NIST 800-171 R2 TO R3 TRANSITION GUIDE

ASSESSMENT OBJECTIVE (AO)-LEVEL ANALYSIS NIST 800-171A TO NIST 800-171A R3

version 2025.3

Disclaimer: This document is provided for educational purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a competent cybersecurity professional.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

While there is a significant increase in the volume of controls between NIST 800-171 R2 and NIST 800-171 R3, the transition is far more complicated than just looking at simple control counts. What matters in compliance is the implementation of the controls at the Assessment Objective (AO) level. Additionally, the governance component of Non-Federal Organization (NFO) controls were incorporated into new CUI controls in NIST 800-171 R3.

Types of Controls	NIST 800-171 R2	NIST 800-171 R3
CUI	110	97 (core controls) 287 (discrete requirements)
NFO	61	0

While it appears there is a roughly 11% drop in the number of CUI controls, the actual number of discrete requirements under the NIST 800-171 R3 CUI controls is 287, which represents an increase of 177 discrete requirements (260% increase). Additionally, NIST 800-171A R3 has a 59% increase in the number of unique requirements at the AO level.

Assessment Objectives	NIST 800-171A	NIST 800-171A R3
# Unique AO Requirements	320	510
% Change In AO Requirements	-	+59%

From a "reasonable person's perspective," when migrating to NIST 800-171A R3, about one-third of the previous AOs directly map and require minimal effort. Approximately one-fifth indirectly map and will require effort to eliminate assumptions. That leaves nearly half of the AOs as requiring significant effort.

Establishing Context	Expected Level of Effort	NIST 800-171A R3	
		AO Count	%
# R3 AOs that directly map to previous version AOs	Minimal	171	34%
# R3 AOs that indirectly map to previous AOs	Moderate	110	22%
# R3 AOs that do not have a clear link to any previous AO	Significant	57	11%
# R3 AOs that are new for NIST 800-171 R3 controls	Significant	172	34%

If you take the time to read this document, we are confident that your understanding of what is needed to migrate from NIST 800-171 R2 to NIST 800-171 R3 will be greatly enhanced.

Tom Cornelius
Senior Partner, ComplianceForge

Ryan Bonner
Founder & CEO, DEFCERT

US DoD Issued Organization Defined Parameters (OPD)

On 10 April 2025, the DoD CIO's office released a memorandum on minimum criteria for NIST SP 800-171 R3 Organizational Defined Parameters (ODP).[1] The following table contains DoD-specified ODPs:

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

[1] *DoD CIO ODP memorandum (2025-04-10) - https://dodcio.defense.gov/Portals/0/Documents/CMMC/OrgDefinedParmsNISTSP800-171.pdf*

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.
03.02.01.a.01	[Assignment: organization- defined frequency]	at least every 12 months
03.02.01.a.02	[Assignment: organization- defined events]	significant, novel incidents, or significant 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, novel incidents, or significant changes to risks
03.02.02.a.01	[Assignment: organization- defined frequency]	at least every 12 months
03.02.02.a.02	[Assignment: organization- defined events]	significant, novel incidents, or significant 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, novel incidents, or significant changes to risks

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) 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 incidents or significant changes to risks
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
03.03.05.a	[Assignment: organization-defined frequency]	at least weekly
03.03.07.b	[Assignment: organization-defined granularity of time measurement]	a granularity of one (1) second or smaller

03.04.01.b	[Assignment: organization- defined frequency]	at least every 12 months and after any significant incidents or significant changes occur
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.
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 incidents or significant changes to risks
03.04.08.c	[Assignment: organization-defined frequency]	at least quarterly
03.04.10.b	[Assignment: organization-defined frequency]	at least quarterly
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
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
03.05.02	[Assignment: organization- defined devices or types of devices]	all devices for identification, where feasible for authentication, and document when not feasible
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
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.
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
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
03.06.03	[Assignment: organization-defined frequency]	at least every 12 months
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, novel incidents, or significant changes to risks
03.08.07.a	[Assignment: organization-defined types of system media]	any removable media not managed by or on behalf of the organization
03.09.01.b	[Assignment: organization- defined conditions requiring rescreening]	an organizational policy requiring rescreening when there is a significant incident, or change in status, related to an individual
03.09.02.a.01	[Assignment: organization-defined time period]	four (4) hours
03.10.01.c	[Assignment: organization- defined frequency]	at least every 12 months, or when there are significant incidents or significant changes to risks
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, novel incidents, or significant changes to risks
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
03.11.01.b	[Assignment: organization- defined frequency]	at least every 12 months, or when there are significant incidents or significant changes to risks
03.11.02.a	[Assignment: organization- defined frequency]	at least monthly, or when there are significant incidents or significant 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
03.12.01	[Assignment: organization- defined frequency]	at least every 12 months, or when there are significant incidents or significant changes to risks
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
03.13.09	[Assignment: organization-defined time period]	no longer than 15 minutes
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
03.13.11	[Assignment: organization- defined types of cryptography]	FIPS Validated Cryptography (https://csrc.nist.gov/Projects/Cryptographic-Module- Validation-Program/Validated-Modules)
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
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
03.14.02.c.01	[Assignment: organization-defined frequency]	at least weekly
03.15.01.b	[Assignment: organization- defined frequency]	at least every 12 months, or when there are significant incidents or significant changes to risks
03.15.02.b	[Assignment: organization- defined frequency]	at least every 12 months, or when there are significant incidents or significant changes to risks
03.15.03.d	[Assignment: organization- defined frequency]	at least every 12 months, or when there are significant incidents or significant changes to risks
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.

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 providers2 must meet NIST SP 800-171 R2.
03.17.01.b	[Assignment: organization- defined frequency]	at least every 12 months, or when there are significant incidents or significant changes to risks
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 vulnerabilities and significant incidents

Breaking Down The NIST SP 800-171 R3 CUI Controls

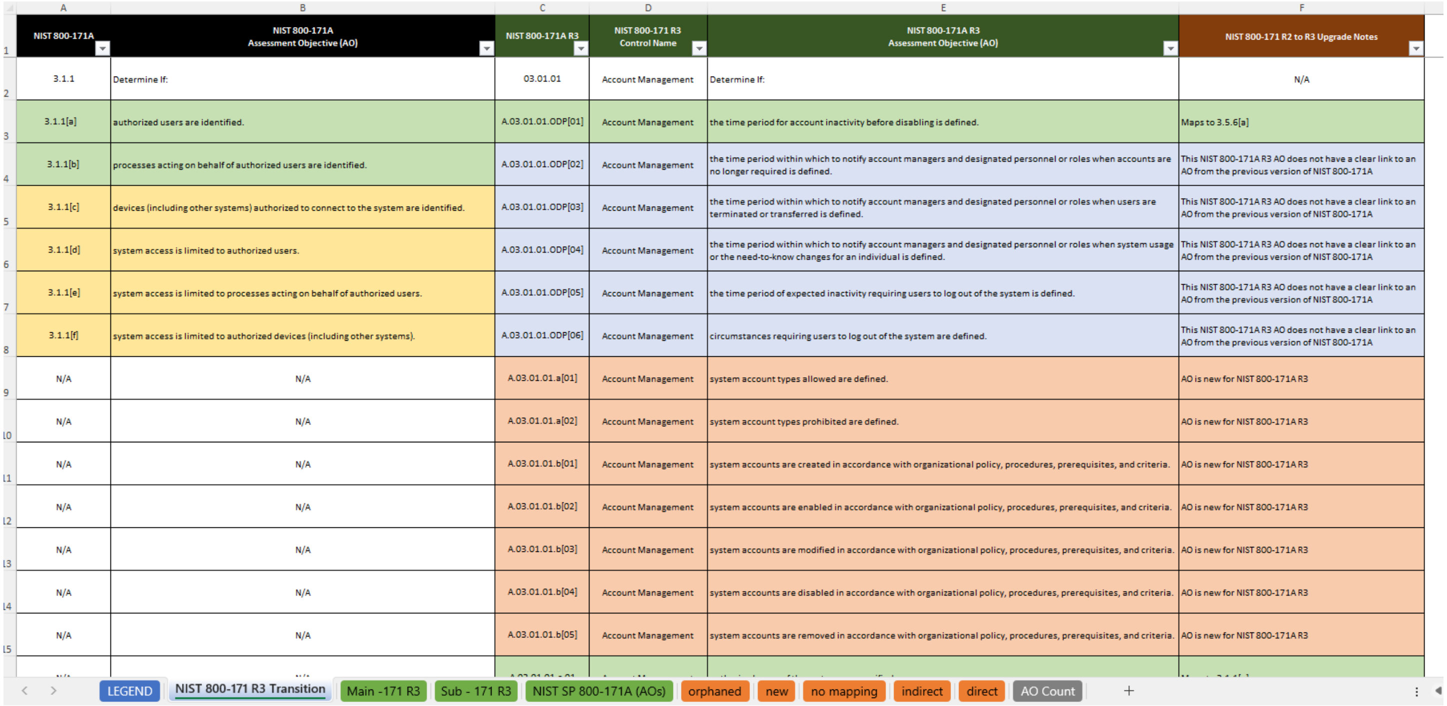
There are significant changes in numbers between the initial one hundred ten (110) CUI controls in NIST SP 800-171 R2 and requirements listed in NIST SP 800-171 R3.

Core CUI Controls

There are ninety-seven (97) core CUI controls listed in NIST SP 800-171 R3 (see Excel spreadsheet for details).

Discrete CUI Requirements (Sub Controls)

There are two hundred eighty-seven (287) discrete requirements (e.g., sub controls) within those ninety-seven (97) core CUI controls listed in NIST SP 800-171 R3 (see Excel spreadsheet for details).



NIST 800-171A	NIST 800-171A Assessment Objective (AO)	NIST 800-171A R3	NIST 800-171 R3 Control Name	NIST 800-171A R3 Assessment Objective (AO)	NIST 800-171 R2 to R3 Upgrade Notes
3.1.1	Determine If:	03.01.01	Account Management	Determine If:	N/A
3.1.1[a]	authorized users are identified.	A.03.01.01.ODP[01]	Account Management	the time period for account inactivity before disabling is defined.	Maps to 3.5.6[a]
3.1.1[b]	processes acting on behalf of authorized users are identified.	A.03.01.01.ODP[02]	Account Management	the time period within which to notify account managers and designated personnel or roles when accounts are no longer required is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
3.1.1[c]	devices (including other systems) authorized to connect to the system are identified.	A.03.01.01.ODP[03]	Account Management	the time period within which to notify account managers and designated personnel or roles when users are terminated or transferred is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
3.1.1[d]	system access is limited to authorized users.	A.03.01.01.ODP[04]	Account Management	the time period within which to notify account managers and designated personnel or roles when system usage or the need-to-know changes for an individual is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
3.1.1[e]	system access is limited to processes acting on behalf of authorized users.	A.03.01.01.ODP[05]	Account Management	the time period of expected inactivity requiring users to log out of the system is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
3.1.1[f]	system access is limited to authorized devices (including other systems).	A.03.01.01.ODP[06]	Account Management	circumstances requiring users to log out of the system are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
N/A	N/A	A.03.01.01.a[01]	Account Management	system account types allowed are defined.	AO is new for NIST 800-171A R3
N/A	N/A	A.03.01.01.a[02]	Account Management	system account types prohibited are defined.	AO is new for NIST 800-171A R3
N/A	N/A	A.03.01.01.b[01]	Account Management	system accounts are created in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3
N/A	N/A	A.03.01.01.b[02]	Account Management	system accounts are enabled in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3
N/A	N/A	A.03.01.01.b[03]	Account Management	system accounts are modified in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3
N/A	N/A	A.03.01.01.b[04]	Account Management	system accounts are disabled in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3
N/A	N/A	A.03.01.01.b[05]	Account Management	system accounts are removed in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3

You can download the Excel spreadsheet at: **https://complianceforge.com/content/nist-800-171-r3-transition.xlsx**

End of Life (EOL) Assessment Objectives

The central issue with End of Life (EOL) Assessment Objectives (AOs) is the undocumented dependencies that exist. Assumptions can lead to non-compliance and/or poor security practices.

Performing a thorough analysis on the differences between NIST 800-171A and NIST 800-171A R3 will uncover several AOs that existed in NIST 800-171A, but do not exist in NIST 800-171A R3:

- The underlying functions still exist in NIST 800-171 R3 (e.g., maintenance operations), but the corresponding AOs lack specificity to call out a unique requirement for the function to be performed (e.g., perform maintenance on assets); and
- Demonstrating compliance with NIST 800-171A R3 relies on assumptions that certain fundamental Information Technology (IT) capabilities exist in a mature enough state to support the control.

Undocumented Dependencies In NIST 800-171A R3

The following areas are points of concern that organizations should take time to review before starting the journey from NIST 800-171 R2 to NIST 800-171 R3. While the intent of NIST 800-171 is to have "reasonable security practices" to protect CUI as it is Stored/Processed/Transmitted (S/P/T), it is clear that NIST created several evidentiary gaps in NIST 800-171A R3 that could lead to assumptions or compliance failures.

Examples of undocumented dependencies in NIST 800-171 R3 and NIST 800-171A R3 include, but are not limited to:

Maintenance Operations

Problem: NIST 800-171A R3 drops a critical NIST 800-171A AO that existed to perform maintenance operations:

- In NIST 800-171A, AO 3.7.1 (determine if system maintenance is performed) existed to ensure IT-related maintenance activities were performed.
- There is no corresponding AO in NIST 800-171A R3 that specifies maintenance-related operations.
- Maintenance-related AOs in NIST 800-171A R3 do not require maintenance to be performed and are limited to:
  - Approving/controlling maintenance tools (A.03.07.04.a[01] & A.03.07.04.a[02]);
  - The use of maintenance tools is monitored A.03.07.04.a[03]; and
  - Controlling maintenance media (A.03.07.04.b & A.03.07.04.c).
- The closest analog AOs in NIST 800-171A R3 blend the concepts of maintenance with:
  - Configuration change control with AO A.03.04.03.c[01] (approved configuration-controlled changes to the system are implemented). This assumes that change control is performing IT-related maintenance activities; or
  - Vulnerability remediation with AO A.03.11.02.b (system vulnerabilities are remediated within <A.03.11.02.ODP[03]: response times>). This assumes that vulnerability management is a key component of IT-related maintenance activities.

