-171 Rev 3: “unambiguously compliant”
  - Can choose to leverage multiple supporting documents
  - Supporting documents: artifacts, procedures, plans
- Documenting can help identify shortfalls in processes
- Unsure whether to document? Document it!

Incident Response Policy (or plan?)

- May be most important document/plan
- When an event happens what do you do?
- IR policies frequently 50+ pages
  - Cover all aspects of Incident Response
- Working with a vendor, partner, or parent company?
  - Examine and document each entity's roles and responsibilities
  - Eliminate Assumptions
  - Granular questions
  - Success = repeatable processes, realistic checkpoints

Sponsored by:

C3 INTEGRATED SOLUTIONS

Where do I start with my documentation?

- At ground zero?
  - GRC platform may help organize
  - Boiler plate templates
- Some documentation?
  - Consider independent trusted advisor
  - Beware of group think
- Almost there?
  - Congratulations!
  - Have someone check your work
  - Avoid blind spots

Sponsored by: C3 INTEGRATED SOLUTIONS

External systems

- **Addresses major flaw of Rev2**
  - **Verifying security of external systems was barely mentioned – and no minimums defined**
    - Cloud hosting providers: AWS, Office 365, SalesForce
    - Service providers: Remote Management clouds, MSPs, MSSPs
    - Other providers: Co-locations, third party datacenters, consultants
- **Flaw drove DoD to add extra requirement: “clouds must be FedRAMP moderate or equivalent”**

  - Will Rev3 clarify expectation is 800-171 for non-federal systems?

Sponsored by:

C3 INTEGRATED SOLUTIONS

Use of External Systems

- **Goal: If an external information system can access your CUI, make sure it is at least as secure as your information system!**

- **3.1.20:** [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; **Identify** [Assignment: **organization-defined controls asserted to be implemented on external systems**]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
  1. Access the system from external systems; and
  2. Process, store, or transmit CUI using external systems; **OR** b. Prohibit the use of [Assignment: organizationally-defined types of external systems].
- **3.1.21:** a. Permit authorized individuals to **use an external system** to **access the system** or to **process, store, or transmit CUI** only after:
  1. Implemented **controls on the external system** as specified in the organization's security policies and security plans **are verified**; or
  2. Approved system connection or processing **agreements** with the organizational entity hosting the external system **are retained**.

Sponsored by:

C3 INTEGRATED SOLUTIONS

External service providers

- **Goals**:
  - Know how your provider is helping you perform security requirements
  - Ensure they perform appropriate controls
  - Evaluate regularly
- a. Require the providers of external system services to **comply with organizational security requirements and** implement the following controls: [Assignment: **organization-defined controls].**
- b. Define and document organizational oversight and user roles and responsibilities with regard to external system services.
- c. Implement the following processes, methods, and techniques to **monitor control compliance by external service providers on an ongoing basis:** [Assignment: organization-defined processes, methods, and techniques]

Sponsored by:

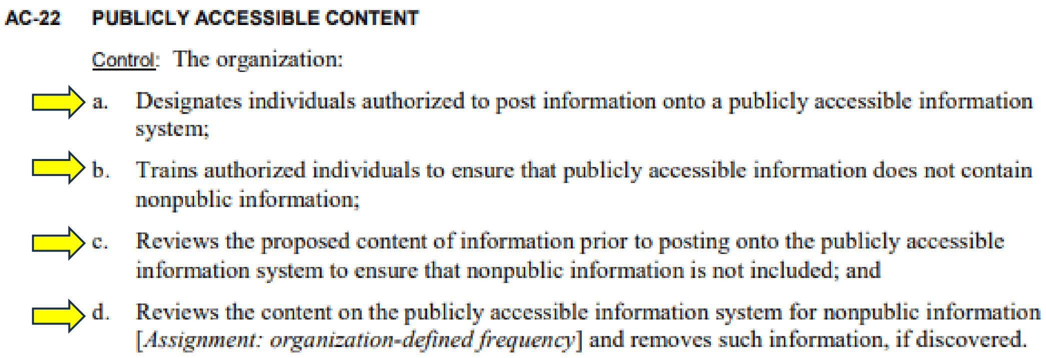
Independent assessment requirements

- **3.12.5. Independent Assessment**
  - Use independent assessors or assessment teams to assess controls
- **Independent assessors or assessment teams**
  - Individuals or groups who conduct impartial security assessments of the system
  - “Impartiality” means assessors are free from perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the system under assessment or the determination of control effectiveness.

