NIST Special Publication (SP) 800-171r3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Initial Public Draft

NIST SP 800-171R3 IPD PURPOSE

Initial Public Draft Issued May 2023

Purpose is to:

- Provide federal agencies with recommended security 23 requirements for protecting the *confidentiality* of CUI:
  - When the CUI is resident in a nonfederal system and organization
  - When the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency
  - 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
- The security requirements in this publication are *only* applicable to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components
- Requirements are intended for use by federal agencies in contractual vehicles or other agreements that are established between those agencies and nonfederal organizations

NIST SP 800-171R3 IPD
Basic Asumptions

The recommended security requirements in this publication are based on the following assumptions:

- Federal information designated as CUI has the same value, whether such information resides in a federal or a nonfederal system or organization
- Statutory and regulatory requirements for the protection of CUI are consistent in federal and nonfederal systems and organizations
- Safeguards implemented to protect CUI are consistent in federal and nonfederal systems and organizations
- The confidentiality impact value for CUI is no less than *moderate*

NIST SP 800-171R3 IPD
Key Definitions

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

controlled unclassified information (CUI): 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

external system (or component): A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness

external system service: A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness

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

Hardware: The material physical components of a system

Incident: An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies

NIST SP 800-171R3 IPD
Key Definitions

information security: The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or 2843 destruction in order to provide confidentiality, integrity, and availability

integrity: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity

risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence

risk assessment: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system

Sanitization: Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means
Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs

system: a nonfederal system that processes, stores, or transmits CUI

Threat: Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

NIST SP 800-171R3 IPD
Security Requirements Families

Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response	Supply Chain Risk Management	

NIST SP 800-171R3 IPD Access Control

Account Management

- Define and document the types of system accounts allowed and prohibited
- Create, enable, modify, disable, and remove accounts in accordance with [*Assignment: organization-defined policy, procedures, prerequisites, and criteria*].
- Specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges)
- Authorize access to the system based on a valid access authorization and intended system usage
- Monitor the use of accounts
- Disable accounts of individuals within [*Assignment: organization-defined time period*] when the accounts:
  - Have expired;
  - Are no longer associated with a user or individual;
  - Are in violation of organizational policy; or
  - Have been inactive for [*Assignment: organization-defined time period*].
- Disable accounts of individuals within [*Assignment: organization-defined time period*] of discovery of [*Assignment: organization-defined significant risks*].
- Notify [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*]:
  - When accounts are no longer required;
  - When users are terminated or transferred; and
  - When system usage or need-to-know changes for an individual

NIST SP 800-171R3 IPD Access Control

Access Enforcement

- Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies

Flow Enforcement

- Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems

Separation of Duties

- Identify the duties of individuals requiring separation
- Define system access authorizations to support separation of duties

Least Privilege

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

NIST SP 800-171R3 IPD Access Control

Least Privilege – Privileged Accounts

- Restrict privileged accounts on the system to [*Assignment: organization-defined personnel or roles*]
- Require that users of system accounts (or roles) with access to [*Assignment: organization-defined security functions or security-relevant information*] use non-privileged accounts or roles when accessing non-security functions

Least Privilege – Privileged Accounts

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

Unsuccessful Logon Attempts

- Limit the number of consecutive invalid logon attempts by a user to [*Assignment: organization-defined number*] in [*Assignment: organization-defined time period*]

System Use Notification

- Display system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable CUI rules

NIST SP 800-171R3 IPD Access Control

Device Lock

- Prevent access to the system by [*Selection (one or more): initiating a device lock after* [*Assignment: organization-defined time period*] *of inactivity; requiring the user to initiate a device lock before leaving the system unattended*]
- Retain the device lock until the user reestablishes access using established identification and authentication procedures
- Conceal, via the device lock, information previously visible on the display with a publicly viewable image

Session Termination

- Terminate a user session automatically after [*Assignment: organization-defined conditions or trigger events*]