Dependency Issue: The issue is that there is a clear assumption that maintenance is being performed. However, there is no actual AO-level requirement in NIST 800-171A R3 to actually perform maintenance operations.

Roles and Responsibilities

Problem: NIST 800-171A R3 drops several NIST 800-171A AOs that establish roles and responsibilities for personnel:

- In NIST 800-171A, the following AOs specifically called for the definition and assignment of roles & responsibilities:
  - 3.1.22[a] - individuals authorized to post or process information on publicly accessible systems are identified.
  - 3.2.2[a] - information security-related duties, roles, and responsibilities are defined.
  - 3.2.2[b] - information security-related duties, roles, and responsibilities are assigned to designated personnel.
- There are no corresponding AOs in NIST 800-171A R3 that specify internal roles and responsibilities. The only requirement to document roles and responsibilities pertains to third-parties:
  - A.03.16.03.b - user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers, are defined and documented.

Dependency Issue: The issue is that there is a clear assumption that cybersecurity-related roles and responsibilities are defined for and assigned to internal personnel. The use of the word "roles" is used throughout NIST 800-171A R3, but there is no requirement to define cybersecurity-related roles and responsibilities for internal personnel.

Documenting The Flow Of CUI

Problem: NIST 800-171A R3 drops several NIST 800-171A AOs that exist to document the flow of CUI:

- In NIST 800-171A, the following AOs specify expectations for controlling the flow of CUI:
  - 3.1.2[a] - the types of transactions and functions that authorized users are permitted to execute are defined
  - 3.1.3[a] - information flow control policies are defined.
  - 3.1.3[b] - methods and enforcement mechanisms for controlling the flow of CUI are defined.
  - 3.1.3[c] - designated sources and destinations (e.g., networks, individuals, and devices) for CUI within systems and between interconnected systems are identified.
  - 3.1.3[d] - authorizations for controlling the flow of CUI are defined.
- There are no corresponding AOs in NIST 800-171A R3 that specify documenting the flow of CUI.
- The closest analog in NIST 800-171A R3 defaults to organizational policy:
  - A.03.01.02[01] - approved authorizations for logical access to CUI are enforced in accordance with applicable access control policies.
  - A.03.01.02[02] - approved authorizations for logical access to system resources are enforced in accordance with applicable access control policies.

Dependency Issue: The issue is that there is a clear assumption that documentation exists that specifies how CUI is to be controlled. This just creates ambiguity as to the acceptable level of due diligence and due care that is necessary to demonstrate compliance with these AOs. The specifications in NIST 800-171A for controlling the flow of CUI could be reasonably addressed in the policy requirements section of NIST 800-171A R3. Additionally, the assumption could be made that the System Security Plan (SSP) is meant to capture this information, but it is not specified as a requirement for the SSP to document.

Logical Access Control / Account Management

Problem: NIST 800-171A R3 drops several NIST 800-171A AOs that affect logical access control / account management:

- In NIST 800-171A, the following AOs affect logical access control / account management:
  - 3.1.5[a] - privileged accounts are identified.
  - 3.1.6[a] - nonsecurity functions are identified.
  - 3.1.6[b] - users are required to use non-privileged accounts or roles when accessing nonsecurity functions.
  - 3.1.7[a] - privileged functions are defined.
  - 3.1.7[b] - non-privileged users are defined.
- There are no corresponding AOs in NIST 800-171A R3 that specify documenting privileged and non-privileged accounts.
- The closest analog in NIST 800-171A R3 defaults to organizational policy:
  - A.03.01.05.ODP[01] - security functions for authorized access are defined.

Dependency Issue: The issue is that there is a clear assumption that privileged accounts are identified and privileged functions are defined. The same assumption applies to non-privileged accounts. The assumption could be made that end user training, assigned roles and responsibilities, etc. provides that clarity, but it would be an assumption and not a documented requirement.

Situational Awareness

Problem: NIST 800-171A R3 drops a critical NIST 800-171A AO that existed to ensure the consistency of time in the management of event logs:

- In NIST 800-171A, the following AO established the need for an authoritative time source:
  - 3.3.7[b] - an authoritative source with which to compare and synchronize internal system clocks is specified.
- There are no corresponding AOs in NIST 800-171A R3 that specify an authoritative time source. The only requirements pertaining to clock synchronization:
  - Granularity of time measurement (A.03.03.07.ODP[01]);
  - Internal system clocks are to be used to generate time stamps (A.03.03.07.a); and
  - Time stamps are recorded (A.03.03.07.b[01] & A.03.03.07.b[02])

Dependency Issue: The issue is that there is a clear assumption that internal system clocks are synchronized with an authoritative time source (e.g., US Naval Observatory (USNO) public time server, etc.). Without an authoritative time source, time is subjective and that can negatively affect (1) event log analysis and (2) incident response actions.

COMPREHENSIVE INVENTORIES

Problem: NIST 800-171A R3 drops several NIST 800-171A AOs that require various types of inventories to provide situational awareness of the assets and personnel that affect the security of CUI:

- In NIST 800-171A, the following AOs affect situational awareness about inventories of systems, users and third-parties:
  - 3.1.18[a] - mobile devices that process, store, or transmit CUI are identified.
  - 3.1.18[c] - mobile device connections are monitored and logged.
  - 3.1.20[a] - connections to external systems are identified.
  - 3.1.20[b] - use of external systems is identified.
  - 3.1.20[d] - use of external systems is verified.
  - 3.5.3[a] - privileged accounts are identified.
  - 3.13.12[a] - collaborative computing devices are identified.
- There are no corresponding AOs in NIST 800-171A R3 that specify an inventory beyond "system components":
  - A.03.04.10.a - an inventory of system components is developed and documented.

Dependency Issue: The issue is that there is a clear assumption that the organization has inventories for:

- Systems (including hardware, software and services);
- Third-parties (e.g., Cloud Service Providers (CSP), External Service Providers (ESP), etc.);
- Privileged users;
- Non-privileged users; and
- Third-party users.

The assumption could be made that anything related to third-parties would be captured within the Supply Chain Risk Management (SCRM) requirements. However, the SCRM Plan requirement lacks that level of specification.

INCIDENT RESPONSE

Problem: NIST 800-171A R3 drops several NIST 800-171A AOs that affect incident response operations:

- In NIST 800-171A, the following AOs affect incident response operations by defining responsible personnel and specifying that incident response operations must occur:
  - 3.3.4[a] - personnel or roles to be alerted in the event of an audit logging process failure are identified.
  - 3.3.4[b] - types of audit logging process failures for which alert will be generated are defined.
  - 3.6.2[d] - organizational officials to whom incidents are to be reported are identified.
  - 3.14.3[a] - response actions to system security alerts and advisories are identified.
  - 3.14.3[c] - actions in response to system security alerts and advisories are taken.
- There are no corresponding AOs in NIST 800-171A R3 that specify:
  - Personnel to be alerted for audit logging process failures;
  - Defining internal "organizational officials" who need to be alerted to incidents; or
  - Defining response actions to physical security incidents.

Dependency Issue: The issue is that there is a clear assumption that incident response operations exist and are documented. This corresponds with the previously discussed assumption about documented roles and responsibilities. There are assumptions that organizations clearly-define the roles and responsibilities of personnel in incident response roles.

PHYSICAL SECURITY

Problem: NIST 800-171A R3 drops several NIST 800-171A AOs that establish the basis for physical security practices:

- In NIST 800-171A, the following AOs affect physical security practices:
  - 3.10.2[a] - the physical facility where that system resides is protected.
  - 3.10.2[b] - the support infrastructure for that system is protected.
  - 3.10.2[d] - the support infrastructure for that system is monitored.
- There are no corresponding AOs in NIST 800-171 R3 that specify:
  - Physical security protections; or
  - Broader physical infrastructure security.

Dependency Issue: The issue is that there is a clear assumption that physical security is being performed and that there is sufficient documentation to prove those physical security practices exist.

ORPHANED NIST 800-171 AOS THAT DO NOT EXIST IN NIST 800-171A R3

The following NIST 800-171A AOs are End of Life (EOL) where these AO cease to exist and there are no corresponding AOs in NIST 800-171A R3. Several of these orphaned AOs create the issue with logical dependencies described in the previous section:

NIST 800-171A	NIST 800-171A Assessment Objective (AO)
3.1.2[a]	the types of transactions and functions that authorized users are permitted to execute are defined
3.1.3[a]	information flow control policies are defined.
3.1.3[b]	methods and enforcement mechanisms for controlling the flow of CUI are defined.
3.1.3[c]	designated sources and destinations (e.g., networks, individuals, and devices) for CUI within systems and between interconnected systems are identified.
3.1.3[d]	authorizations for controlling the flow of CUI are defined.
3.1.5[a]	privileged accounts are identified.
3.1.6[a]	nonsecurity functions are identified.
3.1.6[b]	users are required to use non-privileged accounts or roles when accessing nonsecurity functions.
3.1.7[a]	privileged functions are defined.
3.1.7[b]	non-privileged users are defined.
3.1.12[d]	remote access sessions are monitored.
3.1.18[a]	mobile devices that process, store, or transmit CUI are identified.
3.1.18[c]	mobile device connections are monitored and logged.
3.1.20[a]	connections to external systems are identified.
3.1.20[b]	use of external systems is identified.
3.1.20[d]	use of external systems is verified.
3.1.22	Determine if CUI posted or processed on publicly accessible systems is controlled.
3.1.22[a]	individuals authorized to post or process information on publicly accessible systems are identified.
3.1.22[b]	procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.
3.2.2[a]	information security-related duties, roles, and responsibilities are defined.
3.2.2[b]	information security-related duties, roles, and responsibilities are assigned to designated personnel.
3.3.1[d]	audit records, once created, contain the defined content.
3.3.4[a]	personnel or roles to be alerted in the event of an audit logging process failure are identified.
3.3.4[b]	types of audit logging process failures for which alert will be generated are defined.
3.3.7[b]	an authoritative source with which to compare and synchronize internal system clocks is specified.
3.5.3[a]	privileged accounts are identified.
3.5.3[b]	multifactor authentication is implemented for local access to privileged accounts.
3.6.2[d]	organizational officials to whom incidents are to be reported are identified.
3.10.2[a]	the physical facility where that system resides is protected.
3.10.2[b]	the support infrastructure for that system is protected.
3.10.2[d]	the support infrastructure for that system is monitored.
3.13.12[a]	collaborative computing devices are identified.
3.14.1[a]	the time within which to identify system flaws is specified.
3.14.1[c]	the time within which to report system flaws is specified.
3.14.1[e]	the time within which to correct system flaws is specified.
3.14.3[a]	response actions to system security alerts and advisories are identified.
3.14.3[c]	actions in response to system security alerts and advisories are taken.

Minimal Effort Assessment Objective Transition

For organizations that currently have controls in place for NIST 800-171 R2 and leverage NIST 800-171A, approximately one-third of the AOs in NIST 800-171A R3 should be considered minimal effort from a transition perspective.

NIST 800-171A R3 AOs With Direct Mapping (Existing NIST 800-171 R3 Control)

The following AOs have "direct mapping" which means the NIST 800-171A R3 AO can be clearly mapped back to an existing NIST 800-171A AO.

NIST 800-171A R3	NIST 800-171 R3 Control Name	NIST 800-171A R3 Assessment Objective (AO)	NIST 800-171 R2 to R3 Upgrade Notes
A.03.01.01.ODP[01]	Account Management	the time period for account inactivity before disabling is defined.	Maps to 3.5.6[a]
A.03.01.01.c.01	Account Management	authorized users of the system are specified.	Maps to 3.1.1[a]
A.03.01.01.f.02	Account Management	system accounts are disabled when the accounts have been inactive for <A.03.01.01.ODP[01]: time period>.	Maps to 3.5.6[b]
A.03.01.04.a	Separation of Duties	duties of individuals requiring separation are identified.	Maps to 3.1.4[a]
A.03.01.05.b[01]	Least Privilege	access to <A.03.01.05.ODP[01]: security functions> is authorized.	Maps to 3.1.5[d]
A.03.01.07.a	Least Privilege – Privileged Functions	non-privileged users are prevented from executing privileged functions.	Maps to 3.1.7[c]
A.03.01.07.b	Least Privilege – Privileged Functions	the execution of privileged functions is logged.	Maps to 3.1.7[d]
A.03.01.08.ODP[01]	Unsuccessful Logon Attempts	the number of consecutive invalid logon attempts by a user allowed during a time period is defined.	Maps to 3.1.8[a]
A.03.01.09	System Use Notification	a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed before granting access to the system.	Maps to 3.1.9[a], 3.1.9[b]
A.03.01.10.ODP[01]	Device Lock	one or more of the following PARAMETER VALUES are selected: {a device lock is initiated after <A.03.01.10.ODP[02]: time period> of inactivity; the user is required to initiate a device lock before leaving the system unattended}.	Maps to 3.1.10[b]
A.03.01.10.ODP[02]	Device Lock	the time period of inactivity after which a device lock is initiated is defined (if selected).	Maps to 3.1.10[a]
A.03.01.10.a	Device Lock	access to the system is prevented by <A.03.01.10.ODP[01]: SELECTED PARAMETER VALUES>.	Maps to 3.1.10[b]
A.03.01.10.c	Device Lock	information previously visible on the display is concealed via device lock with a publicly viewable image.	Maps to 3.1.10[c]
A.03.01.11.ODP[01]	Session Termination	conditions or trigger events that require session disconnect are defined.	Maps to 3.1.11[a]
A.03.01.11	Session Termination	a user session is terminated automatically after <A.03.01.11.ODP[01]: conditions or trigger events>.	Maps to 3.1.11[b]
A.03.01.12.a[01]	Remote Access	types of allowable remote system access are defined.	Maps to 3.1.12[b] and elements of 3.1.14[a]
A.03.01.12.c[02]	Remote Access	remote access to the system is routed through managed access control points.	Maps to 3.1.14[b]
A.03.01.16.b	Wireless Access	each type of wireless access to the system is authorized prior to establishing such connections.	Maps to 3.1.16[b]

