DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Department of Defense Organization-Defined Parameters for National Institute of Standards and Technology Special Publication 800-171 Revision 3

Reference: (a) National Institute of Standards and Technology (NIST) Special Publication, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST Special Publication (SP) 800-171 Revision 3, May 2024

A key aspect of reference (a) is the inclusion of organization-defined parameters (ODPs), which allow organizations to tailor select security controls to specific security requirements, as determined by unique organizational risk management strategies. In preparation to implement reference (a) as the minimum requirement for contractors, the Department of Defense (DoD) has defined as policy the attached values for the ODPs identified in the reference (a) source document.

ODP values found in existing federal frameworks served as the foundation for the initial values found in Attachment A: NIST SP 800-171 Revision 3 ODP Values. Input was collected from DoD offices, external government agencies, and subject matter experts from University-Affiliated Research Centers and Federally Funded Research and Development Centers. Additional input from industry stakeholders was included where appropriate. In four (4) instances the ODP has been defined as guidance versus a specified value. The ODP values found in Attachment A represent a consensus position of the DoD stakeholders resulting from this collaborative effort and will be updated as necessary.

MCKEOWN.DAVID.W.1034948050
Digitally signed by MCKEOWN.DAVID.W.1034948050
Date: 2025.04.10 14:34:00 -04'00'

David W. McKeown
Performing the Duties of the Deputy
DoD CIO for Cybersecurity and DoD
Chief Information Security Officer

Attachment:
As stated

Attachment A: NIST SP 800-171 Revision 3 ODP Values

Access Control

3.1.1 System Account Management

a. Define the types of system accounts allowed and prohibited.

b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria.

c. Specify:

1. Authorized users of the system,
2. Group and role membership, and
3. Access authorizations (i.e., privileges) for each account.

d. Authorize access to the system based on:

1. A valid access authorization and
2. Intended system usage.

e. Monitor the use of system accounts.

f. Disable system accounts when:

1. The accounts have expired,
2. The accounts have been inactive for **[Assignment: organization-defined time period]** (03.01.01.f.02),
3. The accounts are no longer associated with a user or individual,
4. The accounts are in violation of organizational policy, or
5. Significant risks associated with individuals are discovered.

g. Notify account managers and designated personnel or roles within:

1. **[Assignment: organization-defined time period]** (03.01.01.g.01) when accounts are no longer required,
2. **[Assignment: organization-defined time period]** (03.01.01.g.02) when users are terminated or transferred, and
3. **[Assignment: organization-defined time period]** (03.01.01.g.03) when system usage or the need-to-know changes for an individual.

h. Require that users log out of the system after:

1. **[Assignment: organization-defined time period]** (03.01.01.h.01) of expected inactivity, or
2. When **[Assignment: organization-defined circumstances]** (03.01.01.h.02).

Related Controls: AC-02, AC-02(03), AC-02(05), AC-02(13)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.01.01.f.02	[Assignment: organization-defined time period]	at most 90 days
03.01.01.g.01	[Assignment: organization-defined time period]	24 hours
03.01.01.g.02	[Assignment: organization-defined time period]	24 hours
03.01.01.g.03	[Assignment: organization-defined time period]	24 hours
03.01.01.h.01	[Assignment: organization-defined time period]	at most 24 hours
03.01.01.h.02	[Assignment: organization-defined circumstances]	the work period ends, for privileged users at a minimum

Access Control

3.1.5 System Access Authorization

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:

1. **[Assignment: organization-defined security functions]** (03.01.05.b.01), and
2. **[Assignment: organization-defined security-relevant information]** (03.01.05.b.02).

c. Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency](03.01.05.c) to validate the need for such privileges.

d. Reassign or remove privileges, as necessary.

Related Controls: AC-06, AC-06(01), AC-06(07), AU-09(04)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.01.05.b.01	[Assignment: organization-defined security functions]	at a minimum and if applicable: establishing system accounts and assigning privileges, configuring access authorizations, configuring settings for events to be audited, establishing vulnerability scanning parameters, establishing intrusion detection parameters, and managing audit information
03.01.05.b.02	[Assignment: organization-defined security-relevant information]	at a minimum and if applicable: threat and vulnerability information, filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, security architecture, access control lists, and audit information
03.01.05.c	[Assignment: organization-defined frequency]	at least every 12 months

Access Control

3.1.6 Privileged Account Management

a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles] (03.01.06.a).

b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.