NIST SP 800-171R3 IPD Access Control

Remote Access

- Establish, authorize, and document usage restrictions, configurations, and connections allowed for each type of permitted remote access
- Monitor and control remote access methods
- Route remote access to the system through managed access control points
- Authorize remote execution of privileged commands and remote access to security-relevant information
- Implement cryptographic mechanisms to protect the confidentiality of remote access sessions

Wireless Access

- Establish configuration requirements, connection requirements, and implementation guidance for wireless access to the system
- Authorize wireless access to the system prior to allowing such connections
- Protect wireless access to the system using authentication and encryption
- Disable, when not intended for use, wireless networking capabilities embedded within the system prior to issuance and deployment

NIST SP 800-171R3 IPD Access Control

Access Control for Mobile Devices

- Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.
- Authorize the connection of mobile devices to the system.
- Implement [*Selection: full-device encryption; container-based encryption*] to protect the confidentiality of CUI on mobile devices

Use of External Systems

- [*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:
  - Access the system from external systems; and
  - Process, store, or transmit CUI using external systems; or
- Prohibit the use of [*Assignment: organizationally-defined types of external systems*]

NIST SP 800-171R3 IPD Access Control

External Systems – Limits and Restrictions on Authorized Use

- Permit authorized individuals to use an external system to access the system or to process, store, or transmit CUI only after:
  - Implemented controls on the external system as specified in the organization’s security policies and security plans are verified; or
  - Approved system connection or processing agreements with the organizational entity hosting the external system are retained
- Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems as follows: [*Assignment: organization-defined usage restrictions*]

Publicly Accessible Content

- Train authorized individuals to ensure that publicly accessible information does not contain CUI
- Review the content on publicly accessible systems for CUI [*Assignment: organization-defined frequency*] and remove such information, if discovered

Account Management – Inactivity Logout

- Require that users log out of the system [*Selection (one or more): after* [*Assignment: organization-defined time period*] *of expected inactivity*; *when* [*Assignment: organization-defined circumstances occur*]]

NIST SP 800-171R3 IPD Awareness and Training

Literacy Training and Awareness

- Provide security literacy training to system users:
  - As part of initial training for new users and [*Assignment: organization-defined frequency*] thereafter; and
  - When required by system changes or following [*Assignment: organization-defined events*]
- Update training and awareness content [*Assignment: organization-defined fre*quency] and following [*Assignment: organization-defined events*]

Role-Based Training

- Provide role-based security training to organizational personnel:
  - Before authorizing access to the system, CUI, or performing assigned duties, and [*Assignment: organization-defined frequency*] thereafter; and
  - When required by system changes
- Update role-based training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]

Advanced Literacy Training

- Provide literacy training on recognizing and reporting potential and actual indicators of insider threat, social engineering, and social mining

NIST SP 800-171R3 IPD
Audit and Accountability

Event Logging

- Specify the following event types for logging within the system: [*Assignment: organization-defined event types*]
- Review and update the event types selected for logging [*Assignment: organization-defined frequency*]

Audit Record Content

- Include the following content in audit records: what type of event occurred; when and where the event occurred; source and outcome of the event; identity of individuals, subjects, objects, or entities associated with the event; and [*Assignment: organization-defined additional information*]

Audit Record Generation

- Provide an audit record generation capability for the event types defined in 3.3.1a.
- Generate audit records for the event types defined in 3.3.1a. that include the audit record content defined in 3.3.2.
- Retain audit records for [*Assignment: organization-defined time period consistent with records retention policy, applicable contract requirement, law, or regulation*]

NIST SP 800-171R3 IPD Audit and Accountability

Response to Audit Logging Process Failures

- Alert [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] in the event of an audit logging process failure
- Take the following additional actions: [*Assignment: organization-defined additional actions*]

Audit Record Review, Analysis, and Reporting

- Review and analyze system audit records [*Assignment: organization-defined frequency*] for indications and potential impact of inappropriate or unusual activity.
- Report findings to [*Assignment: organization-defined personnel or roles*].
- Analyze and correlate audit records across different repositories to gain organization-wide situational awareness