A.03.01.16.d[01]	Wireless Access	wireless access to the system is protected using authentication.	Maps to 3.1.17[b]
A.03.01.16.d[02]	Wireless Access	wireless access to the system is protected using encryption.	Maps to 3.1.17[a]
A.03.01.18.b	Access Control for Mobile Devices	the connection of mobile devices to the system is authorized.	Maps to 3.1.19[a]
A.03.01.18.c	Access Control for Mobile Devices	full-device or container-based encryption is implemented to protect the confidentiality of CUI on mobile devices.	Maps to 3.1.19[b]
A.03.01.22.b[01]	Publicly Accessible Content	the content on publicly accessible systems is reviewed for CUI.	Maps to 3.1.22[c], 3.1.22[d]
A.03.01.22.b[02]	Publicly Accessible Content	CUI is removed from publicly accessible systems, if discovered.	Maps to 3.1.22[e]
A.03.02.01.a.03[01]	Literacy Training and Awareness	security literacy training is provided to system users on recognizing indicators of insider threat.	Maps to 3.2.3[b] and elements of 3.2.1[c], 3.2.1[d], 3.2.3[a]
A.03.02.02.a.01[01]	Role-Based Training	role-based security training is provided to organizational personnel before authorizing access to the system or CUI.	Maps to 3.2.2[c]
A.03.02.02.a.01[02]	Role-Based Training	role-based security training is provided to organizational personnel before performing assigned duties.	Maps to 3.2.2[c]
A.03.02.02.a.01[03]	Role-Based Training	role-based security training is provided to organizational personnel <A.03.02.02.ODP[01]: frequency> after initial training.	Maps to 3.2.2[c]
A.03.02.02.a.02	Role-Based Training	role-based security training is provided to organizational personnel when required by system changes or following <A.03.02.02.ODP[02]: events>.	Maps to 3.2.2[c]
A.03.02.02.b[01]	Role-Based Training	role-based security training content is updated <A.03.02.02.ODP[03]: frequency>.	Maps to 3.2.2[c]
A.03.03.01.ODP[01]	Event Logging	event types selected for logging within the system are defined.	Maps to 3.3.1[a], 3.3.1[b]
A.03.03.01.a	Event Logging	the following event types are specified for logging within the system: <A.03.03.01.ODP[01]: event types>.	Maps to 3.3.1[a], 3.3.1[b]
A.03.03.01.b[02]	Event Logging	the event types selected for logging are updated <A.03.03.01.ODP[02]: frequency>.	Maps to 3.3.3[c]
A.03.03.03.a	Audit Record Generation	audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02 are generated.	Maps to 3.3.1[c] and elements of NFO - SI-4(5)
A.03.03.03.b	Audit Record Generation	audit records are retained for a time period consistent with the records retention policy.	Maps to 3.3.1[f]
A.03.03.04.a	Response to Audit Logging Process Failures	organizational personnel or roles are alerted in the event of an audit logging process failure within <A.03.03.04.ODP[01]: time period>.	Maps to 3.3.4[c]
A.03.03.05.a	Audit Record Review, Analysis, and Reporting	system audit records are reviewed and analyzed <A.03.03.05.ODP[01]: frequency> for indications and the potential impact of inappropriate or unusual activity.	Maps to 3.3.5[a]
A.03.03.05.c[01]	Audit Record Review, Analysis, and Reporting	audit records across different repositories are analyzed to gain organization-wide situational awareness.	Maps to 3.3.5[b]

A.03.03.05.c[02]	Audit Record Review, Analysis, and Reporting	audit records across different repositories are correlated to gain organization-wide situational awareness.	Maps to 3.3.5[b]
A.03.03.06.a[01]	Audit Record Reduction and Report Generation	an audit record reduction and report generation capability that supports audit record review is implemented.	Maps to 3.3.6[a]
A.03.03.06.a[02]	Audit Record Reduction and Report Generation	an audit record reduction and report generation capability that supports audit record analysis is implemented.	Maps to 3.3.6[a]
A.03.03.06.a[03]	Audit Record Reduction and Report Generation	an audit record reduction and report generation capability that supports audit record reporting requirements is implemented.	Maps to 3.3.6[b]
A.03.03.07.a	Time Stamps	internal system clocks are used to generate time stamps for audit records.	Maps to 3.3.7[a]
A.03.03.07.b[01]	Time Stamps	time stamps are recorded for audit records that meet <A.03.03.07.ODP[01]: granularity of time measurement>.	Maps to 3.3.7[c]
A.03.03.08.a[01]	Protection of Audit Information	audit information is protected from unauthorized access, modification, and deletion.	Maps to 3.3.8[a], 3.3.8[b], 3.3.8[c]
A.03.03.08.a[02]	Protection of Audit Information	audit logging tools are protected from unauthorized access, modification, and deletion.	Maps to 3.3.8[d], 3.3.8[e], 3.3.8[f]
A.03.03.08.b	Protection of Audit Information	access to management of audit logging functionality is authorized to only a subset of privileged users or roles.	Maps to 3.3.9[a], 3.3.9[b]
A.03.04.01.a[01]	Baseline Configuration	a current baseline configuration of the system is developed.	Maps to 3.4.1[a], 3.4.1[b], 3.4.2[a]
A.03.04.01.a[02]	Baseline Configuration	a current baseline configuration of the system is maintained under configuration control.	Maps to 3.4.1[c], 3.4.2[b]
A.03.04.02.ODP[01]	Configuration Settings	configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are defined.	Maps to 3.4.2[a], 3.4.6[a], 3.4.6[b] and elements of 3.13.7
A.03.04.02.a[01]	Configuration Settings	the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are established and documented: <A.03.04.02.ODP[01]: configuration settings>.	Maps to 3.4.2[a], 3.4.6[a], 3.4.6[b] and elements of 3.13.7
A.03.04.03.b[01]	Configuration Change Control	proposed configuration-controlled changes to the system are reviewed with explicit consideration for security impacts.	Maps to 3.4.3[a], 3.4.3[b]
A.03.04.03.b[02]	Configuration Change Control	proposed configuration-controlled changes to the system are approved or disapproved with explicit consideration for security impacts.	Maps to 3.4.3[a], 3.4.3[c]
A.03.04.03.c[02]	Configuration Change Control	approved configuration-controlled changes to the system are documented.	Maps to 3.4.3[d]
A.03.04.04.a	Impact Analyses	changes to the system are analyzed to determine potential security impacts prior to change implementation.	Maps to 3.4.4
A.03.04.05[01]	Access Restrictions for Change	physical access restrictions associated with changes to the system are defined and documented.	Maps to 3.4.5[a], 3.4.5[b]

A.03.04.05[02]	Access Restrictions for Change	physical access restrictions associated with changes to the system are approved.	Maps to 3.4.5[c]
A.03.04.05[03]	Access Restrictions for Change	physical access restrictions associated with changes to the system are enforced.	Maps to 3.4.5[d]
A.03.04.05[04]	Access Restrictions for Change	logical access restrictions associated with changes to the system are defined and documented.	Maps to 3.4.5[e], 3.4.5[f]
A.03.04.05[05]	Access Restrictions for Change	logical access restrictions associated with changes to the system are approved.	Maps to 3.4.5[g]
A.03.04.05[06]	Access Restrictions for Change	logical access restrictions associated with changes to the system are enforced.	Maps to 3.4.5[h]
A.03.04.08.a	Authorized Software – Allow by Exception	software programs authorized to execute on the system are identified.	Maps to 3.4.8[a], 3.4.8[b]
A.03.04.08.b	Authorized Software – Allow by Exception	a deny-all, allow-by-exception policy for the execution of authorized software programs on the system is implemented.	Maps to 3.4.8[c] and elements of 3.4.9[a], 3.4.9[b] and NFO CA-3(5) (now SC-7(5))
A.03.04.10.a	System Component Inventory	an inventory of system components is developed and documented.	3.4.1[d] and elements of 3.4.1[e]
A.03.05.01.a[02]	User Identification and Authentication	system users are authenticated.	Maps to 3.5.2[a], 3.5.2[b]
A.03.05.01.a[03]	User Identification and Authentication	processes acting on behalf of users are associated with uniquely identified and authenticated system users.	Maps to 3.1.1[b]
A.03.05.02[02]	Device Identification and Authentication	<A.03.05.02.ODP[01]: devices or types of devices> are authenticated before establishing a system connection.	Maps to 3.5.2[c]
A.03.05.03[01]	Multi-Factor Authentication	multi-factor authentication for access to privileged accounts is implemented.	Maps to 3.5.3[c]
A.03.05.03[02]	Multi-Factor Authentication	multi-factor authentication for access to non-privileged accounts is implemented.	Maps to 3.5.3[d]
A.03.05.04[01]	Replay-Resistant Authentication	replay-resistant authentication mechanisms for access to privileged accounts are implemented.	Maps to 3.5.4
A.03.05.04[02]	Replay-Resistant Authentication	replay-resistant authentication mechanisms for access to non-privileged accounts are implemented.	Maps to 3.5.4
A.03.05.07.ODP[01]	Password Management	the frequency at which to update the list of commonly used, expected, or compromised passwords is defined.	Maps to 3.5.7[b]
A.03.05.07.ODP[02]	Password Management	password composition and complexity rules are defined.	Maps to 3.5.7[a]
A.03.05.07.c	Password Management	passwords are only transmitted over cryptographically protected channels.	Maps to 3.5.10[b]
A.03.05.07.d	Password Management	passwords are stored in a cryptographically protected form.	Maps to 3.5.10[a]
A.03.05.11	Authentication Feedback	feedback of authentication information during the authentication process is obscured.	Maps to 3.5.11

A.03.06.01[01]	Incident Handling	an incident-handling capability that is consistent with the incident response plan is implemented.	Maps to 3.6.1[a] and elements of NFO - IR-8
A.03.06.01[02]	Incident Handling	the incident handling capability includes preparation.	Maps to 3.6.1[b]
A.03.06.01[03]	Incident Handling	the incident handling capability includes detection and analysis.	Maps to 3.6.1[c], 3.6.1[d]
A.03.06.01[04]	Incident Handling	the incident handling capability includes containment.	Maps to 3.6.1[e]
A.03.06.01[05]	Incident Handling	the incident handling capability includes eradication.	Maps to 3.6.1[f]
A.03.06.01[06]	Incident Handling	the incident handling capability includes recovery.	Maps to 3.6.1[g]
A.03.06.02.ODP[02]	Incident Monitoring, Reporting, and Response Assistance	authorities to whom incident information is to be reported are defined.	Maps to 3.6.2[c]
A.03.06.02.a[01]	Incident Monitoring, Reporting, and Response Assistance	system security incidents are tracked.	Maps to 3.6.2[a]
A.03.06.02.a[02]	Incident Monitoring, Reporting, and Response Assistance	system security incidents are documented.	Maps to 3.6.2[b]
A.03.06.02.b	Incident Monitoring, Reporting, and Response Assistance	suspected incidents are reported to the organizational incident response capability within <A.03.06.02.ODP[01]: time period>.	Maps to 3.6.2[f]
A.03.06.02.c	Incident Monitoring, Reporting, and Response Assistance	incident information is reported to <A.03.06.02.ODP[02]: authorities>.	Maps to 3.6.2[e]
A.03.06.03	Incident Response Testing	the effectiveness of the incident response capability is tested <A.03.06.03.ODP[01]: frequency>.	Maps to 3.6.3
A.03.07.04.a[02]	Maintenance Tools	the use of system maintenance tools is controlled.	Maps to 3.7.2[a]
A.03.07.04.b	Maintenance Tools	media with diagnostic and test programs are checked for malicious code before the media are used in the system.	Maps to 3.7.4
A.03.07.05.b[01]	Nonlocal Maintenance	multi-factor authentication is implemented in the establishment of nonlocal maintenance and diagnostic sessions.	Maps to 3.7.5[a]
A.03.07.05.c[01]	Nonlocal Maintenance	session connections are terminated when nonlocal maintenance is completed.	Maps to 3.7.5[b]
A.03.07.05.c[02]	Nonlocal Maintenance	network connections are terminated when nonlocal maintenance is completed.	Maps to 3.7.5[b]
A.03.08.01[01]	Media Storage	system media that contain CUI are physically controlled.	Maps to 3.8.1[a], 3.8.1[b]
A.03.08.01[02]	Media Storage	system media that contain CUI are securely stored.	Maps to 3.8.1[c], 3.8.1[d]

