WHITEPAPER

Redspin
A Division of Clearwater

Exposed: The Hidden Changes in NIST SP 800-171 Rev 3 That Will Transform Your Cybersecurity Strategy

The National Institute of Standards and Technology (NIST) Special Publication 800-171 undergoes periodic revisions to adapt to the evolving cybersecurity landscape. The transition from Revision 2 (r2) to Revision 3 (r3) of NIST 800-171 reflects an ongoing effort to strengthen the protection of Controlled Unclassified Information (CUI) in non-federal systems and organizations. This white paper delves into the key factors driving these changes, providing context and rationale for the updates.

Background of NIST 800-171 Revisions

NIST 800-171 r2, established as a guideline for safeguarding CUI, was rooted in the cybersecurity best practices and compliance requirements relevant to its time of publication. However, the dynamic nature of cyber threats necessitates continuous adaptation of security protocols. The emergence of sophisticated cyberattacks, evolving technology landscapes, and the increasing complexity of information systems underscored the need for an updated framework.

Overall Analysis

Revision 3 of NIST 800-171 introduces significant changes, including but not limited to, enhanced requirements for cryptography, a more restrictive framework for software usage policies, mandatory Multi-Factor Authentication (MFA) for all system accounts, the introduction of supply chain risk management, and a greater emphasis on the documentation and location of information.

The updates reflect a more comprehensive approach to cybersecurity, addressing both technical and procedural aspects of information security in a manner that is consistent with real-time threats. Ultimately, these changes were guided by different – yet, equally compelling – motivations, including:

Redspin, an early adopter working with Cyber-AB to help define the program is the first Authorized CMMC C3PAO and is a RPO.

1. **Advanced Cybersecurity Threats:** The increasing sophistication of cyber threats, including advanced persistent threats (APTs), ransomware, and insider threats, has made the existing guidelines in r2 less effective against newer attack vectors.

2. **Technological Advancements:** The rapid advancement of technology, particularly in cloud computing, artificial intelligence, and the Internet of Things (IoT), demanded an update in the standards to accommodate these emerging areas.

3. **Alignment with NIST SP 800-53 Rev. 5:** Revision 3 was developed in parallel with NIST SP 800-53 Rev. 5 to ensure a harmonized approach to information security across federal and non-federal entities.

4. **Feedback from Stakeholders:** Input from industry professionals, cybersecurity experts, and organizations implementing r2 highlighted areas for improvement, prompting updates to make the guidelines more practical and effective.

5. **Regulatory and Compliance Landscape:** Changes in federal regulations and compliance requirements necessitated an update to ensure that NIST 800-171 remains relevant and effective in meeting legal and contractual obligations.

Overall, these updates provide more meaningful protections, and are addressed through:

Cryptography and Flexibility in CUI Protection

- **New Cryptographic Requirements:** Revision 3 introduces updated cryptographic standards for the protection of CUI. These changes address the evolving cryptographic landscape, including quantum computing threats and the need for more robust encryption methods.

- **Flexibility in Implementation:** The new revision offers greater flexibility in implementing cryptographic controls, allowing organizations to tailor solutions based on their specific security needs and technological capabilities.

Software Usage Policies and Restrictive Framework

- **More Restrictive Software Policies:** Update enforces stricter control over software usage, mandating organizations to adopt more restrictive policies. This includes tighter controls over the installation, usage, and maintenance of software, especially those that process or store CUI.

- **Compliance Requirements:** The revision stipulates comprehensive documentation and approval processes for software, emphasizing the need for regular audits and compliance checks.

Mandatory MFA for All System Accounts

- **MFA Mandate:** One of the most notable changes is the mandatory implementation of Multi-Factor Authentication (MFA) across all system accounts, not just for privileged users. This measure significantly enhances security by adding an extra layer of authentication.

- **Impact on Access Control:** This change emphasizes the importance of robust access control mechanisms and is likely to impact *how* organizations manage user authentication and identity verification processes

Introduction of Supply Chain Risk Management

- **Supply Chain Security:** The new version introduces requirements for managing risks in the supply chain, acknowledging the growing threat posed by third-party vendors and partners.

