NIST Special Publication 800-171 Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations

Published February 2020 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Provide federal agencies with recommended security requirements for protecting the *confidentiality* of CUI

- When the CUI is resident in a non-federal system and organization
- When the non-federal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency and
- Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry

Applies to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components

- May limit the scope of the security requirements by isolating the designated system components in a separate CUI *security domain*

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations

Target Audience

- System development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators)
- Acquisition or procurement responsibilities (e.g., contracting officers)
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers) and
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts)

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations

Some Key Definitions

- **Controlled Unclassified Information:** Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended
- **Availability**: Ensuring timely and reliable access to and use of information
- **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **FIPS-Validated Cryptography**: A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP)
- **Firmware**: Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs
- **Sanitization**: Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means

  Also, Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations

Some More Key Definitions

- **Hardware:** The material physical components of a system
- **Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- **Security**: A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems
- **Security Control**: The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information
- **Security Functions**: The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based

"

Side Track –
"California Password Law"

California SB-327 aka "The California Password Law"

This law deals with the "Security of Connected Devices"

Some Key Terms

- Connected Device: Any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address
- Manufacturer: The person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California
- Security feature: A feature of a device designed to provide security for that device
- Unauthorized access, destruction, use, modification, or disclosure: Access, destruction, use, modification, or disclosure that is not authorized by the consumer

California SB-327 aka "The California Password Law" Key Requirements

A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

- Appropriate to the nature and function of the device
- Appropriate to the information it may collect, contain, or transmit.
- Designed to protect the device and any information contained therein from unauthorized Subject to all of the requirements of subdivision

If a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:

- **The preprogrammed password is unique to each device manufactured**
- **The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time**

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations

Structure

- Consists of 14 Security Requirements Families

Family	Family
Access Control	Media Protection
Awareness & Training	Personnel Security
Audit & Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification & Authentication	Security Assessment
Incident Response	System & Communications Protection
Maintenance	System & Information Integrity

- Each Requirements Family has Basic and Derived Security Requirements plus a 'Discussion' section

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Access Control

Basic Requirements

- Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)
- Limit system access to the types of transactions and functions that authorized users are permitted to execute

Derived Requirements

- Control the flow of CUI in accordance with approved authorizations
- Separate the duties of individuals to reduce the risk of malevolent activity without collusion
- Employ the principle of least privilege, including for specific security functions and privileged accounts
- Use non-privileged accounts or roles when accessing non-security functions
- Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs
- Limit unsuccessful logon attempts
- Provide privacy and security notices consistent with applicable CUI rules

Derived Requirements (cont)

- Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity
- Terminate (automatically) a user session after a defined condition
- Monitor and control remote access sessions
- Employ cryptographic mechanisms to protect the confidentiality of remote access sessions
- Route remote access via managed access control points
- Authorize remote execution of privileged commands and remote access to security-relevant information
- Authorize wireless access prior to allowing such connections
- Protect wireless access using authentication and encryption
- Control connection of mobile devices
- Encrypt CUI on mobile devices and mobile computing platforms
- Verify and control/limit connections to and use of external systems
- Limit use of portable storage devices on external systems
- Control CUI posted or processed on publicly accessible systems

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Awareness and Training

Basic Requirements

- Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems
- Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities

Derived Requirements

- Provide security awareness training on recognizing and reporting potential indicators of insider threat

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Audit and Accountability

Basic Requirements

- Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity
- Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions

Derived Requirements

- Review and update logged events
- Alert in the event of an audit logging process failure
- Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity
- Provide audit record reduction and report generation to support on-demand analysis and reporting
- Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records
- Protect audit information and audit logging tools from unauthorized access, modification, and deletion
- Limit management of audit logging functionality to a subset of privileged users

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Configuration Management

Basic Requirements

- Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles
- Establish and enforce security configuration settings for information technology products employed in organizational systems

Derived Requirements

- Track, review, approve or disapprove, and log changes to organizational systems
- Analyze the security impact of changes prior to implementation
- Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems
- Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities
- Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services
- Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- Control and monitor user-installed software

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Identification and Authentication