A.03.08.02	Media Access	access to CUI on system media is restricted to authorized personnel or roles.	Maps to 3.8.2
A.03.08.03	Media Sanitization	system media that contain CUI are sanitized prior to disposal, release out of organizational control, or release for reuse.	Maps to 3.7.3, 3.8.3[a], 3.8.3[b]
A.03.08.04[01]	Media Marking	system media that contain CUI are marked to indicate distribution limitations.	Maps to 3.8.4[b]
A.03.08.04[03]	Media Marking	system media that contain CUI are marked to indicate applicable CUI markings.	Maps to 3.8.4[a]
A.03.08.05.a[01]	Media Transport	system media that contain CUI are protected during transport outside of controlled areas.	Maps to 3.8.5[a]
A.03.08.05.a[02]	Media Transport	system media that contain CUI are controlled during transport outside of controlled areas.	Maps to 3.8.5[a]
A.03.08.05.b	Media Transport	accountability for system media that contain CUI is maintained during transport outside of controlled areas.	Maps to 3.8.5[b]
A.03.08.07.a	Media Use	the use of the following types of system media is restricted or prohibited: <A.03.08.07.ODP[01]: types of system media>.	Maps to 3.8.7
A.03.08.07.b	Media Use	the use of removable system media without an identifiable owner is prohibited.	Maps to 3.8.8
A.03.08.09.a	System Backup – Cryptographic Protection	the confidentiality of backup information is protected.	Maps to 3.8.9
A.03.08.09.b	System Backup – Cryptographic Protection	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI at backup storage locations.	Maps to 3.8.9
A.03.09.01.a	Personnel Screening	individuals are screened prior to authorizing access to the system.	Maps to 3.9.1
A.03.10.01.a[01]	Physical Access Authorizations	a list of individuals with authorized access to the facility where the system resides is developed.	Maps to 3.10.1[a]
A.03.10.01.a[02]	Physical Access Authorizations	a list of individuals with authorized access to the facility where the system resides is approved.	Maps to 3.10.1[a]
A.03.10.01.a[03]	Physical Access Authorizations	a list of individuals with authorized access to the facility where the system resides is maintained.	Maps to 3.10.1[a]
A.03.10.01.b	Physical Access Authorizations	authorization credentials for facility access are issued.	Maps to 3.10.1[b], 3.10.1[c], 3.10.1[d]
A.03.10.02.a[01]	Monitoring Physical Access	physical access to the facility where the system resides is monitored to detect physical security incidents.	Maps to 3.10.2[c]and elements of NFO - PE-6(1)
A.03.10.06.ODP[01]	Alternate Work Site	security requirements to be employed at alternate work sites are defined.	Maps to 3.10.6[a]
A.03.10.06.b	Alternate Work Site	the following security requirements are employed at alternate work sites: <A.03.10.06.ODP[01]: security requirements>.	Maps to 3.10.6[b]
A.03.10.07.b	Physical Access Control	physical access audit logs for entry or exit points are maintained.	Maps to 3.10.4
A.03.10.07.c[01]	Physical Access Control	visitors are escorted.	Maps to 3.10.3[a]
A.03.11.01.ODP[01]	Risk Assessment	the frequency at which to update the risk assessment is defined.	Maps to 3.11.1[a]
A.03.11.01.a	Risk Assessment	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	Maps to 3.2.1[a], 3.11.1[b]
A.03.11.01.b	Risk Assessment	risk assessments are updated <A.03.11.01.ODP[01]: frequency>.	Maps to 3.11.1[b]

A.03.11.02.ODP[02]	Vulnerability Monitoring and Scanning	the frequency at which the system is scanned for vulnerabilities is defined.	Maps to 3.11.2[a]
A.03.11.02.a[02]	Vulnerability Monitoring and Scanning	the system is scanned for vulnerabilities <A.03.11.02.ODP[02]: frequency>.	Maps to 3.11.2[b] and elements of 3.11.2[c], 3.11.3[a]
A.03.11.02.a[04]	Vulnerability Monitoring and Scanning	the system is scanned for vulnerabilities when new vulnerabilities that affect the system are identified.	Maps to 3.11.2[d] and elements of 3.11.2[c], 3.11.3[a]
A.03.12.01.ODP[01]	Security Assessment	the frequency at which to assess the security requirements for the system and its environment of operation is defined.	Maps to 3.12.1[a]
A.03.12.01	Security Assessment	the security requirements for the system and its environment of operation are assessed <A.03.12.01.ODP[01]: frequency> to determine if the requirements have been satisfied.	Maps to 3.12.1[b]
A.03.13.01.a[01]	Boundary Protection	communications at external managed interfaces to the system are monitored.	Maps to 3.13.1[c] and elements of 3.13.14[b]
A.03.13.01.a[02]	Boundary Protection	communications at external managed interfaces to the system are controlled.	Maps to 3.13.1[e], 3.13.1[g] and elements of 3.13.5[a]
A.03.13.01.a[03]	Boundary Protection	communications at key internal managed interfaces within the system are monitored.	Maps to 3.13.1[d] and elements of 3.13.14[b]
A.03.13.01.a[04]	Boundary Protection	communications at key internal managed interfaces within the system are controlled.	Maps to 3.13.1[f], 3.13.1[h]
A.03.13.04[01]	Information in Shared System Resources	unauthorized information transfer via shared system resources is prevented.	Maps to 3.13.4
A.03.13.04[02]	Information in Shared System Resources	unintended information transfer via shared system resources is prevented.	Maps to 3.13.4
A.03.13.06[01]	Network Communications – Deny by Default – Allow by Exception	network communications traffic is denied by default.	Maps to 3.13.6[a]
A.03.13.06[02]	Network Communications – Deny by Default – Allow by Exception	network communications traffic is allowed by exception.	Maps to 3.13.6[b]
A.03.13.08[01]	Transmission and Storage Confidentiality	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI during transmission.	Maps to 3.13.8[c] and elements of 3.13.8[c], 3.8.6
A.03.13.08[02]	Transmission and Storage Confidentiality	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI while in storage.	Maps to 3.13.8[c] and elements of 3.13.8[c], 3.8.6, 3.13.16
A.03.13.09.ODP[01]	Network Disconnect	the time period of inactivity after which the system terminates a network connection associated with a communications session is defined.	Maps to 3.13.9[a]
A.03.13.09	Network Disconnect	the network connection associated with a communications session is terminated at the end of the session or after <A.03.13.09.ODP[01]: time period> of inactivity.	Maps to 3.13.9[b], 3.13.9[c]
A.03.13.10[01]	Cryptographic Key Establishment	cryptographic keys are established in the system in accordance with the following key management requirements: <A.03.13.10.ODP[01]: requirements>.	Maps to 3.13.10[a]

	and Management		
A.03.13.10[02]	Cryptographic Key Establishment and Management	cryptographic keys are managed in the system in accordance with the following key management requirements: <A.03.13.10.ODP[01]: requirements>.	Maps to 3.13.10[b]
A.03.13.12.a	Collaborative Computing Devices and Applications	the remote activation of collaborative computing devices and applications is prohibited with the following exceptions: <A.03.13.12.ODP[01]: exceptions>.	Maps to 3.13.12[c]
A.03.13.12.b	Collaborative Computing Devices and Applications	an explicit indication of use is provided to users who are physically present at the devices.	Maps to 3.13.12[b]
A.03.13.13.b[01]	Mobile Code	the use of mobile code is authorized.	Maps to 3.13.13[a]
A.03.13.13.b[02]	Mobile Code	the use of mobile code is monitored.	Maps to 3.13.13[b]
A.03.13.13.b[03]	Mobile Code	the use of mobile code is controlled.	Maps to 3.13.13[a]
A.03.13.15	Session Authenticity	the authenticity of communications sessions is protected.	Maps to 3.13.15
A.03.14.01.a[01]	Flaw Remediation	system flaws are identified.	Maps to 3.14.1[b]
A.03.14.01.a[02]	Flaw Remediation	system flaws are reported.	Maps to 3.14.1[d]
A.03.14.01.a[03]	Flaw Remediation	system flaws are corrected.	Maps to 3.14.1[f]
A.03.14.02.ODP[01]	Malicious Code Protection	the frequency at which malicious code protection mechanisms perform scans is defined.	Maps to 3.14.5[a]
A.03.14.02.a[01]	Malicious Code Protection	malicious code protection mechanisms are implemented at system entry and exit points to detect malicious code.	Maps to 3.14.2[a]
A.03.14.02.a[02]	Malicious Code Protection	malicious code protection mechanisms are implemented at system entry and exit points to eradicate malicious code.	Maps to 3.14.2[b]
A.03.14.02.b	Malicious Code Protection	malicious code protection mechanisms are updated as new releases are available in accordance with configuration management policy and procedures.	Maps to 3.14.4
A.03.14.02.c.01[01]	Malicious Code Protection	malicious code protection mechanisms are configured to perform scans of the system <A.03.14.02.ODP[01]: frequency>.	Maps to 3.14.5[b]
A.03.14.02.c.01[02]	Malicious Code Protection	malicious code protection mechanisms are configured to perform real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed.	Maps to 3.14.5[c]
A.03.14.03.a	Security Alerts, Advisories, and Directives	system security alerts, advisories, and directives from external organizations are received on an ongoing basis.	Maps to 3.14.3[b]
A.03.14.06.a.01[01]	System Monitoring	the system is monitored to detect attacks.	Maps to 3.14.6[a]
A.03.14.06.a.01[02]	System Monitoring	the system is monitored to detect indicators of potential attacks.	Maps to 3.14.6[b]
A.03.14.06.a.02	System Monitoring	the system is monitored to detect unauthorized connections.	Maps to 3.14.6[a], 3.14.6[c]

A.03.14.06.b	System Monitoring	unauthorized use of the system is identified.	Maps to 3.14.7[b]
A.03.14.06.c[01]	System Monitoring	inbound communications traffic is monitored to detect unusual or unauthorized activities or conditions.	Maps to 3.14.6[b]
A.03.14.06.c[02]	System Monitoring	outbound communications traffic is monitored to detect unusual or unauthorized activities or conditions.	Maps to 3.14.6[c]
A.03.15.01.a[01]	Policy and Procedures	policies needed to satisfy the security requirements for the protection of CUI are developed and documented.	Maps to 3.2.1[b] and elements of 3.9.2[a]
A.03.15.01.a[02]	Policy and Procedures	policies needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.	Maps to 3.2.1[b]
A.03.15.01.a[03]	Policy and Procedures	procedures needed to satisfy the security requirements for the protection of CUI are developed and documented.	Maps to 3.2.1[b] and elements of 3.9.2[a]
A.03.15.01.a[04]	Policy and Procedures	procedures needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.	Maps to 3.2.1[b]
A.03.15.02.ODP[01]	System Security Plan	the frequency at which the system security plan is reviewed and updated is defined.	Maps to 3.12.4[g]
A.03.15.02.a.01	System Security Plan	a system security plan that defines the constituent system components is developed.	Maps to 3.12.4[a]
A.03.15.02.a.04	System Security Plan	a system security plan that describes the operational environment for the system and any dependencies on or connections to other systems or system components is developed.	Maps to 3.12.4[b], 3.12.4[c], 3.12.4[f]
A.03.15.02.a.05	System Security Plan	a system security plan that provides an overview of the security requirements for the system is developed.	Maps to 3.12.4[d]
A.03.15.02.a.06	System Security Plan	a system security plan that describes the safeguards in place or planned for meeting the security requirements is developed.	Maps to 3.12.4[e]
A.03.15.02.b[01]	System Security Plan	the system security plan is reviewed <A.03.15.02.ODP[01]: frequency>.	Maps to 3.12.4.[h]
A.03.15.02.b[02]	System Security Plan	the system security plan is updated <A.03.15.02.ODP[01]: frequency>.	Maps to 3.12.4.[h]

Moderate Effort Assessment Objective Transition

For organizations that currently have controls in place for NIST 800-171 R2 and leverage NIST 800-171A, approximately one-fifth of the AOs in NIST 800-171A R3 should be considered moderate effort from a transition perspective.

NIST 800-171A R3 AOs With Indirect Mapping (Existing NIST 800-171 R3 Control)

The following AOs have "indirect mapping" which means that there are elements of the NIST 800-171A R3 AO that can be mapped back to an existing NIST 800-171A AO. The indirect nature of the mapping indicates that organizations will have to perform more detailed analysis of what the transition to the new AO requires.

NIST 800-171A R3	NIST 800-171 R3 Control Name	NIST 800-171A R3 Assessment Objective (AO)	NIST 800-171 R2 to R3 Upgrade Notes
A.03.01.01.d.01	Account Management	access to the system is authorized based on a valid access authorization.	Elements of 3.1.1[c], 3.1.1[d], 3.1.1[e], 3.1.1[f]
A.03.01.01.d.02	Account Management	access to the system is authorized based on intended system usage.	Elements of 3.1.1[c], 3.1.1[d], 3.1.1[e], 3.1.1[f]
A.03.01.02[01]	Access Enforcement	approved authorizations for logical access to CUI are enforced in accordance with applicable access control policies.	Elements of 3.1.2[b]
A.03.01.02[02]	Access Enforcement	approved authorizations for logical access to system resources are enforced in accordance with applicable access control policies.	Elements of 3.1.2[b]
A.03.01.03[01]	Information Flow Enforcement	approved authorizations are enforced for controlling the flow of CUI within the system.	Elements of 3.1.3[e]
A.03.01.03[02]	Information Flow Enforcement	approved authorizations are enforced for controlling the flow of CUI between connected systems.	Elements of 3.1.3[e]
A.03.01.04.b	Separation of Duties	system access authorizations to support separation of duties are defined.	Elements of 3.1.4[b], 3.1.4[c]
A.03.01.05.ODP[01]	Least Privilege	security functions for authorized access are defined.	Elements of 3.1.5[c], 3.13.3[a], 3.13.3[b], 3.13.3[c]
A.03.01.05.a	Least Privilege	system access for users (or processes acting on behalf of users) is authorized only when necessary to accomplish assigned organizational tasks.	Elements of 3.1.5[b]
A.03.01.06.ODP[01]	Least Privilege – Privileged Accounts	personnel or roles to which privileged accounts on the system are to be restricted are defined.	Elements of 3.13.3[a], 3.13.3[b], 3.13.3[c]
A.03.01.06.a	Least Privilege – Privileged Accounts	privileged accounts on the system are restricted to <A.03.01.06.ODP[01]: personnel or roles>.	Elements of 3.13.3[a], 3.13.3[b], 3.13.3[c]
A.03.01.06.b	Least Privilege – Privileged Accounts	users (or roles) with privileged accounts are required to use non-privileged accounts when accessing non-security functions or non-security information.	Elements of 3.13.3[a], 3.13.3[b], 3.13.3[c]
A.03.01.08.ODP[02]	Unsuccessful Logon Attempts	the time period to which the number of consecutive invalid logon attempts by a user is limited is defined.	Elements of 3.1.8[b]
A.03.01.08.ODP[03]	Unsuccessful Logon Attempts	one or more of the following PARAMETER VALUES are selected: {the account or node is locked automatically for <A.03.01.08.ODP[04]: time period>; the account or node is locked automatically until released by an administrator; the next logon prompt is delayed automatically; the system administrator is notified automatically; other action is taken automatically}.	Elements of 3.1.8[b]