Related Controls: AC-06(02), AC-06(05)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.01.06.a	[Assignment: organization-defined personnel or roles]	only defined and authorized personnel or administrative roles

3.1.8 Invalid Logon Attempts

a. Enforce a limit of [Assignment: organization-defined number] (03.01.08.a.01) **consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]** (03.01.08.a.02).

b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] (03.01.08.b) **when the maximum number of unsuccessful attempts is exceeded**.

Related Controls: AC-07

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.01.08.a.01	[Assignment: organization-defined number]	at most five (5)
03.01.08.a.02	[Assignment: organization-defined time period]	period of five (5) minutes
03.01.08.b	[Assignment: organization-defined time period]	[Selection (one or more): lock the account or node for an at least 15-minute time period; lock the account or node until released by an administrator and notify a system administrator]

Access Control

3.1.10 Device Lock

a. Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] (03.01.10.a) **of inactivity; requiring the user to initiate a device lock before leaving the system unattended].**

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Related Controls: AC-11, AC-11(01)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.01.10.a	[Assignment: organization-defined time period]	initiating a device lock after “at most 15 minutes” of inactivity and requiring the user to initiate a device lock before leaving the system unattended

Access Control

3.1.11 Session Termination

Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect] (03.01.11)**.**

Related Controls: AC-12

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.01.11	[Assignment: organization-defined conditions or trigger events requiring session disconnect]	a specified duration (maximum of 24 hours) of inactivity, misbehavior (end the session due to an attempted policy violation), and maintenance (terminate sessions to prevent issues with an upgrade or service outage)

Access Control

3.1.20 Use of External Systems

a. Prohibit the use of external systems unless the systems are specifically authorized.

b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements] (03.01.20.b)**.**

c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:

1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied, and
2. Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.

d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

Related Controls: AC-20, AC-20(01), AC-20(02)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.01.20.b	[Assignment: organization-defined security requirements]	Guidance: Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. If applicable, use NIST SP 800-47 as a guide for establishing information exchanges between organizations.

Awareness and Training

3.2.1 Security Literacy Training

a. Provide security literacy training to system users:

1. As part of initial training for new users and **[Assignment: organization-defined frequency]** (03.02.01.a.01) thereafter,
2. When required by system changes or following **[Assignment: organization-defined events]** (03.02.01.a.02), and
3. On recognizing and reporting indicators of insider threat, social engineering, and social mining.

b. Update security literacy training content [Assignment: organization-defined frequency] (03.02.01.b.01) **and following [Assignment: organization-defined events]** (03.02.01.b.02)**.**

Related Controls: AT-02, AT-02(02), AT-02(03)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.02.01.a.01	[Assignment: organization-defined frequency]	at least every 12 months
03.02.01.a.02	[Assignment: organization-defined events]	significant[1], novel incidents, or significant[1] changes to risks
03.02.01.b.01	[Assignment: organization-defined frequency]	at least every 12 months
03.02.01.b.02	[Assignment: organization-defined events]	significant[1], novel incidents, or significant[1] changes to risks

[1] Significant: having or likely to have influence or effect.

Awareness and Training

3.2.2 Role-Based Security Training

a. Provide role-based security training to organizational personnel:

1. Before authorizing access to the system or CUI, before performing assigned duties, and **[Assignment: organization-defined frequency]** (03.02.02.a.01) thereafter,
2. When required by system changes or following **[Assignment: organization-defined events]** (03.02.02.a.02)**.**

b. Update role-based training content [Assignment: organization-defined frequency] (03.02.02.b.01) **and following [Assignment: organization-defined events]** (03.02.02.b.02)**.**

Related Controls: AT-03

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.02.02.a.01	[Assignment: organization-defined frequency]	at least every 12 months
03.02.02.a.02	[Assignment: organization-defined events]	significant[1], novel incidents, or significant[1] changes to risks
03.02.02.b.01	[Assignment: organization-defined frequency]	at least every 12 months
03.02.02.b.02	[Assignment: organization-defined events]	significant[1], novel incidents, or significant[1] changes to risks