- **Risk Assessment and Mitigation:** Organizations are required to assess and mitigate risks associated with their supply chains, ensuring that external entities handling CUI adhere to the same security standards.

Emphasis on Information Location and Documentation

- **Information Location:** The new revision places greater emphasis on understanding and documenting the location of CUI within an organization's systems. This includes both *physical* and *virtual* locations.

- **Documentation:** Clear and thorough documentation of where CUI resides and how it is protected becomes essential, aiding in risk management and compliance efforts.

Formalizing Cybersecurity Policies Review

- **Review and Dissemination:** Revision 3 formalizes the process for reviewing and disseminating cybersecurity policies. This includes regular updates, ensuring that policies reflect the current cybersecurity environment and compliance requirements.

- **Stakeholder Involvement:** The process encourages greater involvement of stakeholders in policy development and review, promoting a culture of cybersecurity awareness and compliance.

Independent Assessments and Control Tailoring

- **Independent Assessments:** The revision emphasizes the importance of independent assessments to validate the effectiveness of security controls, especially those related to CUI protection.

- **Tailoring:** Organizations are guided to tailor controls based on their specific environments, risks, and business needs, allowing for more effective and efficient implementation of security measures.

These changes collectively encourage a more adaptive and comprehensive approach to cybersecurity, taking into account the latest trends, evolving threats, and the increasingly more sophisticated tactics, techniques, and procedures employed by foreign adversaries and actors. The result is a far more robust and proactive system of cybersecurity controls.

Now we'll delve more deeply into specific updates and how they may impact your cybersecurity strategy.

Specific Changes to Control Families and Objectives

Change, especially as it pertains to compliance and security, can often seem daunting. Organizations might view these updates as additional hurdles, potentially impacting business operations or contract status. However, it's important to recognize that these changes are not just procedural in nature; they're intended to foster a much more robust cybersecurity culture. More specifically, they challenge organizations to move beyond the checkbox compliance mentality and urge them to implement security measures that are genuinely effective and tailored to their specific needs and risks.

By focusing on meaningful implementation, organizations are not just protecting themselves; they are contributing to the overall security of the supply chain and, by extension, national security.

Let's first consider the need for advancements in Access Control.

Access Control

Access Control refers to the policies and procedures designed to manage and monitor who can access and use information and information systems. It focuses on ensuring that only authorized individuals have access to controlled unclassified information (CUI) and that their interactions with this information are appropriate and secure. This involves safeguarding against unauthorized access and protecting the confidentiality and integrity of the information.

What are Impacts to the Domain and Practices?

Revision 3 of NIST 800-171 contains several noteworthy updates to Access Control practices.

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

Status: Withdrawn and incorporated into 3.1.12 "Remote Access"

Objectives for 3.1.12 Remote Access:

- Establish usage, configuration, and connection requirements for remote system access.
- Authorize remote system access before connection.
- Route remote access through authorized and managed access control points.
- Authorize remote execution of privileged commands and access to security-relevant information.

3.1.14 “Route remote access via managed access control points.”

Status: Withdrawn and incorporated into 3.1.12 “Remote Access”

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

Status: Incorporated into 3.1.12 “Remote Access”

3.1.17 “Protect wireless access using authentication and encryption.”

Status: Withdrawn and incorporated into 3.1.16 “Wireless Access”

Objectives for 3.1.16 Wireless Access:

- Establish usage, configuration, and connection requirements for wireless access.
- Authorize wireless access before connection.
- Disable wireless networking capabilities when not in use.

3.1.19 “Access Control for Mobile Devices.”

Status: Incorporated into 3.1.18 “Access Control for Mobile Devices”

Objectives for 3.1.18 “Access Control for Mobile Devices:

- Establish usage, configuration, and connection requirements for mobile devices.
- Authorize the connection of mobile devices to the system.
- Implement encryption to protect the confidentiality of CUI on mobile devices.

3.1.21 “Limit use of portable storage devices on external systems.”