Audit Record Reduction and Report Generation

- Implement an audit record reduction and report generation capability that supports on-demand audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents
- Preserve the original content and time ordering of audit records

NIST SP 800-171R3 IPD Audit and Accountability

Time Stamps

- Use internal system clocks to generate time stamps for audit records.
- Record time stamps for audit records that meet [*Assignment: organization-defined granularity of time measurement*] and that:
  - Use Coordinated Universal Time (UTC);
  - Have a fixed local time offset from UTC; or
  - Include the local time offset as part of the time stamp

Protection of Audit Information

- Protect audit information and audit logging tools from unauthorized access, modification, and deletion

Audit Information Access

- Authorize access to management of audit logging functionality to a subset of privileged users or roles

NIST SP 800-171R3 IPD Configuration Management

Baseline Configuration

- a. Develop, document, and maintain under configuration control, a current baseline configuration of the system
- Review and update the baseline configuration of the system [*Assignment: organization-defined frequency*] and when system components are installed or upgraded

Configuration Settings

- a. Establish, document, and implement configuration settings for the system that reflect the most restrictive mode consistent with operational requirements using [*Assignment: organization-defined common secure configurations*]
- Identify, document, and approve any deviations from established configuration settings
- Monitor and control changes to the configuration settings in accordance with organizational policies and procedures

Configuration Change Control

- Determine the types of changes to the system that are configuration-controlled
- Review proposed configuration-controlled changes to the system, and approve or disapprove such changes with explicit consideration for security impacts.
- Implement and document approved configuration-controlled changes to the system.
- Monitor and review activities associated with configuration-controlled changes to the system

NIST SP 800-171R3 IPD Configuration Management

Impact Analyses

- Analyze the security impact of changes to the system prior to implementation
- After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting specified security requirements

Access Restrictions for Change

- Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system

Least Functionality

- Configure the system to provide only mission-essential capabilities
- Prohibit or restrict use of the following functions, ports, protocols, software, and/or services: [*Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services*]
- Prevent program execution in accordance with [*Selection (one or more):* [*Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions*]; *rules authorizing the terms and conditions of software program usage*]
- Review the system [*Assignment: organization-defined frequency*] to identify and disable/remove functions, ports, protocols, software, and/or services identified in 3.4.6b

NIST SP 800-171R3 IPD Configuration Management

Authorized Software – Allow by Exception

- Identify software programs authorized to execute on the system.
- Implement a deny-all, allow-by-exception policy to allow the execution of authorized software programs on the system.
- Review and update the list of authorized software programs [*Assignment: organization-defined frequency*

User-Installed Software

- Establish policies governing the installation of software by users.
- Enforce software installation policies through the following methods: [*Assignment: organization-defined methods*].
- Monitor policy compliance [*Assignment: organization-defined frequency*]

System Component Inventory

- Develop and document an inventory of system components.
- Review and update the system component inventory [*Assignment: organization-defined frequency*] and as part of component installations, removals, and system updates

NIST SP 800-171R3 IPD Configuration Management

Information Location

- Identify and document the location within the system where CUI is processed and stored
- Identify and document the users who have access to the system where CUI is processed and stored
- Document changes to the location where CUI is processed and stored

System and Component Configuration for High-Risk Areas

- Issue [*Assignment: organization-defined system*] with [*Assignment: organization-defined system configurations*] to individuals traveling to locations that the organization deems to be of significant risk
- Apply the following controls to the system when the individuals return from travel: [*Assignment: organization-defined controls*]

NIST SP 800-171R3 IPD Identification and Authentication

User Identification, Authentication, and Re-Authentication

- Uniquely identify and authenticate system user, and associate that unique identification with processes acting on behalf of those users
- Re-authenticate users when [*Assignment: organization-defined circumstances or situations requiring re-authentication*]

Device Identification and Authentication

- Uniquely identify and authenticate [*Assignment: organization-defined devices and/or types of devices*] before establishing a system or network connection