Audit and Accountability

3.3.1 Event Logging

a. Specify the following event types selected for logging within the system: [Assignment: organization-defined event types] (03.03.01.a)**.**

b. Review and update the event types selected for logging [Assignment: organization-defined frequency] (03.03.01.b)**.**

Related Controls: AU-02

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.03.01.a	[Assignment: organization-defined event types]	at a minimum and where applicable: 1) Authentication events: a) Logons (Success/Failure) b) Logoffs (Success) 2) Security Relevant File and Objects events: a) Create (Success/Failure) b) Access (Success/Failure) c) Delete (Success/Failure) d) Modify (Success/Failure) e) Permission Modification (Success/Failure) f) Ownership Modification (Success/Failure) 3) Export/Writes/downloads to devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure) 4) Import/Uploads from devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure) 5) User and Group Management events: a) User add, delete, modify, disable, lock (Success/Failure) b) Group/Role add, delete, modify (Success/Failure) 6) Use of Privileged/Special Rights events: a) Security or audit policy changes (Success/Failure) b) Configuration changes (Success/Failure) 7) Admin or root-level access (Success/Failure) 8) Privilege/Role escalation (Success/Failure) 9) Audit and security relevant log data accesses (Success/Failure)

ODP Identifier	ODP Assignment Text	ODP Value
		10) System reboot, restart, and shutdown (Success/Failure) 11) Print to a device (Success/Failure) 12) Print to a file (e.g., pdf format) (Success/Failure) 13) Application (e.g., Adobe, Firefox, MS Office Suite) initialization (Success/Failure) For additional guidance, see: OMB21-31 ML 1
03.03.01.b	[Assignment: organization-defined frequency]	at least every 12 months and after any significant[1] incidents or significant[1] changes to risks

Audit and Accountability

3.3.4 Audit Logging Process Failure

a. Alert organizational personnel or roles within [Assignment: organization-defined time period] (03.03.04.a) **in the event of an audit logging process failure.**

b. Take the following additional actions: [Assignment: organization-defined additional actions] (03.03.04.b)**.**

Related Controls: AU-05

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.03.04.a	[Assignment: organization-defined time period]	near real time or as soon as practicable upon discovery
03.03.04.b	[Assignment: organization-defined additional actions]	document the failure and resolution, troubleshoot, repair/restart the audit logging process, and report as incident if applicable

Audit and Accountability

3.3.5 Audit Record Review and Analysis

a. Review and analyze system audit records [Assignment: organization-defined frequency] (03.03.05.a) **for indications and the potential impact of inappropriate or unusual activity.**

b. Report findings to organizational personnel or roles.

c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Related Controls: AU-06, AU-06(03)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.03.05.a	[Assignment: organization-defined frequency]	at least weekly

Audit and Accountability

3.3.7 Time Stamps for Audit Records

a. Use internal system clocks to generate time stamps for audit records.

b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] (03.03.07.b) **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.**

Related Controls: AU-08

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.03.07.b	[Assignment: organization-defined granularity of time measurement]	a granularity of one (1) second or smaller

Configuration Management

3.4.1 Baseline Configuration

a. Develop and maintain under configuration control, a current baseline configuration of the system.

b. Review and update the baseline configuration of the system [Assignment: organization-defined frequency] (03.04.01.b) **and when system components are installed or modified.**

Related Controls: CM-02

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.04.01.b	[Assignment: organization-defined frequency]	at least every 12 months and after any significant[1] incidents or significant[1] changes occur

Configuration Management

3.4.2 Configuration Settings

a. Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings] (03.04.02.a)**.**

b. Identify, document, and approve any deviations from established configuration settings.

Related Controls: CM-06

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.04.02.a	[Assignment: organization-defined configuration settings]	Apply the appropriate use of common security configurations available from the National Institute of Standards and Technology's National Checklist Program (NCP) website (https://ncp.nist.gov/repository) and prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other unauthorized connection to resources in external networks. Document any deviations from the published standard or source document.