Status: Incorporated into 3.1.20 “Use of External Systems”

Objectives for 3.1.20 “Use of External Systems”:

- Prohibit unauthorized use of external systems.
- Establish terms, conditions, and security requirements for external systems.

- Verify security requirements on external systems before access.
- Restrict the use of portable storage devices on external systems.

Next, we'll take a look at how Awareness Training practices are redefined in Revision 3 of NIST 800-171.

Awareness and Training

Awareness and Training ensures that all personnel are aware of the security risks associated with their activities and the applicable policies, standards, and procedures related to the security of controlled unclassified information (CUI). The focus is on training staff to recognize and respond to security threats and incidents, thereby enhancing the overall security posture of the organization. This involves regular and effective training to keep employees informed about security best practices and their roles in maintaining organizational security.

What are Impacts to the Domain and Practices?

3.2.3 "Provide security awareness training on recognizing and reporting potential indicators of insider threat."

Status: Incorporated into: 03.02.01 "Role-Based Training"

03.02.01 Role Based Training Objectives include,

- Provide role-based security training to organizational personnel:
- Before authorizing access to the system or CUI, before performing assigned duties, and periodically thereafter.
- When required by system changes or following organization-defined events.
- Update role-based training.

Audit and Accountability

Audit and Accountability involves the practices for creating, protecting, and retaining system logs to provide a record of system activity. This includes monitoring, analyzing, and reporting on user activities, especially those that could affect security or involve access to sensitive data. The focus is on ensuring that actions taken on critical systems can be uniquely traced to an individual, providing a way to hold users accountable for their actions, and detecting and investigating potential security incidents. Robust audit and accountability measures are crucial for maintaining the integrity and security of information systems.

The Audit and Accountability domain also includes several noteworthy changes in Revision 3 of NIST 800-171.

What are Impacts to the Domain and Practices?

3.3.9 "Limit management of audit logging functionality to a subset of privileged users."

Status: Incorporated into: 03.03.08, "Protection of Audit Information"

03.03.08 Protection of Audit Information Objectives include:

- Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
- Authorize access to management of audit logging functionality to only a subset of privileged users or roles.

Another important domain, Configuration Management, also warrants review.

Configuration Management

Configuration Management entails the management and control of information system configurations. It includes establishing baselines and a structured process for systematically managing system changes to maintain system integrity over time. The focus is on ensuring that systems operate securely and as intended, and that unauthorized changes are prevented or detected. This involves keeping an inventory of system components, enforcing security configuration settings, and regularly reviewing and updating configurations to address vulnerabilities and enhance security.

What are Impacts to the Domain and Practices?

3.4.7 “Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.”

Status: Incorporated into: 03.04.06, “Least Functionality”

03.04.06 Least Functionality Objectives:

- Configure the system to provide only mission-essential capabilities.
- Prohibit or restrict use of organization-defined functions, ports, protocols, connections, and services.
- Review the system periodically to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.
- Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.

3.4.9 “Control and monitor user-installed software.”

Status: Addressed by: 03.01.05, 03.01.06 “Least Functionality – Privileged Accounts”, 03.01.07, “Least Privilege – Privileged Functions”, and 03.04.08, “Authorized Software – Allow by Exception”.

Identification and Authentication

Identification and Authentication are fundamental concepts in security systems, ensuring that only authorized individuals gain access to resources. Identification involves presenting an identity, like a username, to claim who you are. Authentication follows this by verifying the identity claim, often through methods like passwords, biometric data, or security tokens. Together, these processes establish and confirm user identities, forming the basis for secure access and interactions in digital environments.

Revision 3 provides some useful updates to the Identification and Authentication domain as well.

What are Impacts to the Domain and Practices?

3.5.6. “Disable identifiers after a defined period of inactivity.”

Status: Withdrawn

3.5.8. “Prohibit password reuse for a specified number of generations.”

Status: Withdrawn

3.5.9. “Allow temporary password use for system logons with an immediate change to a permanent password.”