Phantom Increases

- **800-171r2 formatting obscured too much of the underlying CUI-relevant controls in 800-53r4 creating the illusion that 800-171r3 formatting introduces significant net-new requirement tasks**

800-53r4 **(WAS)**



AC-22 PUBLICLY ACCESSIBLE CONTENT

Control: The organization:

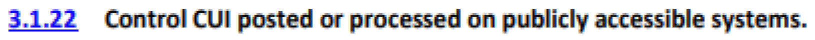
a. Designates individuals authorized to post information onto a publicly accessible information system;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d. Reviews the content on the publicly accessible information system for nonpublic information [*Assignment: organization-defined frequency*] and removes such information, if discovered.

800-171r2 **(IS)**



3.1.22 Control CUI posted or processed on publicly accessible systems.

- Who?
- What?
- When?
- How often?

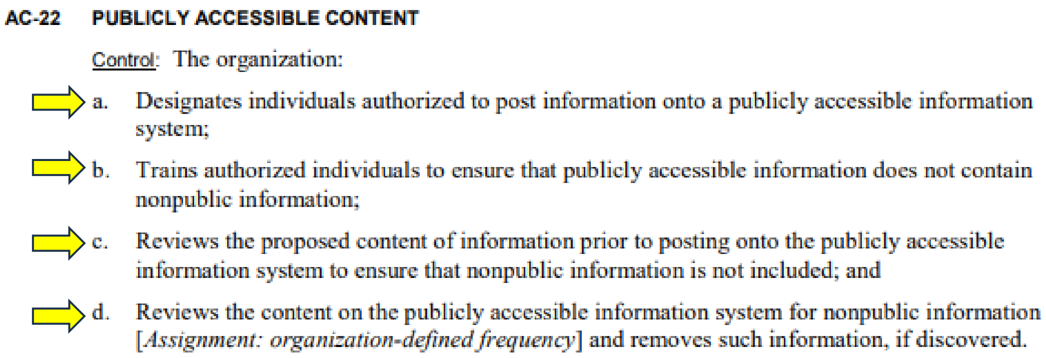
Sponsored by:

C3 INTEGRATED SOLUTIONS

Phantom Increases

- **Changes between 800-171r2 and 800-171r3 have less to do with 171 itself and more to do with changes between 800-53r4 and 800-53r5 (or lack thereof)**

800-53r4 **(WAS)**



AC-22 PUBLICLY ACCESSIBLE CONTENT

Control: The organization:

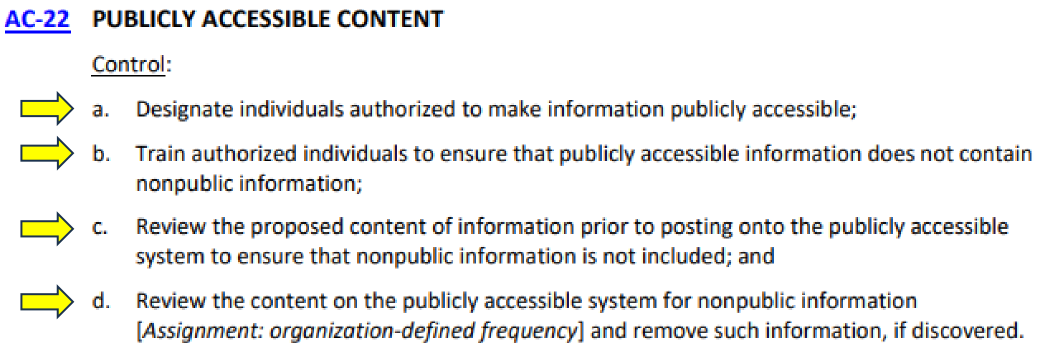
a. Designates individuals authorized to post information onto a publicly accessible information system;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d. Reviews the content on the publicly accessible information system for nonpublic information [*Assignment: organization-defined frequency*] and removes such information, if discovered.

800-53r5 **(IS)**



AC-22 PUBLICLY ACCESSIBLE CONTENT

Control:

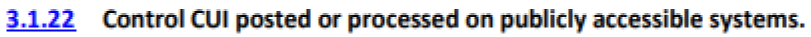
a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information [*Assignment: organization-defined frequency*] and remove such information, if discovered.

800-171r2 **(IS)**



3.1.22 Control CUI posted or processed on publicly accessible systems.

- Who?
- What?
- When?
- How often?