A.03.01.08.ODP[04]	Unsuccessful Logon Attempts	the time period for an account or node to be locked is defined (if selected).	Elements of 3.1.8[b]
A.03.01.08.a	Unsuccessful Logon Attempts	a limit of <A.03.01.08.ODP[01]: number> consecutive invalid logon attempts by a user during <A.03.01.08.ODP[02]: time period> is enforced.	Elements of 3.1.8[b]
A.03.01.08.b	Unsuccessful Logon Attempts	<A.03.01.08.ODP[03]: SELECTED PARAMETER VALUES> when the maximum number of unsuccessful attempts is exceeded.	Elements of 3.1.8[b]
A.03.01.12.a[02]	Remote Access	usage restrictions are established for each type of allowable remote system access.	Elements of 3.1.12[a], 3.1.12[c], 3.1.15[a], 3.1.15[b], 3.1.15[c], 3.1.15[d]
A.03.01.12.a[03]	Remote Access	configuration requirements are established for each type of allowable remote system access.	Elements of 3.1.12[c], 3.1.13[a], 3.1.13[b], 3.13.7
A.03.01.16.a[01]	Wireless Access	each type of wireless access to the system is defined.	Elements of 3.1.16[a]
A.03.01.18.a[03]	Access Control for Mobile Devices	connection requirements are established for mobile devices.	Elements of 3.1.18[b]
A.03.01.20.ODP[01]	Use of External Systems	security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are defined.	Elements of 3.1.20[e]
A.03.01.20.a	Use of External Systems	the use of external systems is prohibited unless the systems are specifically authorized.	Elements of 3.1.21[a], 3.1.21[b], 3.1.21[c]
A.03.01.20.b	Use of External Systems	the following security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are established: <A.03.01.20.ODP[01]: security requirements>.	Elements of 3.1.20[e], 3.1.20[f]
A.03.01.20.c.01	Use of External Systems	authorized individuals are permitted to use external systems to access the organizational system or to process, store, or transmit CUI only after verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied.	Elements of 3.1.20[c]
A.03.01.20.c.02	Use of External Systems	authorized individuals are permitted to use external systems to access the organizational system or to process, store, or transmit CUI only after retaining approved system connection or processing agreements with the organizational entity hosting the external systems.	Elements of 3.1.20[e], 3.1.20[f]
A.03.01.20.d	Use of External Systems	the use of organization-controlled portable storage devices by authorized individuals on external systems is restricted.	Elements of 3.1.20[f]
A.03.02.01.a.01[01]	Literacy Training and Awareness	security literacy training is provided to system users as part of initial training for new users.	Elements of 3.2.1[c], 3.2.1[d]
A.03.02.01.a.01[02]	Literacy Training and Awareness	security literacy training is provided to system users <A.03.02.01.ODP[01]: frequency> after initial training.	Elements of 3.2.1[c], 3.2.1[d]
A.03.02.01.a.02	Literacy Training and Awareness	security literacy training is provided to system users when required by system changes or following <A.03.02.01.ODP[02]: events>.	Elements of 3.2.1[c], 3.2.1[d]
A.03.02.01.a.03[02]	Literacy Training and Awareness	security literacy training is provided to system users on reporting indicators of insider threat.	Elements of 3.2.1[c], 3.2.1[d]

A.03.02.01.a.03[03]	Literacy Training and Awareness	security literacy training is provided to system users on recognizing indicators of social engineering.	Elements of 3.2.1[c], 3.2.1[d]
A.03.02.01.a.03[04]	Literacy Training and Awareness	security literacy training is provided to system users on reporting indicators of social engineering.	Elements of 3.2.1[c], 3.2.1[d]
A.03.02.01.a.03[05]	Literacy Training and Awareness	security literacy training is provided to system users on recognizing indicators of social mining.	Elements of 3.2.1[c], 3.2.1[d]
A.03.02.01.a.03[06]	Literacy Training and Awareness	security literacy training is provided to system users on reporting indicators of social mining.	Elements of 3.2.1[c], 3.2.1[d]
A.03.03.01.b[01]	Event Logging	the event types selected for logging are reviewed <A.03.03.01.ODP[02]: frequency>.	Elements of 3.3.3[a], 3.3.3[b]
A.03.03.02.a.01	Audit Record Content	audit records contain information that establishes what type of event occurred.	Elements of 3.3.2[a], 3.3.2[b]
A.03.03.02.a.02	Audit Record Content	audit records contain information that establishes when the event occurred.	Elements of 3.3.2[a], 3.3.2[b]
A.03.03.02.a.03	Audit Record Content	audit records contain information that establishes where the event occurred.	Elements of 3.3.2[a], 3.3.2[b]
A.03.03.02.a.04	Audit Record Content	audit records contain information that establishes the source of the event.	Elements of 3.3.2[a], 3.3.2[b]
A.03.03.02.a.05	Audit Record Content	audit records contain information that establishes the outcome of the event.	Elements of 3.3.2[a], 3.3.2[b]
A.03.03.02.a.06	Audit Record Content	audit records contain information that establishes the identity of the individuals, subjects, objects, or entities associated with the event.	Elements of 3.3.2[a], 3.3.2[b]
A.03.03.02.b	Audit Record Content	additional information for audit records is provided, as needed.	Elements of 3.3.2[a], 3.3.2[b]
A.03.03.06.a[04]	Audit Record Reduction and Report Generation	an audit record reduction and report generation capability that supports after-the-fact investigations of incidents is implemented.	Elements of 3.3.6[a], 3.3.6[b]
A.03.03.06.b[01]	Audit Record Reduction and Report Generation	the original content of audit records is preserved.	Elements of 3.3.1[e]
A.03.03.06.b[02]	Audit Record Reduction and Report Generation	the original time ordering of audit records is preserved.	Elements of 3.3.1[e], 3.3.7[a]
A.03.04.01.ODP[01]	Baseline Configuration	the frequency of baseline configuration review and update is defined.	Elements of 3.4.1[c] and NFO - CM-2(1)
A.03.04.01.b[01]	Baseline Configuration	the baseline configuration of the system is reviewed <A.03.04.01.ODP[01]: frequency>.	Elements of 3.4.1[c]
A.03.04.01.b[02]	Baseline Configuration	the baseline configuration of the system is updated <A.03.04.01.ODP[01]: frequency>.	Elements of 3.4.1[c]
A.03.04.01.b[03]	Baseline Configuration	the baseline configuration of the system is reviewed when system components are installed or modified.	Elements of 3.4.1[c]
A.03.04.01.b[04]	Baseline Configuration	the baseline configuration of the system is updated when system components are installed or modified.	Elements of 3.4.1[c]
A.03.04.02.a[02]	Configuration Settings	the following configuration settings for the system are implemented: <A.03.04.02.ODP[01]: configuration settings>.	Elements of 3.4.2[a]
A.03.04.02.b[01]	Configuration Settings	any deviations from established configuration settings are identified and documented.	Elements of 3.4.2[b]

A.03.04.02.b[02]	Configuration Settings	any deviations from established configuration settings are approved.	Elements of 3.4.2[b]
A.03.04.03.c[01]	Configuration Change Control	approved configuration-controlled changes to the system are implemented.	Elements of 3.7.1
A.03.04.06.ODP[01]	Least Functionality	functions to be prohibited or restricted are defined.	Elements of multiple 3.4.7 AOs. No clear mapping.
A.03.04.06.ODP[02]	Least Functionality	ports to be prohibited or restricted are defined.	Elements of multiple 3.4.7 AOs and NFO - SA-9(2). No clear mapping.
A.03.04.06.ODP[03]	Least Functionality	protocols to be prohibited or restricted are defined.	Elements of multiple 3.4.7 AOs and NFO - SA-9(2). No clear mapping.
A.03.04.06.ODP[04]	Least Functionality	connections to be prohibited or restricted are defined.	Elements of multiple 3.4.7 AOs. No clear mapping.
A.03.04.06.ODP[05]	Least Functionality	services to be prohibited or restricted are defined.	Elements of multiple 3.4.7 AOs and NFO - SA-9(2). No clear mapping.
A.03.04.06.ODP[06]	Least Functionality	the frequency at which to review the system to identify unnecessary or nonsecure functions, ports, protocols, connections, or services is defined.	Elements of multiple 3.4.7 AOs. No clear mapping.
A.03.04.06.a	Least Functionality	the system is configured to provide only mission-essential capabilities.	Elements of multiple 3.4.7 Aos, 3.13.7 and 3.13.14[a]. No clear mapping.
A.03.04.06.b[01]	Least Functionality	the use of the following functions is prohibited or restricted: <A.03.04.06.ODP[01]: functions>.	Elements of multiple 3.4.7 Aos, 3.13.7 and 3.13.14[a]. No clear mapping.
A.03.04.06.b[02]	Least Functionality	the use of the following ports is prohibited or restricted: <A.03.04.06.ODP[02]: ports>.	Elements of multiple 3.4.7 Aos, 3.13.7 and 3.13.14[a]. No clear mapping.
A.03.04.06.b[03]	Least Functionality	the use of the following protocols is prohibited or restricted: <A.03.04.06.ODP[03]: protocols>.	Elements of multiple 3.4.7 Aos, 3.13.7 and 3.13.14[a]. No clear mapping.
A.03.04.06.b[04]	Least Functionality	the use of the following connections is prohibited or restricted: <A.03.04.06.ODP[04]: connections>.	Elements of multiple 3.4.7 Aos, 3.13.7 and 3.13.14[a]. No clear mapping.
A.03.04.06.b[05]	Least Functionality	the use of the following services is prohibited or restricted: <A.03.04.06.ODP[05]: services>.	Elements of multiple 3.4.7 Aos, 3.13.7 and 3.13.14[a]. No clear mapping.
A.03.04.06.c	Least Functionality	the system is reviewed <A.03.04.06.ODP[06]: frequency> to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.	Elements of multiple 3.4.7 AOs. No clear mapping.
A.03.04.06.d	Least Functionality	unnecessary or nonsecure functions, ports, protocols, connections, and services are disabled or removed.	Elements of multiple 3.4.7 AOs. No clear mapping.
A.03.04.08.ODP[01]	Authorized Software – Allow by Exception	the frequency at which to review and update the list of authorized software programs is defined.	Elements of 3.4.9[c]

A.03.04.08.c	Authorized Software – Allow by Exception	the list of authorized software programs is reviewed and updated <A.03.04.08.ODP[01]: frequency>.	Elements of 3.4.9[c]
A.03.04.10.b[01]	System Component Inventory	the system component inventory is reviewed <A.03.04.10.ODP[01]: frequency>.	Elements exist in NIST 800-171A R3 as 3.4.1[f]
A.03.04.10.b[02]	System Component Inventory	the system component inventory is updated <A.03.04.10.ODP[01]: frequency>.	Elements exist in NIST 800-171A R3 as 3.4.1[f]
A.03.04.10.c[01]	System Component Inventory	the system component inventory is updated as part of component installations.	Elements exist in NIST 800-171A R3 as 3.4.1[f]
A.03.04.10.c[02]	System Component Inventory	the system component inventory is updated as part of component removals.	Elements exist in NIST 800-171A R3 as 3.4.1[f]
A.03.04.10.c[03]	System Component Inventory	the system component inventory is updated as part of system updates.	Elements exist in NIST 800-171A R3 as 3.4.1[f]
A.03.05.01.a[01]	User Identification and Authentication	system users are uniquely identified.	Elements of 3.5.1[a], 3.5.1[b], 3.5.1[c]
A.03.05.05.ODP[01]	Identifier Management	the time period for preventing the reuse of identifiers is defined.	3.5.5[a]
A.03.05.05.c	Identifier Management	the reuse of identifiers for <A.03.05.05.ODP[01]: time period> is prevented.	3.5.5[b]
A.03.05.07.e	Password Management	a new password is selected upon first use after account recovery.	elements of 3.5.9
A.03.05.07.f	Password Management	the following composition and complexity rules for passwords are enforced: <A.03.05.07.ODP[02]: rules>.	elements of 3.5.7[c], 3.5.7[d]
A.03.07.04.a[01]	Maintenance Tools	the use of system maintenance tools is approved.	Elements of 3.7.2[b], 3.7.2[c]
A.03.07.06.a	Maintenance Personnel	a process for maintenance personnel authorization is established.	Elements of 3.7.2[d]
A.03.07.06.b	Maintenance Personnel	a list of authorized maintenance organizations or personnel is maintained.	Elements of 3.7.2[d]
A.03.07.06.c	Maintenance Personnel	non-escorted personnel who perform maintenance on the system possess the required access authorizations.	Elements of 3.7.2[d]
A.03.07.06.d[01]	Maintenance Personnel	organizational personnel with required access authorizations are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Elements of 3.7.6
A.03.07.06.d[02]	Maintenance Personnel	organizational personnel with required technical competence are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Elements of 3.7.6
A.03.09.02.a.01	Personnel Termination and Transfer	upon termination of individual employment, system access is disabled within <A.03.09.02.ODP[01]: time period>.	Elements of 3.9.2[a]
A.03.09.02.a.02[01]	Personnel Termination and Transfer	upon termination of individual employment, authenticators associated with the individual are terminated or revoked.	Elements of 3.9.2[b]