Status: Withdrawn, incorporated into 03.05.07, “Password Management”

03.05.07, “Password Management” Objectives:

- Maintain a list of commonly-used, expected, or compromised passwords and update the list periodically.
- Verify that passwords are not found on the list of commonly-used, expected, or compromised passwords when users create or update passwords.
- Transmit passwords only over cryptographically-protected channels.
- Store passwords in a cryptographically-protected form.
- Select a new password upon first use after account recovery.
- Enforce organization-defined composition and complexity rules for passwords.

3.5.10. “Store and transmit only cryptographically-protected passwords.”

Status: Incorporated into: 03.05.07, “Password Management”

03.05.07, “Password Management” Objectives:

- Maintain a list of commonly-used, expected, or compromised passwords and update the list periodically.
- Verify that passwords are not found on the list of commonly-used, expected, or compromised passwords when users create or update passwords.
- Transmit passwords only over cryptographically-protected channels.
- Store passwords in a cryptographically-protected form.
- Select a new password upon first use after account recovery.
- Enforce organization-defined composition and complexity rules for passwords.

Maintenance

Maintenance, as outlined in NIST 800-171, refers to the processes and controls necessary to

ensure the upkeep and effective operation of information systems. It encompasses regular updates, repairs, and modifications to hardware and software to address security vulnerabilities and operational inefficiencies. This maintenance is guided by policies that prioritize the protection of sensitive data and compliance with security standards. The goal is to sustain the integrity, availability, and confidentiality of information systems, crucial for safeguarding against threats and maintaining compliance in secure environments.

What are Impacts to the Domain and Practices?

3.7.1. "Perform maintenance on organizational systems."

Status: Recategorized as an NCO

3.7.2. "Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance."

Status: Incorporated into: 03.07.04, "Maintenance Tools" and 03.07.06, "Maintenance Personnel"

03.07.04, "Maintenance Tools" Objectives includes:

- Approve, control, and monitor the use of system maintenance tools.
- Inspect the maintenance tools for improper or unauthorized modifications.
- Check media containing diagnostic and test programs for malicious code before use.
- Prevent the removal of system maintenance equipment containing CUI by verifying no CUI is present, sanitizing or destroying the equipment, or retaining the equipment within the facility.

03.07.06 "Maintenance Personnel" objectives include,

a. Establish a process for maintenance personnel authorization.
b. Maintain a list of authorized maintenance organizations or personnel.
c. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.
d. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations

3.7.3. "Ensure equipment removed for off-site maintenance is sanitized of any CUI."

Status: Incorporated into: 03.08.03, "Media Sanitization"

03.08.03, "Media Sanitization" Objectives include:

Sanitize system media containing CUI prior to disposal, release out of organizational control, or release for reuse.

Media Protection

Media Protection, in the context of NIST 800-171, involves implementing measures to safeguard digital and physical media containing sensitive information. This includes policies and procedures for handling, storing, and disposing of media such as hard drives, USB drives, and paper records. The aim is to prevent unauthorized access, alteration, and distribution of the data. Media protection strategies often encompass encryption, access controls, and secure destruction methods. It's essential for maintaining the confidentiality and integrity of information, especially in environments dealing with classified or proprietary data.

What are Impacts to the Domain and Practices?

3.8.6 "Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport."

Status: Withdrawn and incorporated into 03.08.05, "Media Transport"

03.08.05, "Media Transport" Objectives include:

- Protect and control system media containing CUI during transport outside of controlled areas.
- Maintain accountability of system media containing CUI during transport.

3.8.8 "Prohibit the use of portable storage devices when such devices have no identifiable owner."

Status: Incorporated into: 03.08.07, Media Use

03.08.07, Media Use Objectives include:

- Restrict or prohibit the use of organization-defined types of system media.
- Prohibit the use of removable system media without an identifiable owner.

Physical Protection

Physical Protection, as addressed in NIST 800-171, focuses on safeguarding physical facilities and resources that house sensitive information systems. This includes controlling access to buildings, rooms, and data centers, and implementing measures to protect against environmental hazards and unauthorized physical access. The goal is to prevent damage, theft, or compromise of physical assets and the data they contain. This involves a combination of security personnel, surveillance systems, locks, and barriers. Effective physical protection is crucial for ensuring the overall security and integrity of information systems.