Multi-Factor Authentication

- Implement multi-factor authentication for access to system accounts

NIST SP 800-171R3 IPD Identification and Authentication

Replay-Resistant Authentication

- Implement replay-resistant authentication mechanisms for access to system accounts

Identifier Management

- Receive authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, service, or device identifier.
- Select and assign an identifier that identifies an individual, group, role, service, or device
- Prevent reuse of identifiers for [*Assignment: organization-defined time period*].
- Identify the status of each individual with the following characteristic: [*Assignment: organization-defined characteristic*]

NIST SP 800-171R3 IPD Identification and Authentication

Password Management

- Enforce the following password composition and complexity rules: [*Assignment: organization-defined composition and complexity rules*]
- Allow user selection of long passwords and passphrases, including spaces and all printable characters
- Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords
- Transmit passwords only over cryptographically-protected channels
- Store passwords using an approved salted key derivation function, preferably using a keyed hash
- Select a new password immediately upon account recovery.
- Allow the use of a temporary password for system logons with an immediate change to a permanent password

NIST SP 800-171R3 IPD Identification and Authentication

Authentication Feedback

- Obscure feedback of authentication information

Authenticator Management

- Establish initial authenticator content for any authenticators issued by the organization
- Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.
- Establish and implement administrative procedures for initial authenticator distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators
- Protect authenticator content from unauthorized disclosure and modification
- Change default authenticators prior to first use
- Change or refresh authenticators [*Assignment: organization-defined time period by authenticator type*] or when [*Assignment: organization-defined events*]
- Change authenticators for group or role accounts when membership to those accounts change

NIST SP 800-171R3 IPD
Incident Response

Incident Response Plan and Handling

- Develop an incident response plan that provides the organization with a roadmap for implementing its incident response capability
- Implement an incident-handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery
- Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing

Incident Monitoring, Reporting, and Response Assistance

- Track and document system security incidents
- Report incident information to [*Assignment: organization-defined authorities*]
- Provide an incident response support resource that offers advice and assistance to users of the system for the handling and reporting of incidents

Incident Response Testing

- Test the effectiveness of the incident response capability [*Assignment: organization-defined frequency*]

NIST SP 800-171R3 IPD
Incident Response

Incident Response Training

- Provide incident response training to system users consistent with assigned roles and responsibilities
- Review and update incident response training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]

NIST SP 800-171R3 IPD Maintenance

Maintenance Tools

- Approve, control, and monitor the use of system maintenance tools
- Inspect maintenance tools and media containing diagnostic and test programs for malicious code before the media and tools are used in the system
- Prevent the removal of maintenance equipment containing CUI by:
  - Verifying that there is no CUI on the equipment;
  - Sanitizing or destroying the equipment; or
  - Obtaining an exemption from [*Assignment: organization-defined officials*] explicitly authorizing removal of the equipment from the facility

Nonlocal Maintenance

- Approve and monitor nonlocal maintenance and diagnostic activities.
- Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.
- Terminate session and network connections when nonlocal maintenance is completed

NIST SP 800-171R3 IPD Maintenance

Maintenance Personnel

- Establish a process for maintenance personnel authorization, and maintain a list of authorized maintenance organizations or personnel
- Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations
- 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

NIST SP 800-171R3 IPD Media Protection

Media Storage

- Physically control and securely store digital and non-digital media containing CUI until the media are destroyed or sanitized using approved equipment, techniques, and procedures

Media Access

- Restrict access to CUI on digital and non-digital media to [*Assignment: organization-defined personnel or roles*]

Media Sanitization

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

Media Marking

- Mark system media containing CUI indicating distribution limitations, handling caveats, and security markings
- Exempt [*Assignment: organization-defined types of system media containing CUI*] from marking if the media remain within [*Assignment: organization-defined controlled areas*]

NIST SP 800-171R3 IPD
Media Protection

Media Transport

- Protect, control, and maintain accountability for system media containing CUI and during transport outside of controlled areas
- Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI stored on digital media during transport