A.03.09.02.a.02[02]	Personnel Termination and Transfer	upon termination of individual employment, credentials associated with the individual are terminated or revoked.	Elements of 3.9.2[b]
A.03.09.02.b.01[01]	Personnel Termination and Transfer	upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is reviewed.	Elements of 3.9.2[b]
A.03.09.02.b.01[02]	Personnel Termination and Transfer	upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is confirmed.	Elements of 3.9.2[b]
A.03.09.02.b.02	Personnel Termination and Transfer	upon individual reassignment or transfer to other positions in the organization, access authorization is modified to correspond with any changes in operational need.	Elements of 3.9.2[c]
A.03.10.07.c[02]	Physical Access Control	visitor activity is controlled.	Elements of 3.10.3[b] and NFO - PE-8
A.03.10.07.d	Physical Access Control	keys, combinations, and other physical access devices are secured.	Elements of 3.10.5[a], 3.10.5[b], 3.10.5[c]
A.03.11.02.a[03]	Vulnerability Monitoring and Scanning	the system is monitored for vulnerabilities when new vulnerabilities that affect the system are identified.	Elements of 3.11.3[a]
A.03.11.02.b	Vulnerability Monitoring and Scanning	system vulnerabilities are remediated within <A.03.11.02.ODP[03]: response times>.	Elements of 3.11.3[b]
A.03.12.02.a.01	Plan of Action and Milestones	a plan of action and milestones for the system is developed to document the planned remediation actions for correcting weaknesses or deficiencies noted during security assessments.	Elements of 3.12.2[a], 3.12.2[b], 3.12.2[c]
A.03.12.02.a.02	Plan of Action and Milestones	a plan of action and milestones for the system is developed to reduce or eliminate known system vulnerabilities.	Elements of 3.12.2[a], 3.12.2[b], 3.12.2[c]
A.03.12.03[01]	Continuous Monitoring	a system-level continuous monitoring strategy is developed.	Elements of 3.12.3
A.03.12.03[02]	Continuous Monitoring	a system-level continuous monitoring strategy is implemented.	Elements of 3.12.3
A.03.12.03[03]	Continuous Monitoring	ongoing monitoring is included in the continuous monitoring strategy.	Elements of 3.12.3
A.03.12.03[04]	Continuous Monitoring	security assessments are included in the continuous monitoring strategy.	Elements of 3.12.3
A.03.13.01.b	Boundary Protection	subnetworks are implemented for publicly accessible system components that are physically or logically separated from internal networks.	Elements of 3.13.5[b]
A.03.13.11	Cryptographic Protection	the following types of cryptography are implemented to protect the confidentiality of CUI: <A.03.13.11.ODP[01]: types of cryptography>.	Elements of 3.13.11
A.03.16.01.ODP[01]	Security Engineering Principles	systems security engineering principles to be applied to the development or modification of the system and system components are defined.	Elements of 3.13.2[a], 3.13.2[b], 3.13.2[c], 3.13.2[d], 3.13.2[e], 3.13.2[f] and NFO - PL-8
A.03.16.01	Security Engineering Principles	<A.03.16.01.ODP[01]: systems security engineering principles> are applied to the development or modification of the system and system components.	Elements of 3.13.2[a], 3.13.2[b], 3.13.2[c], 3.13.2[d], 3.13.2[e], 3.13.2[f] and NFO - PL-8
A.03.16.03.ODP[01]	External System Services	security requirements to be satisfied by external system service providers are defined.	Elements of 3.1.20[f]

A.03.16.03.a	External System Services	the providers of external system services used for the processing, storage, or transmission of CUI comply with the following security requirements: <A.03.16.03.ODP[01]: security requirements>.	Elements of 3.1.20[f]
A.03.16.03.b	External System Services	user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers, are defined and documented.	Elements of 3.2.2[a], 3.2.2[b]

Significant Effort Assessment Objective Transition

For organizations that currently have controls in place for NIST 800-171 R2 and leverage NIST 800-171A, approximately half of the AOs in NIST 800-171A R3 should be considered significant effort from a transition perspective.

NIST 800-171A R3 AOs With No Clear Mapping (Existing NIST 800-171 R3 Control)

The following AOs have "no clear mapping" which means that there is no clear mapping from the NIST 800-171A R3 AO to an existing NIST 800-171A AO. The lack of mapping indicates that organizations will have to perform detailed analysis of what the transition to the new AO requires.

NIST 800-171A R3	NIST 800-171 R3 Control Name	NIST 800-171A R3 Assessment Objective (AO)	NIST 800-171 R2 to R3 Upgrade Notes
A.03.01.01.ODP[02]	Account Management	the time period within which to notify account managers and designated personnel or roles when accounts are no longer required is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.01.ODP[03]	Account Management	the time period within which to notify account managers and designated personnel or roles when users are terminated or transferred is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.01.ODP[04]	Account Management	the time period within which to notify account managers and designated personnel or roles when system usage or the need-to-know changes for an individual is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.01.ODP[05]	Account Management	the time period of expected inactivity requiring users to log out of the system is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.01.ODP[06]	Account Management	circumstances requiring users to log out of the system are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.05.ODP[02]	Least Privilege	security-relevant information for authorized access is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.05.ODP[03]	Least Privilege	the frequency at which to review the privileges assigned to roles or classes of users is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.12.a[04]	Remote Access	connection requirements are established for each type of allowable remote system access.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.16.a[02]	Wireless Access	usage restrictions are established for each type of wireless access to the system.	This NIST 800-171A R3 AO does not have a clear link to an AO from the

			previous version of NIST 800-171A
A.03.01.18.a[01]	Access Control for Mobile Devices	usage restrictions are established for mobile devices.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.18.a[02]	Access Control for Mobile Devices	configuration requirements are established for mobile devices.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.01.22.a	Publicly Accessible Content	authorized individuals are trained to ensure that publicly accessible information does not contain CUI.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.02.01.ODP[01]	Literacy Training and Awareness	the frequency at which to provide security literacy training to system users after initial training is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.02.01.ODP[02]	Literacy Training and Awareness	events that require security literacy training for system users are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.02.01.ODP[03]	Literacy Training and Awareness	the frequency at which to update security literacy training content is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.02.01.ODP[04]	Literacy Training and Awareness	events that require security literacy training content updates are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.02.02.ODP[01]	Role-Based Training	the frequency at which to provide role-based security training to assigned personnel after initial training is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.02.02.ODP[02]	Role-Based Training	events that require role-based security training are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.02.02.ODP[03]	Role-Based Training	the frequency at which to update role-based security training content is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.03.01.ODP[02]	Event Logging	the frequency of event types selected for logging are reviewed and updated.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A

A.03.03.04.ODP[01]	Response to Audit Logging Process Failures	the time period for organizational personnel or roles receiving audit logging process failure alerts is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.03.04.ODP[02]	Response to Audit Logging Process Failures	additional actions to be taken in the event of an audit logging process failure are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.03.05.ODP[01]	Audit Record Review, Analysis, and Reporting	the frequency at which system audit records are reviewed and analyzed is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.03.07.ODP[01]	Time Stamps	granularity of time measurement for audit record time stamps is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.04.03.a	Configuration Change Control	the types of changes to the system that are configuration-controlled are defined.	Elements of NFO - CM-9
A.03.04.12.ODP[01]	System and Component Configuration for High-Risk Areas	configurations for systems or system components to be issued to individuals traveling to high-risk locations are defined.	Elements of NFO - CM-2(7)
A.03.05.01.ODP[01]	User Identification and Authentication	circumstances or situations that require re-authentication are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.05.02.ODP[01]	Device Identification and Authentication	devices or types of devices to be uniquely identified and authenticated before establishing a connection are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.05.02[01]	Device Identification and Authentication	<A.03.05.02.ODP[01]: devices or types of devices> are uniquely identified before establishing a system connection.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.05.05.ODP[02]	Identifier Management	characteristic used to identify individual status are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.05.07.a[01]	Password Management	a list of commonly used, expected, or compromised passwords is maintained.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.05.07.a[02]	Password Management	a list of commonly used, expected, or compromised passwords is updated <A.03.05.07.ODP[01]: frequency>.	This NIST 800-171A R3 AO does not have a clear link to an AO from the

			previous version of NIST 800-171A
A.03.06.02.ODP[01]	Incident Monitoring, Reporting, and Response Assistance	the time period to report suspected incidents to the organizational incident response capability is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.07.05.a[01]	Nonlocal Maintenance	nonlocal maintenance and diagnostic activities are approved.	Elements of NFO - MA-4(2)
A.03.07.05.a[02]	Nonlocal Maintenance	nonlocal maintenance and diagnostic activities are monitored.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.08.04[02]	Media Marking	system media that contain CUI are marked to indicate handling caveats.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.09.02.ODP[01]	Personnel Termination and Transfer	the time period within which to disable system access is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.10.01.ODP[01]	Physical Access Authorizations	the frequency at which to review the access list detailing authorized facility access by individuals is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.10.02.ODP[01]	Monitoring Physical Access	the frequency at which to review physical access logs is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.10.02.ODP[02]	Monitoring Physical Access	events or potential indications of events requiring physical access logs to be reviewed are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.10.02.a[02]	Monitoring Physical Access	physical security incidents are responded to.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.10.06.a	Alternate Work Site	alternate work sites allowed for use by employees are determined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.11.02.ODP[01]	Vulnerability Monitoring and Scanning	the frequency at which the system is monitored for vulnerabilities is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.11.02.ODP[03]	Vulnerability Monitoring and Scanning	response times to remediate system vulnerabilities are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the

			previous version of NIST 800-171A
A.03.11.02.ODP[04]	Vulnerability Monitoring and Scanning	the frequency at which to update system vulnerabilities to be scanned is defined.	Elements of NFO - NFO - RA-5(1), RA-5(2)
A.03.11.02.a[01]	Vulnerability Monitoring and Scanning	the system is monitored for vulnerabilities <A.03.11.02.ODP[01]: frequency>.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.12.02.b.01	Plan of Action and Milestones	the existing plan of action and milestones is updated based on the findings from security assessments.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.13.01.c	Boundary Protection	external system connections are only made through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.13.10.ODP[01]	Cryptographic Key Establishment and Management	requirements for key generation, distribution, storage, access, and destruction are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.13.12.ODP[01]	Collaborative Computing Devices and Applications	exceptions where remote activation is to be allowed are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.13.13.a[01]	Mobile Code	acceptable mobile code is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.13.13.a[02]	Mobile Code	acceptable mobile code technologies are defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.14.01.ODP[01]	Flaw Remediation	the time period within which to install security-relevant software updates after the release of the updates is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.14.01.ODP[02]	Flaw Remediation	the time period within which to install security-relevant firmware updates after the release of the updates is defined.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.14.01.b[01]	Flaw Remediation	security-relevant software updates are installed within <A.03.14.01.ODP[01]: time period> of the release of the updates.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A

A.03.14.03.b[01]	Security Alerts, Advisories, and Directives	internal security alerts, advisories, and directives are generated, as necessary.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A
A.03.14.03.b[02]	Security Alerts, Advisories, and Directives	internal security alerts, advisories, and directives are disseminated, as necessary.	This NIST 800-171A R3 AO does not have a clear link to an AO from the previous version of NIST 800-171A

NIST 800-171A R3 AOs With No Transition Path (Newly Added NIST 800-171 R3 Control)

The following AOs are associated with a new AO for NIST 800-171A R3. The reality is these are net new AOs without a transition from an existing AO:

NIST 800-171A R3	NIST 800-171 R3 Control Name	NIST 800-171A R3 Assessment Objective (AO)	NIST 800-171 R2 to R3 Upgrade Notes
A.03.01.01.a[01]	Account Management	system account types allowed are defined.	AO is new for NIST 800-171A R3
A.03.01.01.a[02]	Account Management	system account types prohibited are defined.	AO is new for NIST 800-171A R3
A.03.01.01.b[01]	Account Management	system accounts are created in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3
A.03.01.01.b[02]	Account Management	system accounts are enabled in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3
A.03.01.01.b[03]	Account Management	system accounts are modified in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3
A.03.01.01.b[04]	Account Management	system accounts are disabled in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3
A.03.01.01.b[05]	Account Management	system accounts are removed in accordance with organizational policy, procedures, prerequisites, and criteria.	AO is new for NIST 800-171A R3
A.03.01.01.c.02	Account Management	group and role memberships are specified.	AO is new for NIST 800-171A R3
A.03.01.01.c.03	Account Management	access authorizations (i.e., privileges) for each account are specified.	AO is new for NIST 800-171A R3
A.03.01.01.e	Account Management	the use of system accounts is monitored.	AO is new for NIST 800-171A R3
A.03.01.01.f.01	Account Management	system accounts are disabled when the accounts have expired.	AO is new for NIST 800-171A R3
A.03.01.01.f.03	Account Management	system accounts are disabled when the accounts are no longer associated with a user or individual.	AO is new for NIST 800-171A R3
A.03.01.01.f.04	Account Management	system accounts are disabled when the accounts violate organizational policy.	AO is new for NIST 800-171A R3
A.03.01.01.f.05	Account Management	system accounts are disabled when significant risks associated with individuals are discovered.	AO is new for NIST 800-171A R3
A.03.01.01.g.01	Account Management	account managers and designated personnel or roles are notified within <A.03.01.01.ODP[02]: time period> when accounts are no longer required.	AO is new for NIST 800-171A R3
A.03.01.01.g.02	Account Management	account managers and designated personnel or roles are notified within <A.03.01.01.ODP[03]: time period> when users are terminated or transferred.	AO is new for NIST 800-171A R3
A.03.01.01.g.03	Account Management	account managers and designated personnel or roles are notified within <A.03.01.01.ODP[04]: time period> when system usage or the need-to-know changes for an individual.	AO is new for NIST 800-171A R3
A.03.01.01.h	Account Management	users are required to log out of the system after <A.03.01.01.ODP[05]: time period> of expected inactivity or when the following circumstances occur: <A.03.01.01.ODP[06]: circumstances>.	AO is new for NIST 800-171A R3
A.03.01.05.b[02]	Least Privilege	access to <A.03.01.05.ODP[02]: security-relevant information> is authorized.	AO is new for NIST 800-171A R3