What are Impacts to the Domain and Practices?

3.10.3. "Escort visitors and monitor visitor activity."

Status: Incorporated into: 3.10.07 Physical Access Control

3.10.07 Physical Access Control Objectives include:

- Control physical access at the location where the system resides by verifying individual physical access authorizations and controlling ingress and egress.
- Maintain physical access audit logs for entry or exit points.
- Escort visitors and control visitor activity under organization-defined circumstances.
- Secure keys, combinations, and other physical access devices.

3.10.4. “Maintain audit logs of physical access.”

Status: Incorporated into: 3.10.07 Physical Access Control

3.10.07 Physical Access Control Objectives include:

- Control physical access at the location where the system resides by verifying individual physical access authorizations and controlling ingress and egress.
- Maintain physical access audit logs for entry or exit points.
- Escort visitors and control visitor activity under organization-defined circumstances.
- Secure keys, combinations, and other physical access devices.

3.10.5. “Control and manage physical access devices.”

Status: Incorporated into: 3.10.07 Physical Access Control

3.10.07 Physical Access Control Objectives include:

- Control physical access at the location where the system resides by verifying individual physical access authorizations and controlling ingress and egress.
- Maintain physical access audit logs for entry or exit points.
- Escort visitors and control visitor activity under organization-defined circumstances.
- Secure keys, combinations, and other physical access devices.

3.10.6 “Alternate Work Sites”

Status: NEW

Includes the following Objectives:

- Determine alternate work sites allowed for use by employees.
- Employ organization-defined security requirements at alternate work sites.

Note: Includes private residences and other facilities designated by the organization.

Risk Assessment

Risk Assessment is the systematic process of identifying, analyzing, and evaluating risks associated with information systems and their environments. This involves understanding potential threats and vulnerabilities and assessing the impact of potential security incidents.

The aim is to prioritize risks based on their likelihood and impact, guiding the development of strategies to mitigate or manage these risks effectively. This process is crucial for making informed decisions about security measures, ensuring the protection of data, and maintaining the overall health and resilience of information systems.

What are Impacts to the Domain and Practices?

3.11.3 "Remediate vulnerabilities in accordance with risk assessments."

Status: Incorporated into: 03.11.02, "Vulnerability Monitoring and Scanning"

03.11.02, "Vulnerability Monitoring and Scanning" Objectives include:

- Monitor and scan for vulnerabilities in the system periodically and when new vulnerabilities are identified.
- Remediate system vulnerabilities within organization-defined response times.
- Update system vulnerabilities to be scanned periodically and when new vulnerabilities are identified and reported.

Security Assessment

Security Assessment involves a thorough evaluation of an organization's information systems to determine the effectiveness of security measures in place. This process includes reviewing security controls, policies, and procedures to identify vulnerabilities and weaknesses. The goal is to ensure that security measures adequately protect data and resources against threats and comply with regulatory standards. It often involves testing, analysis, and documentation of security practices, leading to recommendations for improvement. Regular security assessments are crucial for maintaining a robust security posture and adapting to evolving cyber threats.

What are Impacts to the Domain and Practices?

3.12.4, "Develop, document, and periodically update system security plans."

Status: Incorporated into: 3.15.02, "System Security Plan"

3.15.02, "System Security Plan" Objectives include:

a. Develop a system security plan that:

1. Defines the constituent system components;
2. Describes the system operating environment;
3. Describes specific threats to the system that are of concern to the organization;
4. Provides an overview of the security requirements for the system;
5. Identifies connections to other systems;
6. Identifies individuals that fulfill system roles and responsibilities; and
7. Includes other relevant information necessary for the protection of CUI.

b. Review and update the system security plan periodically.

c. Protect the system security plan from unauthorized disclosure

Systems and Communications Protection

Systems and Communications Protection involves implementing measures to safeguard information in networked systems and during data transmission. This includes deploying security controls like firewalls, encryption, and intrusion detection systems to prevent unauthorized access, data breaches, and interception. The focus is on maintaining the integrity and confidentiality of data as it is processed, stored, and communicated. This protection is essential for ensuring that information remains secure from external and internal threats, and for preserving the trustworthiness and reliability of communication channels and information systems.