Configuration Management

3.4.6 System Configuration

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] (03.04.06.b)**.**

c. Review the system [Assignment: organization-defined frequency] (03.04.06.c) **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.

Related Controls: CM-07, CM-07(01)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.04.06.b	[Assignment: organization-defined functions, ports, protocols, connections, and services]	Guidance: Where feasible, organizations should limit component functionality to a single function per component. Organizations should consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations should employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality should also be achieved as part of the fundamental design and development of the system.
03.04.06.c	[Assignment: organization-defined frequency]	at least every 12 months, when any system functions, ports, protocols, or services changes are made, and after any significant[1] incidents or significant[1] changes to risks

3.4.8 Software Execution Authorization

a. Identify software programs authorized to execute on the system.

b. Implement a deny-all, allow-by-exception policy for the execution of authorized software programs on the system.

c. Review and update the list of authorized software programs [Assignment: organization-defined frequency] (03.04.08.c)**.**

Related Controls: CM-07(05)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.04.08.c	[Assignment: organization-defined frequency]	at least quarterly

Configuration Management

3.4.10 System Component Inventory

a. Develop and document an inventory of system components.

b. Review and update the system component inventory [Assignment: organization-defined frequency] (03.04.10.b)**.**

c. Update the system component inventory as part of installations, removals, and system updates.

Related Controls: CM-08, CM-08(01)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.04.10.b	[Assignment: organization-defined frequency]	at least quarterly

Configuration Management

3.4.12 System Configurations for High-Risk Locations

a. Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations] (03.04.12.a)**.**

b. Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security requirements] (03.04.12.b)**.**

Related Controls: CM-02(07)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.04.12.a	[Assignment: organization-defined system configurations]	a configuration that has no CUI or FCI stored on the system and prevents the processing, storing, and transmission of CUI and FCI, unless a specific exception is granted in writing by the Contracting Officer
03.04.12.b	[Assignment: organization-defined security requirements]	examine the system for signs of physical tampering and take the appropriate actions, and then either purge and reimage all storage media or destroy the system

Identification and Authentication

3.5.1 User Identification and Authentication

a. Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.

b. Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication] (03.05.01.b)**.**

Related Controls: IA-02, IA-11

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.05.01.b	[Assignment: organization-defined circumstances or situations requiring re-authentication]	roles, authenticators, or credentials change (including modification of user privilege); when security categories of systems change; when the execution of privileged functions occurs; and after a session termination

Identification and Authentication

3.5.2 Device Identification and Authentication

Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] (03.05.02) **before establishing a system connection.**

Related Controls: IA-03

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.05.02	[Assignment: organization-defined devices or types of devices]	all devices for identification, where feasible for authentication, and document when not feasible

Identification and Authentication

3.5.5 Identifier Management

a. Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.

b. Select and assign an identifier that identifies an individual, group, role, service, or device.

c. Prevent the reuse of identifiers for [Assignment: organization-defined time period] (03.05.05.c)**.**

d. Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status] (03.05.05.d)**.**

Related Controls: IA-04, IA-04(04)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.05.05.c	[Assignment: organization-defined time period]	at least ten (10) years
03.05.05.d	[Assignment: organization-defined characteristic identifying individual status]	privileged or non-privileged users; contractors, foreign nationals, and/or non-organizational users

Identification and Authentication

3.5.7 Password Management

a. Maintain a list of commonly used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] (03.05.07.a) **and when organizational passwords are suspected to have been compromised.**

b. Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.

c. Transmit passwords only over cryptographically protected channels.

d. Store passwords in a cryptographically protected form.

e. Select a new password upon first use after account recovery.

f. Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules] (03.05.07.f)**.**

Related Controls: IA-05(01)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.05.07.a	[Assignment: organization-defined frequency]	at least quarterly
03.05.07.f	[Assignment: organization-defined composition and complexity rules]	1) Must have a minimum length of 16 characters. 2) Contains a string of characters that does not include the user's account name or full name.

Identification and Authentication

3.5.12 Authenticator Management

a. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.

b. Establish initial authenticator content for any authenticators issued by the organization.

c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.

d. Change default authenticators at first use.

e. Change or refresh authenticators [Assignment: organization-defined frequency] (03.05.12.e.01) **or when the following events occur: [Assignment: organization-defined events]** (03.05.12.e.02)**.**

f. Protect authenticator content from unauthorized disclosure and modification.