A.03.01.05.c	Least Privilege	the privileges assigned to roles or classes of users are reviewed <A.03.01.05.ODP[03]: frequency> to validate the need for such privileges.	AO is new for NIST 800-171A R3
A.03.01.05.d	Least Privilege	privileges are reassigned or removed, as necessary.	AO is new for NIST 800-171A R3
A.03.01.10.b	Device Lock	the device lock is retained until the user reestablishes access using established identification and authentication procedures.	AO is new for NIST 800-171A R3
A.03.01.12.b	Remote Access	each type of remote system access is authorized prior to establishing such connections.	AO is new for NIST 800-171A R3
A.03.01.12.c[01]	Remote Access	remote access to the system is routed through authorized access control points.	AO is new for NIST 800-171A R3. Elements of NFO - SC-7(3)
A.03.01.12.d[1]	Remote Access	remote execution of privileged commands is authorized.	AO is new for NIST 800-171A R3
A.03.01.12.d[2]	Remote Access	remote access to security-relevant information is authorized.	AO is new for NIST 800-171A R3
A.03.01.16.a[03]	Wireless Access	configuration requirements are established for each type of wireless access to the system.	AO is new for NIST 800-171A R3
A.03.01.16.a[04]	Wireless Access	connection requirements are established for each type of wireless access to the system.	AO is new for NIST 800-171A R3
A.03.01.16.c	Wireless Access	wireless networking capabilities not intended for use are disabled prior to issuance and deployment.	AO is new for NIST 800-171A R3
A.03.02.01.b[01]	Literacy Training and Awareness	security literacy training content is updated <A.03.02.01.ODP[03]: frequency>.	AO is new for NIST 800-171A R3
A.03.02.01.b[02]	Literacy Training and Awareness	security literacy training content is updated following <A.03.02.01.ODP[04]: events>.	AO is new for NIST 800-171A R3
A.03.02.02.ODP[04]	Role-Based Training	events that require role-based security training content updates are defined.	AO is new for NIST 800-171A R3
A.03.02.02.b[02]	Role-Based Training	role-based security training content is updated following <A.03.02.02.ODP[04]: events>.	AO is new for NIST 800-171A R3
A.03.03.04.b	Response to Audit Logging Process Failures	the following additional actions are taken: <A.03.03.04.ODP[02]: additional actions>.	AO is new for NIST 800-171A R3
A.03.03.05.b	Audit Record Review, Analysis, and Reporting	findings are reported to organizational personnel or roles.	AO is new for NIST 800-171A R3
A.03.03.07.b[02]	Time Stamps	time stamps are recorded for audit records 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.	AO is new for NIST 800-171A R3
A.03.04.03.d[01]	Configuration Change Control	activities associated with configuration-controlled changes to the system are monitored.	AO is new for NIST 800-171A R3
A.03.04.03.d[02]	Configuration Change Control	activities associated with configuration-controlled changes to the system are reviewed.	AO is new for NIST 800-171A R3
A.03.04.04.b	Impact Analyses	the security requirements for the system continue to be satisfied after the system changes have been implemented.	AO is new for NIST 800-171A R3
A.03.04.10.ODP[01]	System Component Inventory	the frequency at which to review and update the system component inventory is defined.	AO is new for NIST 800-171A R3

A.03.04.11.a[01]	Information Location	the location of CUI is identified and documented.	AO is new for NIST 800-171A R3
A.03.04.11.a[02]	Information Location	the system components on which CUI is processed are identified and documented.	AO is new for NIST 800-171A R3
A.03.04.11.a[03]	Information Location	the system components on which CUI is stored are identified and documented.	AO is new for NIST 800-171A R3
A.03.04.11.b[01]	Information Location	changes to the system or system component location where CUI is processed are documented.	AO is new for NIST 800-171A R3
A.03.04.11.b[02]	Information Location	changes to the system or system component location where CUI is stored are documented.	AO is new for NIST 800-171A R3
A.03.04.12.ODP[02]	System and Component Configuration for High-Risk Areas	security requirements to be applied to the system or system components when individuals return from travel are defined.	AO is new for NIST 800-171A R3
A.03.04.12.a	System and Component Configuration for High-Risk Areas	systems or system components with the following configurations are issued to individuals traveling to high-risk locations: <A.03.04.12.ODP[01]: configurations>.	AO is new for NIST 800-171A R3
A.03.04.12.b	System and Component Configuration for High-Risk Areas	the following security requirements are applied to the system or system components when the individuals return from travel: <A.03.04.12.ODP[02]: security requirements>.	AO is new for NIST 800-171A R3
A.03.05.01.b	User Identification and Authentication	users are reauthenticated when <A.03.05.01.ODP[01]: circumstances or situations>.	AO is new for NIST 800-171A R3
A.03.05.05.a	Identifier Management	authorization is received from organizational personnel or roles to assign an individual, group, role, service, or device identifier.	AO is new for NIST 800-171A R3
A.03.05.05.b[01]	Identifier Management	an identifier that identifies an individual, group, role, service, or device is selected.	AO is new for NIST 800-171A R3
A.03.05.05.b[02]	Identifier Management	an identifier that identifies an individual, group, role, service, or device is assigned.	AO is new for NIST 800-171A R3
A.03.05.05.d	Identifier Management	individual identifiers are managed by uniquely identifying each individual as <A.03.05.05.ODP[02]: characteristic>.	AO is new for NIST 800-171A R3
A.03.05.07.a[03]	Password Management	a list of commonly used, expected, or compromised passwords is updated when organizational passwords are suspected to have been compromised.	AO is new for NIST 800-171A R3
A.03.05.07.b	Password Management	passwords are verified not to be found on the list of commonly used, expected, or compromised passwords when they are created or updated by users.	AO is new for NIST 800-171A R3
A.03.05.12.ODP[01]	Authenticator Management	the frequency for changing or refreshing authenticators is defined.	AO is new for NIST 800-171A R3
A.03.05.12.ODP[02]	Authenticator Management	events that trigger the change or refreshment of authenticators are defined.	AO is new for NIST 800-171A R3
A.03.05.12.a	Authenticator Management	the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified.	AO is new for NIST 800-171A R3
A.03.05.12.b	Authenticator Management	initial authenticator content for any authenticators issued by the organization is established.	AO is new for NIST 800-171A R3
A.03.05.12.c[01]	Authenticator Management	administrative procedures for initial authenticator distribution are established.	AO is new for NIST 800-171A R3

A.03.05.12.c[02]	Authenticator Management	administrative procedures for lost, compromised, or damaged authenticators are established.	AO is new for NIST 800-171A R3
A.03.05.12.c[03]	Authenticator Management	administrative procedures for revoking authenticators are established.	AO is new for NIST 800-171A R3
A.03.05.12.c[04]	Authenticator Management	administrative procedures for initial authenticator distribution are implemented.	AO is new for NIST 800-171A R3
A.03.05.12.c[05]	Authenticator Management	administrative procedures for lost, compromised, or damaged authenticators are implemented.	AO is new for NIST 800-171A R3
A.03.05.12.c[06]	Authenticator Management	administrative procedures for revoking authenticators are implemented.	AO is new for NIST 800-171A R3
A.03.05.12.d	Authenticator Management	default authenticators are changed at first use.	AO is new for NIST 800-171A R3
A.03.05.12.e	Authenticator Management	authenticators are changed or refreshed <A.03.05.12.ODP[01]: frequency> or when the following events occur: <A.03.05.12.ODP[02]: events>.	AO is new for NIST 800-171A R3
A.03.05.12.f[01]	Authenticator Management	authenticator content is protected from unauthorized disclosure.	AO is new for NIST 800-171A R3
A.03.05.12.f[02]	Authenticator Management	authenticator content is protected from unauthorized modification.	AO is new for NIST 800-171A R3
A.03.06.02.d	Incident Monitoring, Reporting, and Response Assistance	an incident response support resource that offers advice and assistance to system users on handling and reporting incidents is provided.	AO is new for NIST 800-171A R3
A.03.06.03.ODP[01]	Incident Response Testing	the frequency at which to test the effectiveness of the incident response capability for the system is defined.	AO is new for NIST 800-171A R3
A.03.06.04.ODP[01]	Incident Response Training	the time period within which incident response training is to be provided to system users is defined.	AO is new for NIST 800-171A R3
A.03.06.04.ODP[02]	Incident Response Training	the frequency at which to provide incident response training to users after initial training is defined.	AO is new for NIST 800-171A R3
A.03.06.04.ODP[03]	Incident Response Training	the frequency at which to review and update incident response training content is defined.	AO is new for NIST 800-171A R3
A.03.06.04.ODP[04]	Incident Response Training	events that initiate a review of the incident response training content are defined.	AO is new for NIST 800-171A R3
A.03.06.04.a.01	Incident Response Training	incident response training for system users consistent with assigned roles and responsibilities is provided within <A.03.06.04.ODP[01]: time period> of assuming an incident response role or responsibility or acquiring system access.	AO is new for NIST 800-171A R3
A.03.06.04.a.02	Incident Response Training	incident response training for system users consistent with assigned roles and responsibilities is provided when required by system changes.	AO is new for NIST 800-171A R3
A.03.06.04.a.03	Incident Response Training	incident response training for system users consistent with assigned roles and responsibilities is provided <A.03.06.04.ODP[02]: frequency> thereafter.	AO is new for NIST 800-171A R3
A.03.06.04.b[01]	Incident Response Training	incident response training content is reviewed <A.03.06.04.ODP[03]: frequency>.	AO is new for NIST 800-171A R3
A.03.06.04.b[02]	Incident Response Training	incident response training content is updated <A.03.06.04.ODP[03]: frequency>.	AO is new for NIST 800-171A R3

A.03.06.04.b[03]	Incident Response Training	incident response training content is reviewed following <A.03.06.04.ODP[04]: events>.	AO is new for NIST 800-171A R3
A.03.06.04.b[04]	Incident Response Training	incident response training content is updated following <A.03.06.04.ODP[04]: events>.	AO is new for NIST 800-171A R3
A.03.06.05.a.01	Incident Response Plan	an incident response plan is developed that provides the organization with a roadmap for implementing its incident response capability.	AO is new for NIST 800-171A R3
A.03.06.05.a.02	Incident Response Plan	an incident response plan is developed that describes the structure and organization of the incident response capability.	AO is new for NIST 800-171A R3
A.03.06.05.a.03	Incident Response Plan	an incident response plan is developed that provides a high-level approach for how the incident response capability fits into the overall organization.	AO is new for NIST 800-171A R3
A.03.06.05.a.04	Incident Response Plan	an incident response plan is developed that defines reportable incidents.	AO is new for NIST 800-171A R3
A.03.06.05.a.05	Incident Response Plan	an incident response plan is developed that addresses the sharing of incident information.	AO is new for NIST 800-171A R3
A.03.06.05.a.06	Incident Response Plan	an incident response plan is developed that designates responsibilities to organizational entities, personnel, or roles.	AO is new for NIST 800-171A R3
A.03.06.05.b[01]	Incident Response Plan	copies of the incident response plan are distributed to designated incident response personnel (identified by name or by role).	AO is new for NIST 800-171A R3
A.03.06.05.b[02]	Incident Response Plan	copies of the incident response plan are distributed to organizational elements.	AO is new for NIST 800-171A R3
A.03.06.05.c	Incident Response Plan	the incident response plan is updated to address system and organizational changes or problems encountered during plan implementation, execution, or testing.	AO is new for NIST 800-171A R3
A.03.06.05.d	Incident Response Plan	the incident response plan is protected from unauthorized disclosure.	AO is new for NIST 800-171A R3
A.03.07.04.a[03]	Maintenance Tools	the use of system maintenance tools is monitored.	AO is new for NIST 800-171A R3
A.03.07.04.c	Maintenance Tools	the removal of system maintenance equipment containing CUI is prevented by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.	AO is new for NIST 800-171A R3
A.03.07.05.b[02]	Nonlocal Maintenance	replay resistance is implemented in the establishment of nonlocal maintenance and diagnostic sessions.	AO is new for NIST 800-171A R3
A.03.08.05.c	Media Transport	activities associated with the transport of system media that contain CUI are documented.	AO is new for NIST 800-171A R3
A.03.08.07.ODP[01]	Media Use	types of system media with usage restrictions or that are prohibited from use are defined.	AO is new for NIST 800-171A R3
A.03.09.01.ODP[01]	Personnel Screening	conditions that require the rescreening of individuals are defined.	AO is new for NIST 800-171A R3
A.03.09.01.b	Personnel Screening	individuals are rescreened in accordance with the following conditions: <A.03.09.01.ODP[01]: conditions>.	AO is new for NIST 800-171A R3

A.03.09.02.a.03	Personnel Termination and Transfer	upon termination of individual employment, security-related system property is retrieved.	AO is new for NIST 800-171A R3
A.03.10.01.c	Physical Access Authorizations	the facility access list is reviewed <A.03.10.01.ODP[01]: frequency>.	AO is new for NIST 800-171A R3
A.03.10.01.d	Physical Access Authorizations	individuals from the facility access list are removed when access is no longer required.	AO is new for NIST 800-171A R3
A.03.10.02.b[01]	Monitoring Physical Access	physical access logs are reviewed <A.03.10.02.ODP[01]: frequency>.	AO is new for NIST 800-171A R3
A.03.10.02.b[02]	Monitoring Physical Access	physical access logs are reviewed upon occurrence of <A.03.10.02.ODP[02]: events or potential indicators of events>.	AO is new for NIST 800-171A R3
A.03.10.07.a.01	Physical Access Control	physical access authorizations are enforced at entry and exit points to the facility where the system resides by verifying individual physical access authorizations before granting access.	AO is new for NIST 800-171A R3
A.03.10.07.a.02	Physical Access Control	physical access authorizations are enforced at entry and exit points to the facility where the system resides by controlling ingress and egress with physical access control systems, devices, or guards.	AO is new for NIST 800-171A R3
A.03.10.07.e	Physical Access Control	physical access to output devices is controlled to prevent unauthorized individuals from obtaining access to CUI.	AO is new for NIST 800-171A R3
A.03.10.08	Access Control for Transmission	physical access to system distribution and transmission lines within organizational facilities is controlled.	AO is new for NIST 800-171A R3
A.03.11.02.c[01]	Vulnerability Monitoring and Scanning	system vulnerabilities to be scanned are updated <A.03.11.02.ODP[04]: frequency>.	AO is new for NIST 800-171A R3
A.03.11.02.c[02]	Vulnerability Monitoring and Scanning	system vulnerabilities to be scanned are updated when new vulnerabilities are identified and reported.	AO is new for NIST 800-171A R3
A.03.11.04[01]	Risk Response	findings from security assessments are responded to.	AO is new for NIST 800-171A R3
A.03.11.04[02]	Risk Response	findings from security monitoring are responded to.	AO is new for NIST 800-171A R3
A.03.11.04[03]	Risk Response	findings from security audits are responded to.	AO is new for NIST 800-171A R3
A.03.12.02.b.02	Plan of Action and Milestones	the existing plan of action and milestones is updated based on the findings from audits or reviews.	AO is new for NIST 800-171A R3
A.03.12.02.b.03	Plan of Action and Milestones	the existing plan of action and milestones is updated based on the findings from continuous monitoring activities.	AO is new for NIST 800-171A R3
A.03.12.05.ODP[01]	Information Exchange	one or more of the following PARAMETER VALUES are selected: {interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements}.	AO is new for NIST 800-171A R3
A.03.12.05.ODP[02]	Information Exchange	the frequency at which to review and update agreements is defined.	AO is new for NIST 800-171A R3