Impacts to the Domain and Practices

3.13.2 "Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems"

Status: Withdrawn and recategorized as an NCO

3.13.3 "Separate user functionality from system management functionality. "

Status: Withdrawn, addressed by 03.01.01, 03.01.02, 03.01.03, 03.01.04, 03.01.05, 03.01.06, 03.01.07.

03.01.01 Account Management objectives include,

a. Define the types of system accounts allowed and prohibited.
b. Create, enable, modify, disable, and remove system accounts in accordance with organizational 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 system accounts.
f. Disable system accounts when:
    a. The accounts have expired;
    b. The accounts have been inactive for [Assignment: organization-defined time period];
    c. The accounts are no longer associated with a user or individual;
    d. The accounts are in violation of organizational policy; or
    e. Significant risks associated with individuals are discovered.
g. Notify organizational personnel or roles when:
    a. Accounts are no longer required;

b. Users are terminated or transferred; and 159 3. System usage or need-to-know changes for an individual.

03.01.02 Access Enforcement requires that organizations,
Enforce approved authorizations for logical access to CUI and system resources.

03.01.03 Information Flow Enforcement requires that organizations,
Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.

03.01.04 Separation of Duties includes the following objectives,

a. Identify the duties of individuals requiring separation.
b. Define system access authorizations to support separation of duties

03.01.05 Least Privilege includes the following,

a. Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.
b. Authorize access to [Assignment: organization-defined security functions and security relevant information].
c. Review the privileges assigned to roles or classes of users periodically to validate the need for such privileges.
d. Reassign or remove privileges, as necessary.

03.01.06 Least Privilege: Privileged Accounts includes the following objectives,

a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].
b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing nonsecurity functions or nonsecurity information.

03.01.07 Least Privilege: Privileged Functions includes the following objectives,

a. Prevent non-privileged users from executing privileged functions.
b. Log the execution of privileged functions

3.13.5. “Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks “

Status: incorporated into 3.13.01. Boundary Protection.

3.13.01 Boundary Protection incorporates the following objectives,

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.
b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
c. Connect to external systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture

3.13.7. “Prevent remote devices from simultaneously establishing non-remote connections with

organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling) “

Status: Withdrawn, addressed by 03.01.12 “Remote Access”, 03.04.02 “Configuration Settings” and 03.04.06 “Least Functionality.”

3.1.12 Remote Access requires,

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

3.4.2 Configuration Settings requires,

a. Establish, document, and implement the following configuration settings for the system that 791 reflect the most restrictive mode consistent with operational requirements: [Assignment: 792 organization-defined configuration settings].
b. Identify, document, and approve any deviations from established configuration settings.

3.4.6 Least Functionality

a. Configure the system to provide only mission-essential capabilities.
b. Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services].
c. Review the system periodically to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.
d. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.

3.13.14. “Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. “

Status: Withdrawn with the note “Technology Specific”

3.13.16. ” Protect the confidentiality of CUI at rest.”

Status: Withdrawn, incorporated into 3.13.08 Transmission and Storage Confidentiality.

3.13.08 Transmission and Storage Confidentiality requires the organization to Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage

Systems and Information Integrity

Systems and Information Integrity refers to the measures and practices aimed at ensuring the accuracy and reliability of information and the proper functioning of systems. This involves protecting against unauthorized changes, data corruption, and loss. It encompasses the implementation of software updates, virus protection, and intrusion detection systems, as well as regular monitoring for anomalies and security breaches. The objective is to maintain the trustworthiness of information and systems, ensuring they operate as intended and that data remains consistent, accurate, and accessible when needed. This integrity is vital for the overall security and effectiveness of information systems.

Impacts to the Domain and Practices

3.14.4 “Update malicious code protection mechanisms when new releases are available “ and

3.14.5 “Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed. “

Status: Withdrawn, addressed in 3.14.2 “Malicious Code Protection.