Sponsored by:

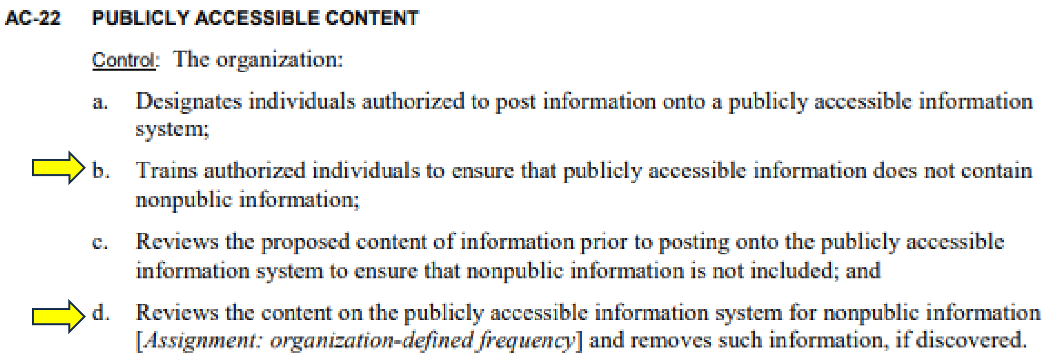
C3 INTEGRATED SOLUTIONS

Phantom Increases

NDIA

- Many "new" requirement line items aren't new at all from NIST's perspective; 800-171r3 requirements still represent portions of 800-53 controls, but with more clarity & traceability

800-53r4 **(WAS)**



AC-22 PUBLICLY ACCESSIBLE CONTENT

Control: The organization:

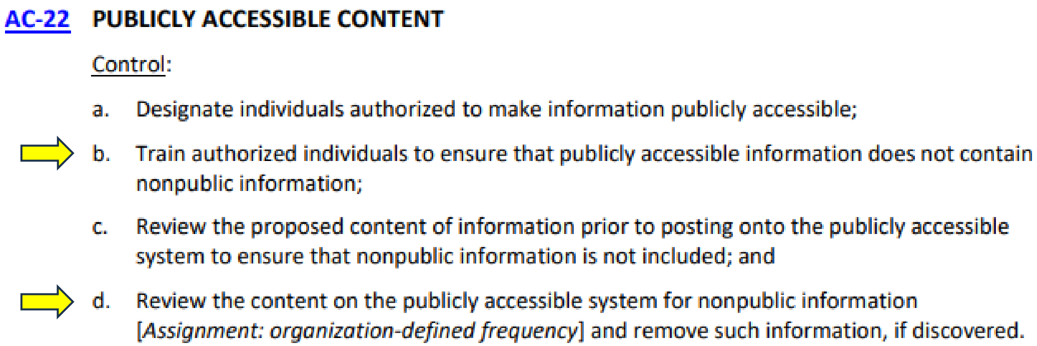
a. Designates individuals authorized to post information onto a publicly accessible information system;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d. Reviews the content on the publicly accessible information system for nonpublic information [*Assignment: organization-defined frequency*] and removes such information, if discovered.

800-53r5 **(IS)**



AC-22 PUBLICLY ACCESSIBLE CONTENT

Control:

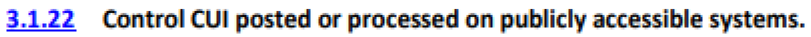
a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information [*Assignment: organization-defined frequency*] and remove such information, if discovered.

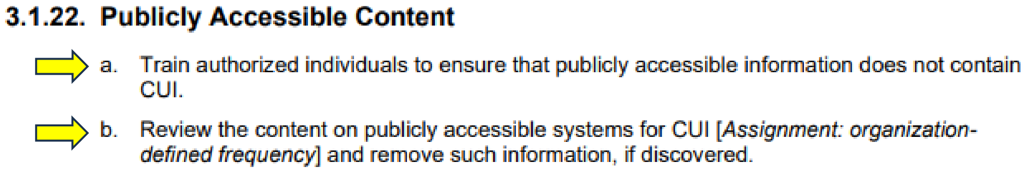
800-171r2 **(IS)**



3.1.22 Control CUI posted or processed on publicly accessible systems.

- Who?
- What?
- When?
- How often?

171r3 IPD **(WILL BE)**



3.1.22. Publicly Accessible Content

a. Train authorized individuals to ensure that publicly accessible information does not contain CUI.

b. Review the content on publicly accessible systems for CUI [*Assignment: organization-defined frequency*] and remove such information, if discovered.

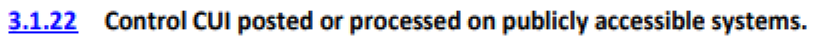
Sponsored by:

C3 INTEGRATED SOLUTIONS

Phantom Increases

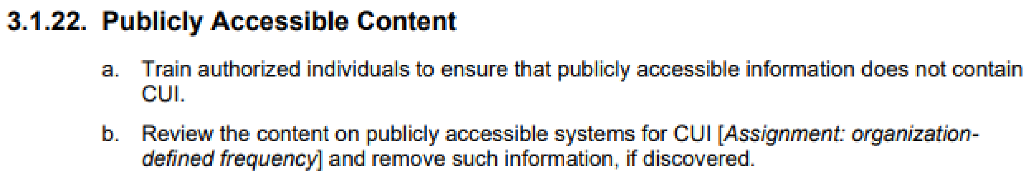
- **Many “new” requirement line items aren’t new at all from NIST’s perspective; 800-171r3 requirements still represent portions of 800-53 controls, but with more clarity & traceability**

800-171r2 **(IS)**



3.1.22 Control CUI posted or processed on publicly accessible systems.

171r3 IPD **(WILL BE)**



3.1.22. Publicly Accessible Content

a. Train authorized individuals to ensure that publicly accessible information does not contain CUI.