A.03.12.05.a[01]	Information Exchange	the exchange of CUI between the system and other systems is approved using <A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>.	AO is new for NIST 800-171A R3
A.03.12.05.a[02]	Information Exchange	the exchange of CUI between the system and other systems is managed using <A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>.	AO is new for NIST 800-171A R3
A.03.12.05.b[01]	Information Exchange	interface characteristics for each system are documented as part of the exchange agreements.	AO is new for NIST 800-171A R3
A.03.12.05.b[02]	Information Exchange	security requirements for each system are documented as part of the exchange agreements.	AO is new for NIST 800-171A R3
A.03.12.05.b[03]	Information Exchange	responsibilities for each system are documented as part of the exchange agreements.	AO is new for NIST 800-171A R3
A.03.12.05.c[01]	Information Exchange	exchange agreements are reviewed <A.03.12.05.ODP[02]: frequency>.	AO is new for NIST 800-171A R3
A.03.12.05.c[02]	Information Exchange	exchange agreements are updated <A.03.12.05.ODP[02]: frequency>.	AO is new for NIST 800-171A R3
A.03.13.11.ODP[01]	Cryptographic Protection	the types of cryptography for protecting the confidentiality of CUI are defined.	AO is new for NIST 800-171A R3
A.03.14.01.b[02]	Flaw Remediation	security-relevant firmware updates are installed within <A.03.14.01.ODP[02]: time period> of the release of the updates.	AO is new for NIST 800-171A R3
A.03.14.02.c.02	Malicious Code Protection	malicious code protection mechanisms are configured to block malicious code, quarantine malicious code, or take other actions in response to malicious code detection.	AO is new for NIST 800-171A R3
A.03.14.08[01]	Information Management and Retention	CUI within the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	AO is new for NIST 800-171A R3
A.03.14.08[02]	Information Management and Retention	CUI within the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	AO is new for NIST 800-171A R3
A.03.14.08[03]	Information Management and Retention	CUI output from the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	AO is new for NIST 800-171A R3
A.03.14.08[04]	Information Management and Retention	CUI output from the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	AO is new for NIST 800-171A R3
A.03.15.01.ODP[01]	Policy and Procedures	the frequency at which the policies and procedures for satisfying security requirements are reviewed and updated is defined.	AO is new for NIST 800-171A R3
A.03.15.01.b[01]	Policy and Procedures	policies and procedures are reviewed <A.03.15.01.ODP[01]: frequency>.	AO is new for NIST 800-171A R3
A.03.15.01.b[02]	Policy and Procedures	policies and procedures are updated <A.03.15.01.ODP[01]: frequency>.	AO is new for NIST 800-171A R3
A.03.15.02.a.02	System Security Plan	a system security plan that identifies the information types processed, stored, and transmitted by the system is developed.	AO is new for NIST 800-171A R3
A.03.15.02.a.03	System Security Plan	a system security plan that describes specific threats to the system that are of concern to the organization is developed.	AO is new for NIST 800-171A R3
A.03.15.02.a.07	System Security Plan	a system security plan that identifies individuals that fulfill system roles and responsibilities is developed.	AO is new for NIST 800-171A R3

A.03.15.02.a.08	System Security Plan	a system security plan that includes other relevant information necessary for the protection of CUI is developed.	AO is new for NIST 800-171A R3
A.03.15.02.c	System Security Plan	the system security plan is protected from unauthorized disclosure.	AO is new for NIST 800-171A R3
A.03.15.03.ODP[01]	Rules of Behavior	the frequency at which the rules of behavior are reviewed and updated is defined.	AO is new for NIST 800-171A R3
A.03.15.03.a	Rules of Behavior	rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.	AO is new for NIST 800-171A R3. Elements of NFO - NFO - PL-4, PL-4(1)
A.03.15.03.b	Rules of Behavior	rules are provided to individuals who require access to the system.	AO is new for NIST 800-171A R3
A.03.15.03.c	Rules of Behavior	a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior is received before authorizing access to CUI and the system.	AO is new for NIST 800-171A R3. Elements of NFO - NFO - PS-6
A.03.15.03.d[01]	Rules of Behavior	the rules of behavior are reviewed <A.03.15.03.ODP[01]: frequency>.	AO is new for NIST 800-171A R3
A.03.15.03.d[02]	Rules of Behavior	the rules of behavior are updated <A.03.15.03.ODP[01]: frequency>.	AO is new for NIST 800-171A R3
A.03.16.02.a	Unsupported System Components	system components are replaced when support for the components is no longer available from the developer, vendor, or manufacturer.	AO is new for NIST 800-171A R3
A.03.16.02.b	Unsupported System Components	options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced are provided.	AO is new for NIST 800-171A R3
A.03.16.03.c	External System Services	processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.	AO is new for NIST 800-171A R3
A.03.17.01.ODP[01]	Supply Chain Risk Management Plan	the frequency at which to review and update the supply chain risk management plan is defined.	AO is new for NIST 800-171A R3
A.03.17.01.a[01]	Supply Chain Risk Management Plan	a plan for managing supply chain risks is developed.	AO is new for NIST 800-171A R3. Elements of NFO -PS-7
A.03.17.01.a[02]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the research and development of the system, system components, or system services.	AO is new for NIST 800-171A R3
A.03.17.01.a[03]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the design of the system, system components, or system services.	AO is new for NIST 800-171A R3
A.03.17.01.a[04]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the manufacturing of the system, system components, or system services.	AO is new for NIST 800-171A R3
A.03.17.01.a[05]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the acquisition of the system, system components, or system services.	AO is new for NIST 800-171A R3
A.03.17.01.a[06]	Supply Chain Risk	the SCRM plan addresses risks associated with the delivery of the system, system components, or system services.	AO is new for NIST 800-171A R3. Elements of NFO - PE-16

	Management Plan		
A.03.17.01.a[07]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the integration of the system, system components, or system services.	AO is new for NIST 800-171A R3
A.03.17.01.a[08]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the operation of the system, system components, or system services.	AO is new for NIST 800-171A R3
A.03.17.01.a[09]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the maintenance of the system, system components, or system services.	AO is new for NIST 800-171A R3
A.03.17.01.a[10]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the disposal of the system, system components, or system services.	AO is new for NIST 800-171A R3
A.03.17.01.b[01]	Supply Chain Risk Management Plan	the SCRM plan is reviewed <A.03.17.01.ODP[01]: frequency>.	AO is new for NIST 800-171A R3
A.03.17.01.b[02]	Supply Chain Risk Management Plan	the SCRM plan is updated <A.03.17.01.ODP[01]: frequency>.	AO is new for NIST 800-171A R3
A.03.17.01.c	Supply Chain Risk Management Plan	the SCRM plan is protected from unauthorized disclosure.	AO is new for NIST 800-171A R3
A.03.17.02[01]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are developed to identify supply chain risks.	AO is new for NIST 800-171A R3
A.03.17.02[02]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are developed to protect against supply chain risks.	AO is new for NIST 800-171A R3
A.03.17.02[03]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are developed to mitigate supply chain risks.	AO is new for NIST 800-171A R3
A.03.17.02[04]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are implemented to identify supply chain risks.	AO is new for NIST 800-171A R3
A.03.17.02[05]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are implemented to protect against supply chain risks.	AO is new for NIST 800-171A R3
A.03.17.02[06]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are implemented to mitigate supply chain risks.	AO is new for NIST 800-171A R3
A.03.17.03.ODP[01]	Supply Chain Requirements and Processes	security requirements to protect against supply chain risks to the system, system components, or system	AO is new for NIST 800-171A R3. Elements of NFO - SA-9

		services and to limit the harm or consequences from supply chain-related events are defined.	
A.03.17.03.a[01]	Supply Chain Requirements and Processes	a process for identifying weaknesses or deficiencies in the supply chain elements and processes is established.	AO is new for NIST 800-171A R3
A.03.17.03.a[02]	Supply Chain Requirements and Processes	a process for addressing weaknesses or deficiencies in the supply chain elements and processes is established.	AO is new for NIST 800-171A R3
A.03.17.03.b	Supply Chain Requirements and Processes	the following security requirements are enforced to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences of supply chain-related events: <A.03.17.03.ODP[01]: security requirements>.	AO is new for NIST 800-171A R3. Elements of NFO - SA-9

PRACTICAL STEPS TO TRANSITION FROM NIST 800-171 R2 TO NIST 800-171 R3

The following information is provided to establish a basic direction that your organization can take to transition from NIST 800-171 R2 to NIST 800-171 R3. Every organization is unique in its business practices, technologies and resource limitations, so this information is provided as a generic roadmap for transition purposes.

ASSUMPTIONS

Based on the premise that your organization is transitioning from established practices for NIST 800-171 R2, there are several assumptions that your organization has:

1. Documented evidence of due diligence and due care for NIST 8001-171 R2 / CMMC 2.0:
    a. Policies, standards & procedures;
    b. System Security Plan (SSP);
    c. Documented roles & responsibilities (internal and external stakeholders); and
    d. Plan of Action & Milestones (POA&M) for any identified deficiencies;
2. Executive sponsorship to make changes to technologies, third-party relationships and/or business practices; and
3. Third-parties are contractually obligated to comply with flow-down requirements (e.g., NIST 800-171, CMMC, etc.).

KEY NIST 800-171 R3 TRANSITION STEPS

The following transition steps focus on the biggest changes between NIST 800-171 R2 and NIST 800-171 R3 and should be prioritized:

GOVERNANCE OVERSIGHT

One of the issues with previous versions of NIST 800-171 involved Non-Federal Organization (NFO) controls (Appendix E). These were controls that NIST felt were reasonably expected and did not need further clarification, since the requirements were fundamentals to a cybersecurity program (e.g., policies, procedures, training records, etc.). NIST 800-171 R3 corrected this oversight by removing NFO controls entirely. With the removal of NFO controls, this increases the governance requirements in CUI controls. Therefore, ensuring governance oversight is properly established is the most logical step in your transition plan. This should involve:

1. Updating policies & standards to ensure coverage for all NIST 800-171 R3 requirements, down to the Assessment Objective (AO) level.
2. Inventorying all External Service Providers (ESP) to determine ESP access to CUI and/or in-scope systems, applications and/or services.

SUPPLY CHAIN RISK MANAGEMENT (SCRM) PLAN

Arguably, the “heaviest lift” in an organization’s transition from NIST 800-171 R2 to NIST 800-171 R3 is going to be the development of a Supply Chain Risk Management (SCRM) Plan. There are multiple approaches that can be taken to achieve this, but the most likely approach for most organizations will be to align with NIST 800-161 R1 for SCRM-related practices.[2]

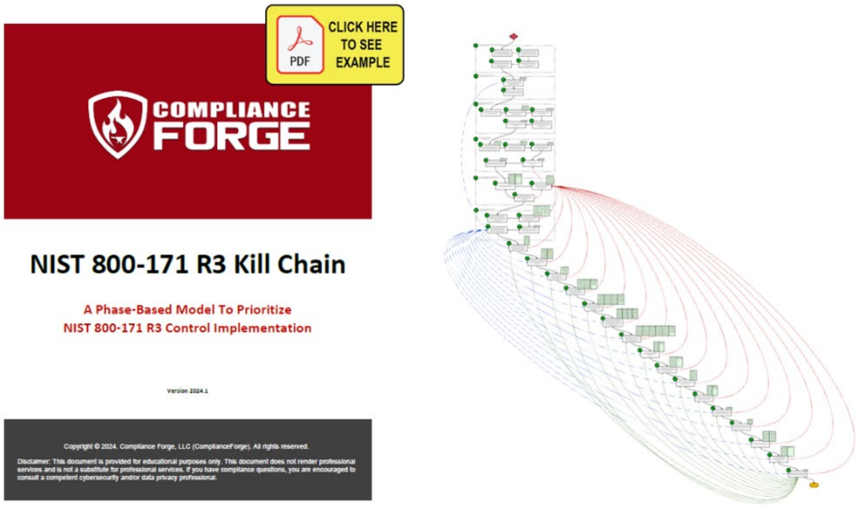
NIST 800-171 R3 has basic requirements established for what a SCRM Plan must contain, but it is going to require a significant amount of time to develop and implement.

[2] *NIST 800-161 R1 - https://csrc.nist.gov/pubs/sp/800/161/r1/final*

FREE RESOURCES TO ASSIST IN YOUR TRANSITION TO NIST 800-171 R3

NIST 800-171 R3 KILL CHAIN

The NIST 800-171 R3 Kill Chain compliments efforts to upgrade from NIST 800-171 R2 to NIST 800-171 R3. This free guide can be downloaded from: **https://complianceforge.com/content/NIST-800-171-R3-Kill-Chain.pdf**



NIST 800-171 R3 Kill Chain

A Phase-Based Model To Prioritize NIST 800-171 R3 Control Implementation

Version 2024.1

Copyright © 2024. Compliance Forge, LLC (ComplianceForge). All rights reserved.

Disclaimer: This document is provided for educational purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a competent cybersecurity and/or data privacy professional.

CMMC CENTER OF AWESOMENESS (CMMC COA) – NIST 800-171 R3 AWESOMENESS SPREADSHEET

The CMMC Center of Awesomeness (CMMC COA) published its updated "CMMC Awesomeness Spreadsheet" for NIST 800-171 R3 and NIST 800-171A R3. This free resource offers a "paint by numbers" approach to addressing NIST 800-171 R3. You can also download the existing spreadsheets for NIST 800-171 R2 and CMMC 2.0:

- Control to Assessment Objective (AO) visibility
- Crosswalk mapping to the SCF, NIST 800-53, NIST CSF 2.0, ISO 27002, etc.
- RASCI matrix (shared responsibility matrix)
- Roles & responsibilities (based on NIST NICE Cybersecurity Workforce Framework)
- Cadence for control execution (e.g., daily, weekly, monthly, etc.)
- Evidence Request List (ERL) identifies reasonable evidence for each AO

This free resource can be downloaded from: **https://cmmc-coa.com**