3.14.2 “Malicious Code Protection” is comprised of the following objectives,

a. Implement malicious code protection mechanisms at designated locations within the system to detect and eradicate malicious code.
b. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policy and procedures.
c. Configure malicious code protection mechanisms to:
    1. Perform scans of the system [Assignment: organization-defined frequency] and real time scans of files from external sources at endpoints or network entry and exit points as the files are downloaded, opened, or executed; and
    2. Block malicious code, quarantine malicious code, or take other actions in response to malicious code detection.

3.14.7 “Identify unauthorized use of organizational systems. withdrawn,”

Status: withdrawn, incorporated into 3.14.06 System Monitoring is comprised of the following objectives,

a. Monitor the system to detect:
    1. Attacks and indicators of potential attacks; and
    2. Unauthorized connections.
b. Identify unauthorized use of the system.
c. Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.

Revision 3 of NIST 800-171 adds multiple new domains that we describe in the next few sections.

3.15 Planning (NEW)3.15.1 Policy and Procedures

Status: NEW

Includes the following objectives,

a. Develop, document, and disseminate to organizational personnel or roles, policies and 2018 procedures needed to implement security requirements
b. Review and update policies and procedures periodically.

3.15.2 System Security Plan

Status: NEW

Includes the following objectives,

a. Develop a system security plan that: 2035
    a. Defines the constituent system components;
    b. Describes the system operating environment;
    c. Describes specific threats to the system that are of concern to the organization;
    d. Provides an overview of the security requirements for the system;
    e. Identifies connections to other systems;
    f. Identifies individuals that fulfill system roles and responsibilities; and
    g. Includes other relevant information necessary for the protection of CUI. 2042
b. Review and update the system security plan periodically.
c. Protect the system security plan from unauthorized disclosure

3.15.3 Rules of Behavior

Status: NEW

Includes the following objectives,

a. Establish and provide to individuals requiring access to the system, rules that describe their responsibilities and expected behavior for handling CUI and system usage.
b. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.
c. Review and update the rules of behavior periodically.

3.16 System and Service Acquisition (NEW)

3.16.1 Acquisition Process

Status: NEW

Include the following security requirements, explicitly or by reference, in the acquisition contract for the system, system component, or system service: [Assignment: organization-defined security requirements].

3.16.2 Unsupported System Components

Status: NEW

Requires that organizations,

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.
b. Provide options for risk mitigation or alternative sources for continued support for 2099 unsupported components if components cannot be replaced

3.16.3 External System Services

Status: NEW

a. Require the providers of external system services used for the processing, storage, or transmission of CUI, to comply with the following security requirements: [Assignment: organization-defined security requirements].
b. Define and document user roles and responsibilities with regard to external system services including shared responsibilities with external providers.
c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.

3.17 Supply Chain Risk Management (NEW)

3.17.1 Supply Chain Risk Management

Status: NEW

Includes,

a. Develop a plan for managing supply chain risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.
b. Review and update the supply chain risk management plan periodically.
c. Protect the supply chain risk management plan from unauthorized disclosure

3.17.2 Acquisition Strategies, Tools, and Methods

Status: NEW

Includes,
Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.

3.17.3 Supply Chain Requirements and Processes

Status: NEW

Includes,

a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.
b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined security requirements

Tailoring

Tailoring allows organizations to implement security controls in a manner that is both effective and efficient, while still maintaining the security of CUI in accordance with federal requirements. This approach recognizes that a one-size-fits-all model is not effective for information security, and that organizations have different environments, capabilities, and risk tolerances.
In NIST SP 800-171 Revision 3, "tailoring" refers to the updated criteria that have been introduced to adjust the security requirements and controls. This update is part of a series of significant changes in this revision, which include:

1. **Updates to Security Requirements:** Aligning with the updates in NIST SP 800-53, Revision 5, and the NIST SP 800-53B moderate control baseline.
2. **Updated Tailoring Criteria:** This specifically refers to the modifications made to adapt the security requirements to various scenarios.
3. **Increased Specificity in Security Requirements:** Enhancing the clarity and effectiveness of implementation and assessment scopes.
4. **Introduction of Organization-Defined Parameters (ODP):** These parameters are introduced in selected security requirements to enhance flexibility and assist organizations in better risk management.

