Configuration Management Implementation Checklist

Policy and Documentation

- ☐ **CM-01**: Develop, document, and disseminate organization-level, mission/business process-level, and system-level configuration management policy
- ☐ **CM-01**: Ensure configuration management policy addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- ☐ **CM-01**: Verify configuration management policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
- ☐ **CM-01**: Document procedures to facilitate implementation of the configuration management policy and associated controls
- ☐ **CM-01**: Designate an official to manage the development, documentation, and dissemination of configuration management policy and procedures
- ☐ **CM-01**: Review and update configuration management policy at least every 3 years or as required by federal or organizational policy changes
- ☐ **CM-01**: Review and update configuration management procedures at least every 3 years or as required by federal or organizational policy changes

Baseline Configuration Management

- ☐ **CM-02**: Develop, document, and maintain under configuration control a current baseline configuration of the system
- ☐ **CM-02**: Review and update baseline configuration at least annually
- ☐ **CM-02**: Review and update baseline configuration when required due to organization-defined circumstances
- ☐ **CM-02**: Review and update baseline configuration when system components are installed or upgraded
- ☐ **CM-02(02)**: Maintain currency, completeness, accuracy, and availability of baseline configuration using organization-defined automated mechanisms

- ☐ **CM-02(03)**: Retain at least one previous version of baseline configurations to support rollback
- ☐ **CM-02(07)**: Issue organization-defined systems or system components with organization-defined configurations to individuals traveling to locations deemed to be of significant risk
- ☐ **CM-02(07)**: Apply organization-defined controls to systems or components when individuals return from travel to high-risk locations

Configuration Change Control

- ☐ **CM-03**: Determine and document types of changes to the system that are configuration-controlled
- ☐ **CM-03**: Review proposed configuration-controlled changes and approve or disapprove with explicit consideration for security and privacy impact analyses
- ☐ **CM-03**: Document configuration change decisions associated with the system
- ☐ **CM-03**: Implement approved configuration-controlled changes to the system
- ☐ **CM-03**: Retain records of configuration-controlled changes for at least 1 year
- ☐ **CM-03**: Monitor and review activities associated with configuration-controlled changes
- ☐ **CM-03**: Coordinate and provide oversight for configuration change control activities through organization-defined configuration change control element
- ☐ **CM-03**: Convene configuration change control element as required by the CCB or for changes identified by the organization
- ☐ **CM-03(02)**: Test, validate, and document changes to the system before finalizing implementation
- ☐ **CM-03(04)**: Require organization-defined security and privacy representatives to be members of the configuration change control element

Security and Privacy Impact Analysis

- ☐ **CM-04**: Analyze changes to the system to determine potential security and privacy impacts prior to change implementation
- ☐ **CM-04(02)**: After system changes, verify that impacted controls are implemented correctly
- ☐ **CM-04(02)**: After system changes, verify that impacted controls are operating as intended

- ☐ **CM-04(02)**: After system changes, verify that impacted controls are producing desired outcome with regard to meeting security and privacy requirements

Access Restrictions for Change

- ☐ **CM-05**: Define physical and logical access restrictions associated with changes to the system
- ☐ **CM-05**: Document physical and logical access restrictions associated with changes to the system
- ☐ **CM-05**: Approve physical and logical access restrictions associated with changes to the system
- ☐ **CM-05**: Enforce physical and logical access restrictions associated with changes to the system
- ☐ **CM-05(01)**: Enforce access restrictions using organization-defined automated mechanisms
- ☐ **CM-05(01)**: Automatically generate audit records of the enforcement actions
- ☐ **CM-05(05)**: Limit privileges to change system components and system-related information within production or operational environment
- ☐ **CM-05(05)**: Review and reevaluate privileges at least annually

Configuration Settings

- ☐ **CM-06**: Establish and document configuration settings for system components that reflect most restrictive mode consistent with operational requirements
- ☐ **CM-06**: Use United States Government Configuration Baseline (USGCB) for the applicable technology
- ☐ **CM-06**: Implement configuration settings
- ☐ **CM-06**: Identify, document, and approve any deviations from established configuration settings for organization-defined system components
- ☐ **CM-06**: Base deviations on organization-defined operational requirements
- ☐ **CM-06**: Monitor and control changes to configuration settings in accordance with organizational policies and procedures
- ☐ **CM-06(01)**: Manage configuration settings for organization-defined system components using organization-defined automated mechanisms

- ☐ **CM-06(01)**: Apply configuration settings for organization-defined system components using organization-defined automated mechanisms
- ☐ **CM-06(01)**: Verify configuration settings for organization-defined system components using organization-defined automated mechanisms