Basic Requirements

- Identify system users, processes acting on behalf of users, and devices
- Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems

Derived Requirements

- Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts
- Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts
- Prevent reuse of identifiers for a defined period
- Disable identifiers after a defined period of inactivity
- **Enforce a minimum password complexity and change of characters when new passwords are created**
- **Prohibit password reuse for a specified number of generations**
- **Allow temporary password use for system logons with an immediate change to a permanent password**
- **Store and transmit only cryptographically-protected passwords**
- Obscure feedback of authentication information

Incident Response

Basic Requirements

- Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities
- Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization

Derived Requirements

- Test the organizational incident response capability

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Maintenance

Basic Requirements

- Perform maintenance on organizational systems
- Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance

Derived Requirements

- Ensure equipment removed for off-site maintenance is sanitized of any CUI
- Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems
- Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete
- Supervise the maintenance activities of maintenance personnel without required access authorization

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Media Protection

Basic Requirements

- Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital
- Limit access to CUI on system media to authorized users
- Sanitize or destroy system media containing CUI before disposal or release for reuse
  - Sanitization techniques, **including clearing, purging, cryptographic erase, and destruction**, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal

Derived Requirements

- Mark media with necessary CUI markings and distribution limitations
- Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas
- Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards
- Control the use of removable media on system components
- Prohibit the use of portable storage devices when such devices have no identifiable owner
- Protect the confidentiality of backup CUI at storage locations

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Personnel Security

Basic Requirements

- Screen individuals prior to authorizing access to organizational systems containing CUI
- Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

Derived Requirements

None

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Physical Protection

Basic Requirements

- Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals
- Protect and monitor the physical facility and support infrastructure for organizational systems

Derived Requirements

- Escort visitors and monitor visitor activity
- Maintain audit logs of physical access
- Control and manage physical access devices
- Enforce safeguarding measures for CUI at alternate work sites

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
Risk Assessment

Basic Requirements

- Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI

Derived Requirements

- Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified
- Remediate vulnerabilities in accordance with risk assessments

Basic Requirements

- Periodically assess the security controls in organizational systems to determine if the controls are effective in their application
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems
- Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls
- Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems

Derived Requirements

None

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
System and Communications Protection

Basic Requirements

- Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems
- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems

Derived Requirements

- Separate user functionality from system management functionality
- Prevent unauthorized and unintended information transfer via shared system resources
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks
- Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception)
- 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)

NIST SP 800-171R2
Protecting Controlled Unclassified Information in Non-federal Systems and Organizations
System and Communications Protection

Derived Requirements (cont)

- Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards
- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity
- Establish and manage cryptographic keys for cryptography employed in organizational systems
- Employ FIPS-validated cryptography when used to protect the confidentiality of CUI
- Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device
- Control and monitor the use of mobile code
- Control and monitor the use of Voice over Internet Protocol (VoIP) technologies
- Protect the authenticity of communications sessions
- Protect the confidentiality of CUI at rest

Basic Requirements

- Identify, report, and correct system flaws in a timely manner
- Provide protection from malicious code at designated locations within organizational systems
- Monitor system security alerts and advisories and take action in response

Derived Requirements

- Update malicious code protection mechanisms when new releases are available
- Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed
- Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks
- Identify unauthorized use of organizational systems

Tailoring

Criteria for Tailoring

- The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government)
- The control or control enhancement is not directly related to protecting the confidentiality of CUI
- The control or control enhancement is expected to be routinely satisfied by non-federal organizations without specification

When is NIST SP 800-171R2 Required?

I have seen it worded in different ways, but essentially it is this:

Any organization that that **processes, stores or transmits CUI for the DoD, GSA or NASA, and other federal or state agencies, including subcontractors** must comply with NIST SP 800-171. It is recommended for other organizations that do not do business with federal or state agencies.

The issue I see is that the security controls and tailoring guidelines in NIST SP 800-171R2 are designed for organizations that do business with the government, and not for the doctor's office that has to comply with HIPAA laws.

NIST needs to develop a version of SP 800-171 tailored to small businesses that process, store or transmit CUI for non-government customers