Related Controls: IA-05

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.05.12.e.01	[Assignment: organization-defined frequency]	never for passwords where MFA is employed, at least every five (5) years for hard tokens and identification badges, and at least every three (3) years for all other authenticators
03.05.12.e.02	[Assignment: organization-defined events]	after a relevant security incident or any evidence of compromise or loss

Incident Response

3.6.2 Incident Tracking and Reporting

a. Track and document system security incidents.

b. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period] (03.06.02.b)**.**

c. Report incident information to [Assignment: organization-defined authorities] (03.06.02.c)**.**

d. Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.

Related Controls: IR-05, IR-06, IR-07

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.06.02.b	[Assignment: organization-defined time period]	near real time or as soon as practicable upon discovery
03.06.02.c	[Assignment: organization-defined authorities]	all applicable personnel and entities as specified by the contract, and in accordance with any incident response plan notification procedures

Incident Response

3.6.3 Incident Response Testing

Test the effectiveness of the incident response capability [Assignment: organization-defined frequency] (03.06.03)**.**

Related Controls: IR-03

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.06.03	[Assignment: organization-defined frequency]	at least every 12 months

Incident Response

3.6.4 Incident Response Training

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

1. Within **[Assignment: organization-defined time period]** (03.06.04.a.01) of assuming an incident response role or responsibility or acquiring system access,
2. When required by system changes, and
3. **[Assignment: organization-defined frequency]** (03.06.04.a.03) thereafter.

b. Review and update incident response training content [Assignment: organization-defined frequency] (03.06.04.b.01) **and following [Assignment: organization-defined events]** (03.06.04.b.02)**.**

Related Controls: IR-02

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.06.04.a.01	[Assignment: organization-defined time period]	ten (10) days for privileged users, thirty (30) days for all other roles
03.06.04.a.03	[Assignment: organization-defined frequency]	at least every 12 months
03.06.04.b.01	[Assignment: organization-defined frequency]	at least every 12 months
03.06.04.b.02	[Assignment: organization-defined events]	significant[1], novel incidents, or significant[1] changes to risks

Media Protection

3.8.7 System Media Restrictions

a. Restrict or prohibit the use of [Assignment: organization-defined types of system media] (03.08.07.a)**.**

b. Prohibit the use of removable system media without an identifiable owner.

Related Controls: MP-07

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.08.07.a	[Assignment: organization-defined types of system media]	any removable media not managed by or on behalf of the organization

Personnel Security

3.9.1 Screening and Rescreening

a. Screen individuals prior to authorizing access to the system.

b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening] (03.09.01.b)**.**

Related Controls: PS-03

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.09.01.b	[Assignment: organization-defined conditions requiring rescreening]	an organizational policy requiring rescreening when there is a significant[1] incident, or change in status, related to an individual

Personnel Security

3.9.2 Employment Termination and Reassignment

a. When individual employment is terminated:

1. Disable system access within **[Assignment: organization-defined time period]** (03.09.02.a.01),
2. Terminate or revoke authenticators and credentials associated with the individual, and
3. Retrieve security-related system property.

b. When individuals are reassigned or transferred to other positions in the organization:

1. Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and
2. Modify access authorization to correspond with any changes in operational need.

Related Controls: PS-04, PS-05

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.09.02.a.01	[Assignment: organization-defined time period]	four (4) hours

Physical Protection

3.10.1 Facility Access Control

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.

b. Issue authorization credentials for facility access.

c. Review the facility access list [Assignment: organization-defined frequency] (03.10.01.c)**.**

d. Remove individuals from the facility access list when access is no longer required.