Least Functionality

- ☐ **CM-07**: Configure system to provide only organization-defined mission essential capabilities
- ☐ **CM-07**: Prohibit or restrict use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services
- ☐ **CM-07(01)**: Review system at least monthly to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services
- ☐ **CM-07(01)**: Disable or remove organization-defined functions, ports, protocols, software, and services deemed unnecessary and/or nonsecure
- ☐ **CM-07(02)**: Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions
- ☐ **CM-07(02)**: Prevent program execution in accordance with rules authorizing terms and conditions of software program usage
- ☐ **CM-07(05)**: Identify organization-defined software programs authorized to execute on the system
- ☐ **CM-07(05)**: Employ deny-all, permit-by-exception policy to allow execution of authorized software programs
- ☐ **CM-07(05)**: Review and update list of authorized software programs at least annually

System Component Inventory

- ☐ **CM-08**: Develop and document inventory of system components that accurately reflects the system
- ☐ **CM-08**: Ensure inventory includes all components within the system
- ☐ **CM-08**: Ensure inventory does not include duplicate accounting of components or components assigned to any other system
- ☐ **CM-08**: Ensure inventory is at level of granularity deemed necessary for tracking and reporting

- ☐ **CM-08**: Include organization-defined information deemed necessary to achieve effective system component accountability
- ☐ **CM-08**: Review and update system component inventory at least monthly
- ☐ **CM-08(01)**: Update inventory of system components as part of component installations, removals, and system updates
- ☐ **CM-08(03)**: Detect presence of unauthorized hardware, software, and firmware components using organization-defined automated mechanisms continuously where practical, and at least monthly otherwise
- ☐ **CM-08(03)**: Disable network access by unauthorized components when detected
- ☐ **CM-08(03)**: Isolate unauthorized components when detected
- ☐ **CM-08(03)**: Notify organization-defined personnel or roles when unauthorized components are detected

Configuration Management Plan

- ☐ **CM-09**: Develop configuration management plan that addresses roles, responsibilities, and configuration management processes and procedures
- ☐ **CM-09**: Establish process for identifying configuration items throughout system development life cycle
- ☐ **CM-09**: Establish process for managing configuration of configuration items
- ☐ **CM-09**: Define configuration items for the system
- ☐ **CM-09**: Place configuration items under configuration management
- ☐ **CM-09**: Ensure configuration management plan is reviewed and approved by organization-defined personnel or roles
- ☐ **CM-09**: Protect configuration management plan from unauthorized disclosure and modification
- ☐ **CM-09**: Document configuration management plan
- ☐ **CM-09**: Implement configuration management plan

Software Usage Restrictions

- ☐ **CM-10**: Use software and associated documentation in accordance with contract agreements and copyright laws
- ☐ **CM-10**: Track use of software and associated documentation protected by quantity licenses to control copying and distribution

- ☐ **CM-10**: Control and document use of peer-to-peer file sharing technology
- ☐ **CM-10**: Ensure peer-to-peer file sharing technology is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work

User-Installed Software

- ☐ **CM-11**: Establish organization-defined policies governing installation of software by users
- ☐ **CM-11**: Enforce software installation policies through organization-defined methods
- ☐ **CM-11**: Monitor policy compliance at least monthly

Information Location

- ☐ **CM-12**: Identify and document location of organization-defined information and specific system components on which the information is processed and stored
- ☐ **CM-12**: Identify and document users who have access to system and system components where the information is processed and stored
- ☐ **CM-12**: Document changes to the location (i.e., system or system components) where the information is processed and stored
- ☐ **CM-12(01)**: Use automated tools to identify organization-defined information by information type on organization-defined system components
- ☐ **CM-12(01)**: Ensure controls are in place to protect organizational information and individual privacy through automated information location tracking

Key Timeframes Summary

- ☐ **Policy Review**: At least every 3 years or when federal/organizational policy changes occur
- ☐ **Baseline Configuration Review**: At least annually, when circumstances require, or when system components are installed or upgraded
- ☐ **Configuration Change Records Retention**: At least 1 year
- ☐ **System Review for Unnecessary Functions**: At least monthly
- ☐ **Authorized Software List Review**: At least annually
- ☐ **Component Inventory Review**: At least monthly
- ☐ **Unauthorized Component Detection**: Continuously where practical, at least monthly otherwise
- ☐ **Software Installation Policy Compliance Monitoring**: At least monthly

- [ ] **Privilege Review for Changes**: At least annually