Media Use

- [*Selection: Restrict; Prohibit*] the use of [*Assignment: organization-defined removable system media*]
- Prohibit the use of portable storage devices when such devices have no identifiable owner

System Backup – Cryptographic Protection

- Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations

NIST SP 800-171R3 IPD Personnel Security

Personnel Screening

- Screen individuals prior to authorizing access to the system
- Rescreen individuals in accordance with [*Assignment: organization-defined conditions requiring rescreening*]

Personnel Termination and Transfer

- When individual employment is terminated:
  - Disable system access within [*Assignment: organization-defined time period*];
  - Terminate or revoke authenticators and credentials associated with the individual; and
  - Retrieve all security-related system property
- When individuals are reassigned or transferred to other positions within the organization:
  - Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility;
  - Initiate [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*]; and
  - Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer

NIST SP 800-171R3 IPD Personnel Security

External Personnel Security

- Establish and document personnel security requirements, including security roles and responsibilities for external providers
- Require external providers to comply with the personnel security policies and procedures established by the organization
- Monitor provider compliance with personnel security requirements

NIST SP 800-171R3 IPD Physical Protection

Physical Access Authorizations

- Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides
- Issue authorization credentials for facility access
- Review the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]
- Remove individuals from the facility access list when access is no longer required

Monitoring Physical Access

- Monitor physical access to the facility where the system resides to detect and respond to physical security incidents
- Review physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]
- Coordinate the results of reviews and investigations with the organizational incident response capability

NIST SP 800-171R3 IPD Physical Protection

Alternate Work Site

- Determine and document alternate work sites allowed for use by employees
- b. Employ the following controls at alternate work sites: [*Assignment: organization-defined controls*]

Physical Access Control

- Enforce physical access authorizations at [*Assignment: organization-defined entry and exit points to the facility where the system resides*] by:
  - Verifying individual access authorizations before granting access to the facility; and
  - Controlling ingress and egress to the facility using [*Selection (one or more): [Assignment: organization-defined physical access control systems or devices*]; *guards*]
- Maintain physical access audit logs for [*Assignment: organization-defined entry or exit points*].
- Escort visitors and control visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity*]
- Secure keys, combinations, and other physical access device

NIST SP 800-171R3 IPD
Physical Protection

Access Control for Transmission and Output Devices

- Control physical access to system distribution and transmission lines within organizational facilities
- Control physical access to output from [*Assignment: organization-defined output devices*] to prevent unauthorized individuals from obtaining the output

NIST SP 800-171R3 IPD Risk Assessment

Risk Assessment

- Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI
- Update risk assessments (including supply chain risk) [*Assignment: organization-defined frequency*]

Vulnerability Monitoring and Scanning

- Monitor and scan for vulnerabilities in the system [*Assignment: organization-defined frequency*] and when new vulnerabilities affecting the system are identified
- Remediate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk
- Update vulnerabilities to be scanned [*Assignment: organization-defined frequency*]
- Implement privileged access authorization to the system for vulnerability scanning activities

Risk Response

- Respond to findings from security assessments, monitoring, and audits

NIST SP 800-171R3 IPD Security Assessment and Monitoring

Control Assessments

- Assess the controls in the system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting specified security requirements

Plan of Action and Milestones

- Develop a plan of action and milestones for the system:
  - To document the planned remediation actions to correct weaknesses or deficiencies noted during control assessments; and
  - To reduce or eliminate known vulnerabilities in the system
- Update the existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities

Continuous Monitoring

- Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and assessment of control effectiveness

NIST SP 800-171R3 IPD
Security Assessment and Monitoring

Independent Assessment

- Use independent assessors or assessment teams to assess controls

Information Exchange

- Approve, document, and manage the exchange of CUI between the system and other systems using [*Assignment: organization-defined agreements*]
- Review and update the agreements [*Assignment: organization-defined frequency*]

Internal System Connections

- Authorize internal system connections of [*Assignment: organization-defined system components or classes of components*]
- Review the continued need for each internal system connection [*Assignment: organization-defined frequency*]