Related Controls: PE-02

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.10.01.c	[Assignment: organization-defined frequency]	at least every 12 months, or when there are significant[1] incidents or significant[1] changes to risks

Physical Protection

3.10.2 Physical Access Monitoring and Review

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.

b. Review physical access logs [Assignment: organization-defined frequency] (03.10.02.b.01) **and upon occurrence of [Assignment: organization-defined events or potential indications of events]** (03.10.02.b.02)**.**

Related Controls: PE-06

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.10.02.b.01	[Assignment: organization-defined frequency]	at least every 45 days
03.10.02.b.02	[Assignment: organization-defined events or potential indications of events]	significant[1], novel incidents, or significant[1] changes to risks

Physical Protection

3.10.6 Alternate Work Sites

a. Determine alternate work sites allowed for use by employees.

b. Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements] (03.10.06.b)**.**

Related Controls: PE-17

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.10.06.b	[Assignment: organization-defined security requirements]	adequate security, comparable to organizational security requirements at the primary work site where practical, documented in policy, and covered by training

Risk Assessment

3.11.1 Risk Assessment

a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.

b. Update risk assessments [Assignment: organization-defined frequency] (03.11.01.b)**.**

Related Controls: RA-03, RA-03(01), SR-06

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.11.01.b	[Assignment: organization-defined frequency]	at least every 12 months, or when there are significant[1] incidents or significant[1] changes to risks

Risk Assessment

3.11.2 System Vulnerability Management

a. Monitor and scan the system for vulnerabilities [Assignment: organization-defined frequency] (03.11.02.a) **and when new vulnerabilities affecting the system are identified.**

b. Remediate system vulnerabilities within [Assignment: organization-defined response times] (03.11.02.b)**.**

c. Update system vulnerabilities to be scanned [Assignment: organization-defined frequency] (03.11.02.c) **and when new vulnerabilities are identified and reported.**

Related Controls: RA-05, RA-05(02)

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.11.02.a	[Assignment: organization-defined frequency]	at least monthly, or when there are significant[1] incidents or significant[1] changes to risks
03.11.02.b	[Assignment: organization-defined response times]	thirty (30) days from date of discovery for high-risk vulnerabilities (including both critical and high); 90 days from date of discovery for moderate-risk vulnerabilities; and 180 days from date of discovery for low-risk vulnerabilities
03.11.02.c	[Assignment: organization-defined frequency]	no more than 24 hours prior to running the scans

Security Assessment and Monitoring

3.12.1 Security Requirements Assessment

Assess the security requirements for the system and its environment of operation [Assignment: organization-defined frequency] (03.12.01) **to determine if the requirements have been satisfied.**

Related Controls: CA-02

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.12.01	[Assignment: organization-defined frequency]	at least every 12 months, or when there are significant[1] incidents or significant[1] changes to risks

Security Assessment and Monitoring

3.12.5 Exchange of Controlled Unclassified Information (CUI)

a. Approve and manage the exchange of CUI between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements] (03.12.05.a)**.**

b. Document interface characteristics, security requirements, and responsibilities for each system as part of the exchange agreements.

c. Review and update the exchange agreements [Assignment: organization-defined frequency] (03.12.05.c)**.**

Related Controls: CA-03

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.12.05.a	[Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; nondisclosure agreements; other types of agreements]	requirements as described in the contract
03.12.05.c	[Assignment: organization-defined frequency]	at least every 12 months

3.13.9 Termination of Network Connections

Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] (03.13.09) **of inactivity.**

Related Controls: SC-10

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.13.09	[Assignment: organization-defined time period]	no longer than 15 minutes

System and Communications Protection

3.13.10 Cryptographic Key Management

Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction] (03.13.10)**.**

Related Controls: SC-12

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.13.10	[Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]	Guidance: At a minimum, establish a policy and procedure in line with the latest Cryptographic key management guidance

System and Communications Protection

3.13.11 Cryptography for Confidentiality of CUI

Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography] (03.13.11)**.**

Related Controls: SC-13

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.13.11	[Assignment: organization-defined types of cryptography]	FIPS Validated Cryptography (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules)

System and Communications Protection

3.13.12 Remote Activation of Collaborative Computing Devices

a. Prohibit the remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed] (03.13.12.a)**.**

b. Provide an explicit indication of use to users physically present at the devices.