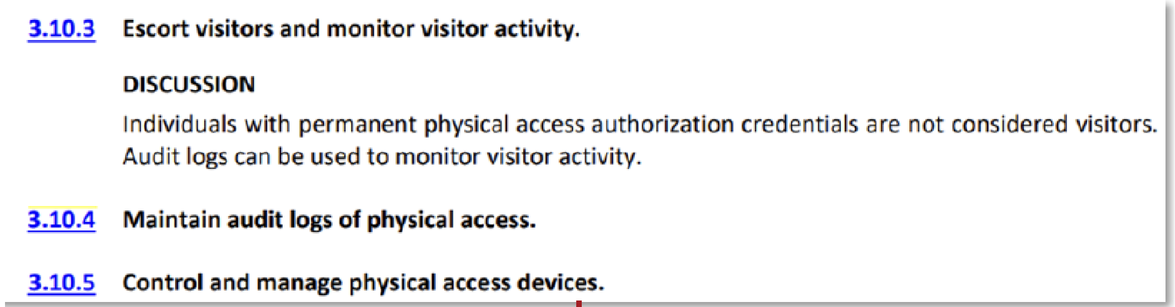
b. Review the content on publicly accessible systems for CUI [*Assignment: organization-defined frequency*] and remove such information, if discovered.

Is this really a 50% increase in the number of line items?
Is it actually “new”?

Sponsored by:

Phantom Decreases

SP 800-171r2



3.10.3 **Escort visitors and monitor visitor activity.**

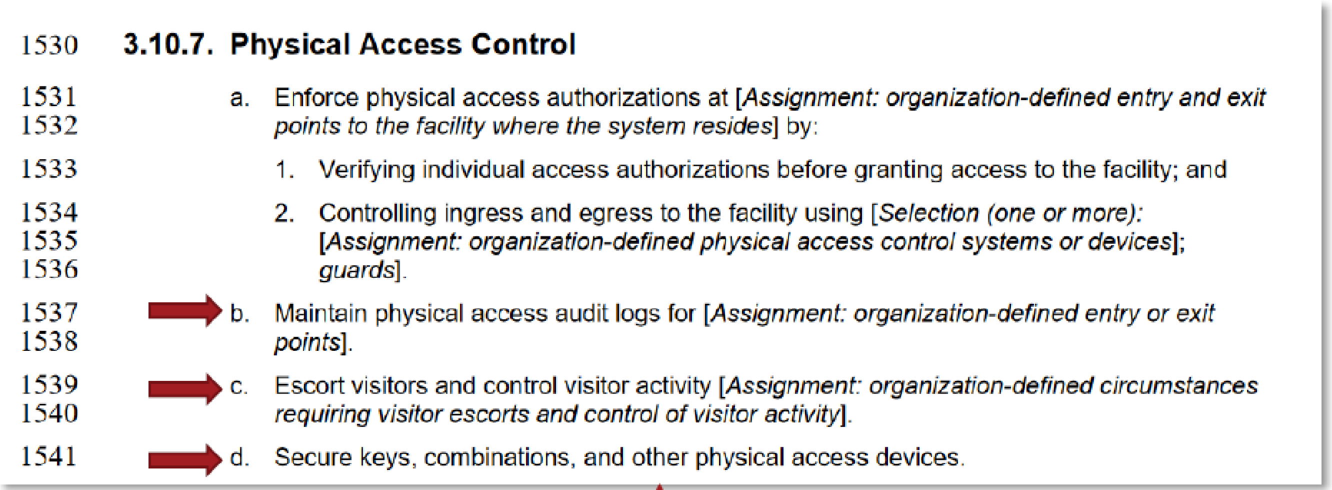
DISCUSSION

Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

3.10.4 **Maintain audit logs of physical access.**

3.10.5 **Control and manage physical access devices.**

SP 800-171r3 IPD



3.10.7. Physical Access Control

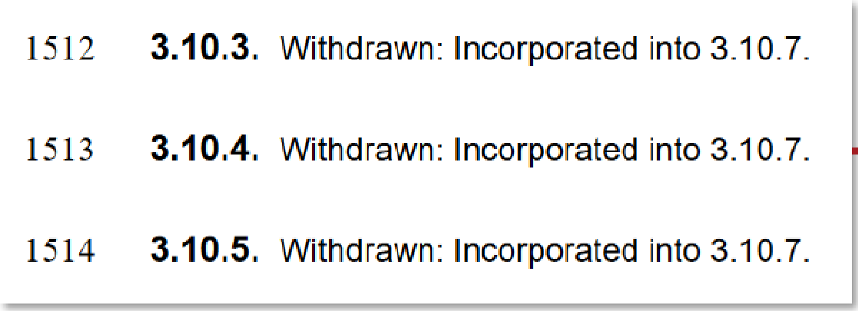
a. Enforce physical access authorizations at [*Assignment: organization-defined entry and exit points to the facility where the system resides*] by:

1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress and egress to the facility using [*Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards*].

b. Maintain physical access audit logs for [*Assignment: organization-defined entry or exit points*].

c. Escort visitors and control visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity*].

d. Secure keys, combinations, and other physical access devices.



3.10.3. Withdrawn: Incorporated into 3.10.7.

3.10.4. Withdrawn: Incorporated into 3.10.7.

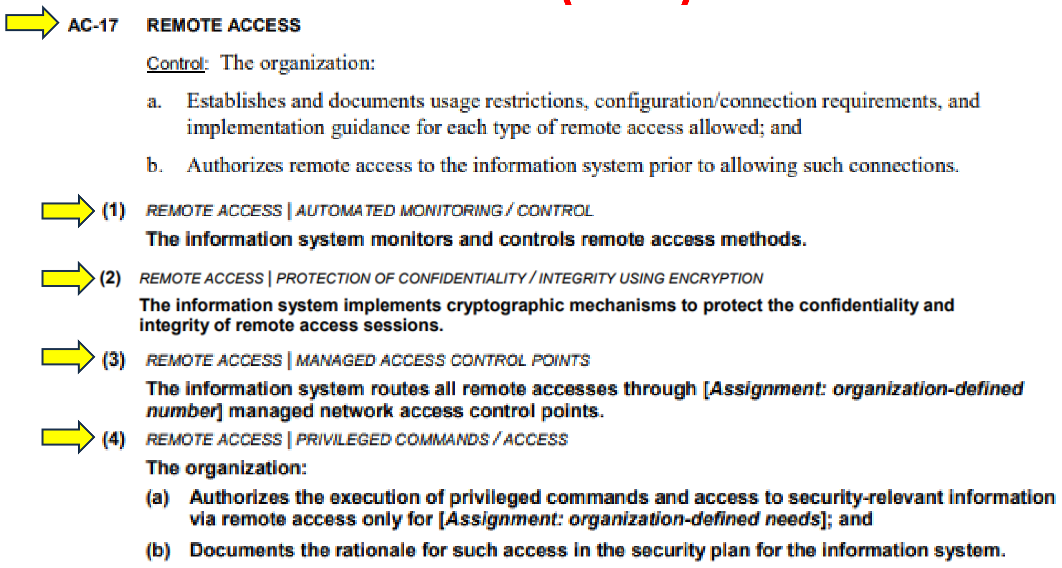
3.10.5. Withdrawn: Incorporated into 3.10.7.

Sponsored by:

Phantom Decreases

- **Most “withdrawn” requirements simply arrange 800-53 control elements according to 800-53 catalog formatting & hierarchy rather than representing as independent requirements in 171r2**

800-53r4 **(WAS)**



AC-17 REMOTE ACCESS

Control: The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorizes remote access to the information system prior to allowing such connections.

(1) *REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*

The information system monitors and controls remote access methods.

(2) *REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

(3) *REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*

The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

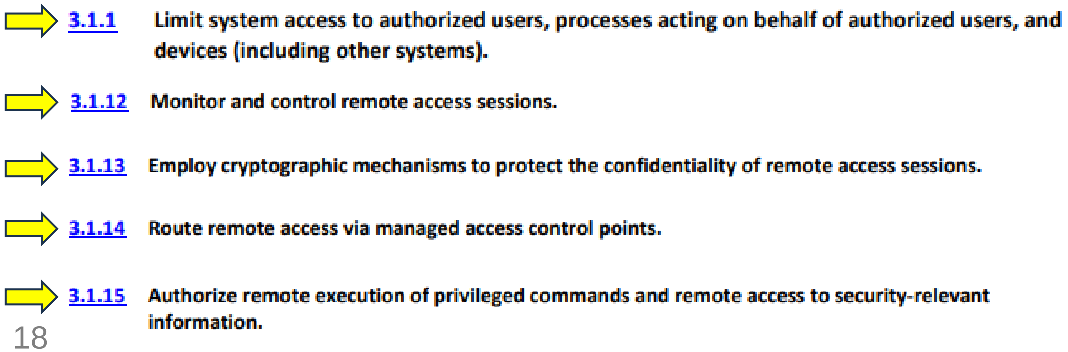
(4) *REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*

The organization:

(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and

(b) Documents the rationale for such access in the security plan for the information system.