NIST SP 800-171R3 IPD
System and Communications Protection

Boundary Protection

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

Separation of System and User Functionality

- Separate user functionality from system management functionality

Information in Shared System Resources

- Prevent unauthorized and unintended information transfer via shared system resources

Network Communications – Deny by Default – Allow by Exception

- Deny network communications traffic by default, and allow network communications traffic by exception

NIST SP 800-171R3 IPD System and Communications Protection

Split Tunneling

- Prevent split tunneling for remote devices unless the split tunnel is securely provisioned using [*Assignment: organization-defined safeguards*]

Transmission and Storage Confidentiality

- Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage

Network Disconnect

- Terminate network connections associated with communications sessions at the end of the sessions or after [*Assignment: organization-defined time period*] of inactivity

Cryptographic Key Establishment and Management

- Establish and manage cryptographic keys when cryptography is implemented in the system in accordance with the following key management requirements: [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*]

Cryptographic Protection

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

NIST SP 800-171R3 IPD
System and Communications Protection

Collaborative Computing Devices and Applications

- Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]
- Provide an explicit indication of use to users physically present at the devices

Mobile Code

- Define acceptable and unacceptable mobile code and mobile code technologies
- Authorize, control, and monitor the use of mobile code

Session Authenticity

- Protect the authenticity of communications sessions

Internal Network Communications Traffic

- Route internal network communications traffic to external networks through an authenticated proxy server

System Access Points

- Limit the number of external network connections to the system

NIST SP 800-171R3 IPD
System and Information Integrity

Flaw Remediation

- Identify, report, and correct system flaws
- Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation
- Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates

Malicious Code Protection

- Implement malicious code protection mechanisms at designated locations within the system to detect and eradicate malicious code
- Update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures

Security Alerts, Advisories, and Directives

- Receive security alerts, advisories, and directives from external organizations
- Generate internal security alerts, advisories, and directives, as necessary

NIST SP 800-171R3 IPD System and Information Integrity

System Monitoring

- Monitor the system, including inbound and outbound communications traffic, to detect:
  - Attacks and indicators of potential attacks;
  - Unusual or unauthorized activities or conditions; and
  - Unauthorized connections
- Identify unauthorized use of the system

Spam Protection

- Implement spam protection mechanisms at designated locations within the system to detect and act on unsolicited messages
- Update spam protection mechanisms [*Assignment: organization-defined frequency*]

NIST SP 800-171R3 IPD Planning

Policy and Procedures

- Develop, document, and disseminate to organizational personnel or roles, policies and procedures needed to implement security requirements
- Review and update policies and procedures [*Assignment: organization-defined frequency*]

System Security Plan

- Develop and document a system security plan that describes:
  - System boundary and operating environment;
  - Security requirements, tailoring actions, and implementation; and
  - Connections to other systems
- Review and update the plan at [*Assignment: organization-defined frequency*]

Rules of Behavior

- Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for handling CUI and system usage
- Review and update the rules of behavior [*Assignment: organization-defined frequency*]

NIST SP 800-171R3 IPD System and Services Acquisition

Security Engineering Principles

- Apply systems security engineering principles in the specification, design, development, implementation, and modification of the system and system components

Unsupported System Components

- Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
- Provide options for alternative sources for continued support for unsupported components

External System Services

- Require the providers of external system services to comply with organizational security requirements, and implement the following controls: [*Assignment: organization-defined controls*]
- Define and document organizational oversight and user roles and responsibilities with regard to external system services
- 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*]

NIST SP 800-171R3 IPD Supply Chain Risk Management

Supply Chain Risk Management Plan

- 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
- Review and update the plan [*Assignment: organization-defined frequency*]

Acquisition Strategies, Tools, and Methods

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

Supply Chain Controls and Processes

- Establish a process or processes for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes
- Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [*Assignment: organization-defined supply chain controls*]

Component Disposal

- Dispose of system components, documentation, or tools containing CUI using the following techniques and methods: [*Assignment: organization-defined techniques and methods*