Related Controls: SC-15

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.13.12.a	[Assignment: organization-defined exceptions where remote activation is to be allowed]	only as enumerated and justified in the System Security Plan before such remote activation occurs, and only when there are no other options, and the remote activation is operationally critical

System and Information Integrity

3.14.1 System Flaw Remediation

a. Identify, report, and correct system flaws.

b. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] (03.14.01.b) **of the release of the updates.**

Related Controls: SI-02

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.14.01.b	[Assignment: organization-defined time period]	thirty (30) days for high-risk flaws (including both critical and high), 90 days for moderate-risk flaws, and 180 days for low-risk flaws

System and Information Integrity

3.14.2 Malicious Code Protection

a. Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

b. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures.

c. Configure malicious code protection mechanisms to:

1. Perform scans of the system **[Assignment: organization-defined frequency]** (03.14.02.c.01) and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed; and
2. Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection.

Related Controls: SI-03

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.14.02.c.01	[Assignment: organization-defined frequency]	at least weekly

Planning

3.15.1 Policy and Procedure Development

a. Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.

b. Review and update policies and procedures [Assignment: organization-defined frequency] (03.15.01.b)**.**

Related Controls: AC-01, AT-01, AU-01, CA-01, CM-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PS-01, RA-01, SA-01, SC-01, SI-01, SR-01

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.15.01.b	[Assignment: organization-defined frequency]	at least every 12 months, or when there are significant[1] incidents or significant[1] changes to risks

Planning

3.15.2 System Security Plan

a. Develop a system security plan that:

1. Defines the constituent system components;
2. Identifies the information types processed, stored, and transmitted by the system;
3. Describes specific threats to the system that are of concern to the organization;
4. Describes the operational environment for the system and any dependencies on or connections to other systems or system components;
5. Provides an overview of the security requirements for the system;
6. Describes the safeguards in place or planned for meeting the security requirements;
7. Identifies individuals that fulfill system roles and responsibilities; and
8. Includes other relevant information necessary for the protection of CUI.

b. Review and update the system security plan [Assignment: organization-defined frequency] (03.15.02.b)**.**

c. Protect the system security plan from unauthorized disclosure.

Related Controls: PL-02

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.15.02.b	[Assignment: organization-defined frequency]	at least every 12 months, or when there are significant[1] incidents or significant[1] changes to risks

Planning

3.15.3 Rules of Behavior

a. Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.

b. Provide rules to individuals who require access to the system.

c. 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.

d. Review and update the rules of behavior [Assignment: organization-defined frequency] (03.15.03.d)**.**

Related Controls: PL-04

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.15.03.d	[Assignment: organization-defined frequency]	at least every 12 months, or when there are significant[1] incidents or significant[1] changes to risks

System and Services Acquisition

3.16.1 Systems Security Engineering Principles

Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles] (03.16.01)**.**

Related Controls: SA-08

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.16.01	[Assignment: organization-defined systems security engineering principles]	Guidance: At a minimum, documentation that provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation should be based on the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

System and Services Acquisition

3.16.3 External System Services

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] (03.16.03.a)**.**

b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.

c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.

Related Controls: SA-09

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.16.03.a	[Assignment: organization-defined security requirements]	1. For cloud service providers: (i) FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or (ii) meets security requirements established by the government equivalent to the FedRAMP Moderate (or higher) baseline. 2. All other external service providers[2] must meet NIST SP 800-171 R2.

[2] External Service Providers (ESP): External people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization.

Supply Chain Risk Management

3.17.1 Supply Chain Risk Management Plan

a. Develop a plan for managing supply chain risks associated with the research and 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 [Assignment: organization-defined frequency] (03.17.01.b)**.**

c. Protect the supply chain risk management plan from unauthorized disclosure.

Related Controls: SR-02

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.17.01.b	[Assignment: organization-defined frequency]	at least every 12 months, or when there are significant[1] incidents or significant[1] changes to risks

Supply Chain Risk Management

3.17.3 Supply Chain Security Requirements

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] (03.17.03.b)**.**

Related Controls: SR-03

ODP Values

ODP Identifier	ODP Assignment Text	ODP Value
03.17.03.b	[Assignment: organization-defined security requirements]	at a minimum, integrate Supply Chain Risk Management (SCRM) into acquisition/procurement policies, provide adequate SCRM resources, define the SCRM control baseline, establish processes to ensure suppliers disclose significant[1] vulnerabilities and significant[1] incidents