800-171r2 **(IS)**



3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

3.1.12 Monitor and control remote access sessions.

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

3.1.14 Route remote access via managed access control points.

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

Sponsored by:

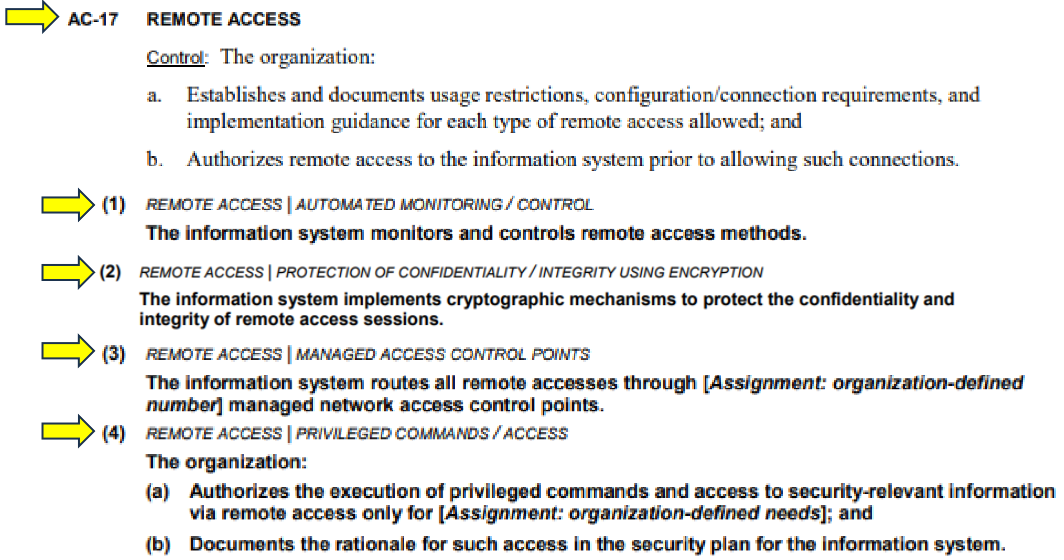
C3 INTEGRATED SOLUTIONS

Phantom Decreases

NDIA

- **800-53 controls have multiple "enhancements" which provides a general approach to sequencing implementation that 800-171r2 formatting obscured**

800-53r4 **(WAS)**



AC-17 REMOTE ACCESS

Control: The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorizes remote access to the information system prior to allowing such connections.

(1) *REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*

The information system monitors and controls remote access methods.

(2) *REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

(3) *REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*

The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

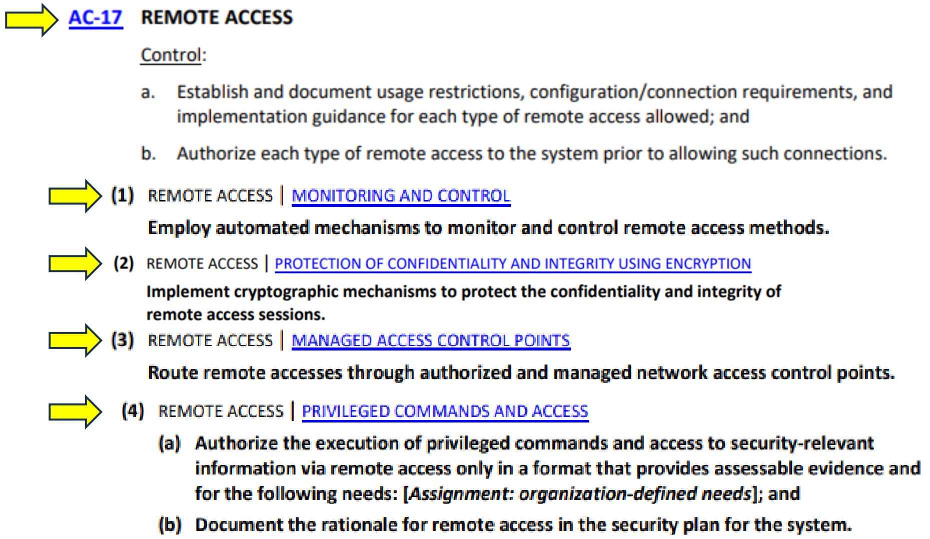
(4) *REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*

The organization:

(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and

(b) Documents the rationale for such access in the security plan for the information system.