The following tailoring categories have been defined.

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.

N/A: The control is not applicable.

CUI: The control is directly related to protecting the confidentiality of CUI

How do the NIST 800-171 rev 3 changes impact organizations?

1. Organizations Beginning Compliance Journey: For organizations new to the NIST controls and facing the transition from NIST 800-171 r2 to NIST 800-171 r3, the process can be challenging but manageable with the right approach. Organizations should start out by gaining a thorough understanding of the NIST security requirements, as well as the

assessment requirements for the Cybersecurity Maturity Model Certification (CMMC) rules. Initial steps may include conducting a comprehensive gap analysis to determine the current state of cybersecurity controls, their efficacy and efficiency. A gap analysis will not only help to isolate implementation issues, but it can also help an organization understand impacts and prioritization of these weaknesses. Adopting a phased approach to compliance, focusing on the most critical areas first, will make the process much more manageable.

At a high level, remember:

- **Newly added and modified controls** may require significant investment in cybersecurity infrastructure and training.
- **Withdrawn controls** might simplify compliance efforts, reducing the burden on resources for new adopters.
- The complexity of new controls might pose challenges, especially in terms of resources and technical expertise.
- Tailoring guidance in r3 can help SMEs focus on relevant controls, making compliance more manageable.

2. Organizations Already Compliant with NIST 800-171 r2: Organizations with experience in NIST assessments, and who are transitioning from NIST SP 800-171 revision 2 to NIST SP 800-171 revision 3 will need to update and refine their existing cybersecurity controls and measures. As these organizations already possess a foundational knowledge of the NIST standard, their focus will be on identifying and implementing specific r3 changes. The process should begin with a detailed comparative analysis, evaluating the 'current state' baseline with the 'to be implemented' baseline. Based on the new requirements, the organization may need to update their cybersecurity infrastructure,including hardware, software, and network configurations. Internal policy and procedural documents should be updated accordingly. Note that all proposed changes should be evaluated for their security impact, taking special measures not to introduce new vulnerabilities or risks.

- Transitioning to r3 will require a review and possible overhaul of existing cybersecurity practices.
- Adaptation to new controls might be more straightforward, given the existing foundation in cybersecurity practices.
- Withdrawn controls could lead to a reevaluation of current security measures and potential cost savings.
- These entities may already have advanced security measures, so adapting to new controls could be more seamless.
- The introduction of new controls, especially around supply chain risk management, might necessitate a broader review of security policies extending beyond the organization itself.

The transition from NIST SP 800-171 r2 to NIST SP 800-171 r3 marks a crucial and necessary evolution in cybersecurity standards. As digital threats, including those predicated by our foreign adversaries, become more sophisticated and pervasive, it's imperative for organizations to stay ahead in safeguarding our nation's critical information. The changes introduced not only address the emerging vulnerabilities and attack vectors, but they also align more closely with our technological landscape and regulatory environments. This revision ensures that

our cybersecurity measures do not stagnate; rather, that they adapt to new challenges while maintaining the integrity and confidentiality of controlled unclassified information. Embracing these changes are not just a compliance requirement; it's a strategic step towards fostering a more secure and resilient digital infrastructure.

WHY REDSPIN

- Over 100 security advisors and assessors, ready to scale with you as needed
- Possesses the know-how from performing over 1,000 assessments in highly regulated industries, including multiple Joint Surveillance Voluntary Assessment Program (JSVAP) assessments
- Uplifts its service offering to validate your security, giving you the confidence that your people, processes, and technology are effective
- Our team understands CMMC requirements and follows professional conduct to help you on your journey to becoming CMMC-ready and certified

Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies for the Defense Industrial Base. Our exclusive focus on tailoring our CMMC assessment, training, consulting, and managed services for each client delivers peace of mind by lowering the risk of a security incident or breach, and meeting/maintaining compliance regulations. Since our founding in 2001, we've become a thought leader in IT security, helped countless clients control their security risk, develop their security strategy, and avoid a breach headline.

Redspin
A Division of Clearwater

40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com