800-53r5 **(IS)**



AC-17 REMOTE ACCESS

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

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

(1) REMOTE ACCESS | MONITORING AND CONTROL

Employ automated mechanisms to monitor and control remote access methods.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

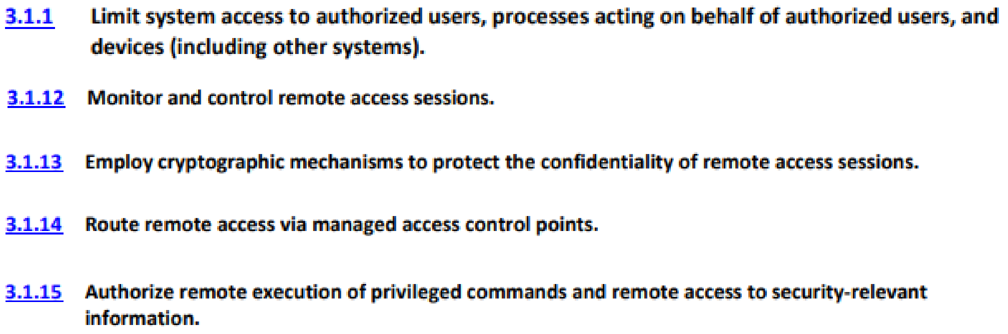
Route remote accesses through authorized and managed network access control points.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [*Assignment: organization-defined needs*]; and

(b) Document the rationale for remote access in the security plan for the system.

800-171r2 **(IS)**



3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

3.1.12 Monitor and control remote access sessions.

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

3.1.14 Route remote access via managed access control points.

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

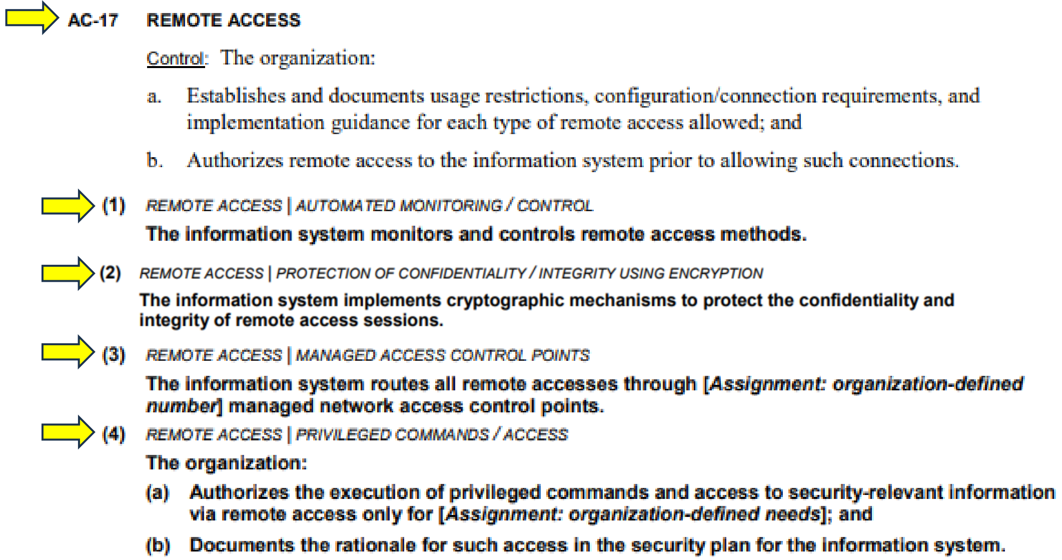
Sponsored by:

C3 INTEGRATED SOLUTIONS

Phantom Decreases

- Understanding what 800-171 is asking for, in which sequence, and how to anticipate future changes in 171r3 and beyond requires familiarity with 800-53; it's an extremely valuable reference

800-53r4 **(WAS)**



AC-17 REMOTE ACCESS

Control: The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorizes remote access to the information system prior to allowing such connections.

(1) *REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*

The information system monitors and controls remote access methods.

(2) *REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

(3) *REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*

The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

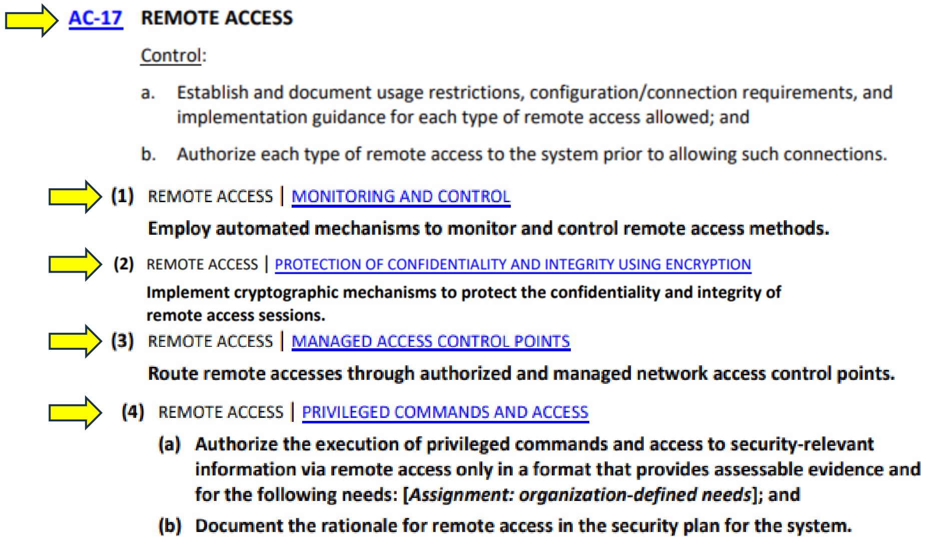
(4) *REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*

The organization:

(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and

(b) Documents the rationale for such access in the security plan for the information system.

800-53r5 **(IS)**



AC-17 REMOTE ACCESS

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

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

(1) REMOTE ACCESS | MONITORING AND CONTROL

Employ automated mechanisms to monitor and control remote access methods.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

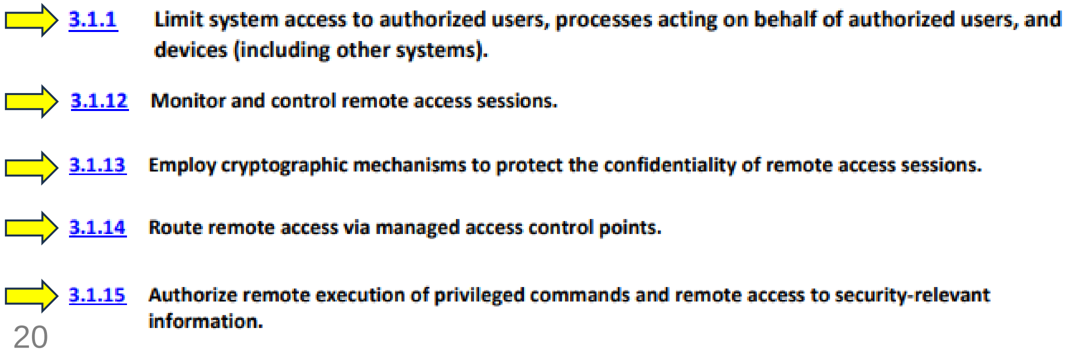
Route remote accesses through authorized and managed network access control points.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [*Assignment: organization-defined needs*]; and

(b) Document the rationale for remote access in the security plan for the system.

800-171r2 **(IS)**



3.1.1 **Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).**

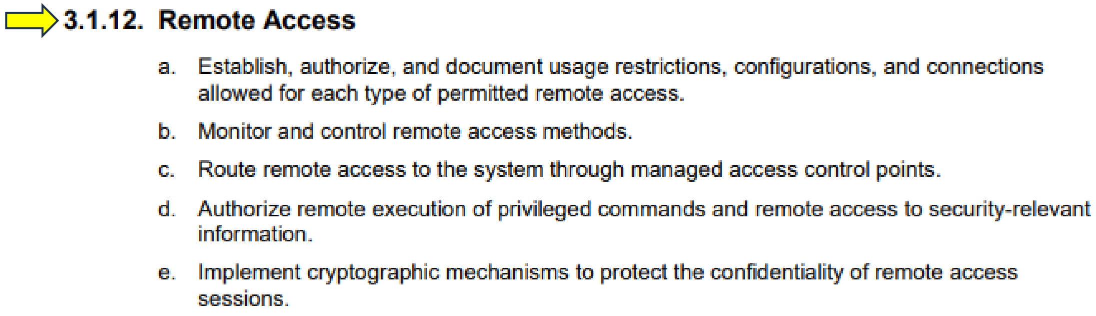
3.1.12 **Monitor and control remote access sessions.**

3.1.13 **Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.**

3.1.14 **Route remote access via managed access control points.**

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

171r3 IPD **(WILL BE)**



3.1.12. Remote Access

a. Establish, authorize, and document usage restrictions, configurations, and connections allowed for each type of permitted remote access.

b. Monitor and control remote access methods.

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

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

e. Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

Secure Your Networks and Systems In Physical Space and Cyberspace

NDIA

- Secure your Networks. Now
- Know your contracts
- Know your business processes
  - Cybersecurity is an operational imperative, not an IT problem
- Based on your contracts and processes, implement the biggest impact/biggest value solutions
- ISO 27001 Certification?
- Comments on R3? membership@ndia.org by 4 July for consolidation prior to the 14 July deadline

Sponsored by:

C3 INTEGRATED SOLUTIONS

Questions?

Sponsored by: