MARCO Federal Managed Computer Services

Cybersecurity Maturity Model Certification Initiative

Configuration Management Policy

Document No

MOJVII-305-00

Effective Date	*Review Date*	*Version*	*Page No.*
02/15/2021	*02/01/2021*	*3*	*1 of 12*

Scope

Information Security Policies are the foundation for information technology security at MARCO-ONOPA JVII (MOJVII). The policies set out the information security standards required by NIST 800-171, which directs the Chief Information Officer (CIO) to establish a set of standards for information technology security to maximize the functionality, security, and interoperability of the distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. This policy covers all information and information systems to include those used, managed, or operated by a contractor, an MOJVII, or other organization on behalf of the. This policy applies to all employees, contractors, and all other users of information and information systems that support the operation and assets of the. This is a living document subject to change in accordance with NIST SP 800-53 and CMMC v 1.02

Responsibilities

All covered personnel who utilize MOJVII IT resources are responsible for adhering to this policy and any local Configuration Management requirements.

Role	Definition
MOJVII Management	The MOJVII Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level are assigned the responsibility for the continued development, implementation, operation and monitoring of the Configuration Management program. Ensures that personnel with significant responsibilities for configuration management are trained.
MOJVII Security Liaison	The MOJVII Security Liaison is responsible for ensuring that security risks are managed in compliance with MOJVII's requirements by collaborating with organizational entities. Liaisons are responsible for ensuring the appropriate configuration management controls are in effect for MOJVII information systems.
Information System Owner	The information system owner is the individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. Develops and maintains configuration management for the information system in coordination with information owners, the system administrator, the information system security officer, and functional "end users."
Information Owner	The information owner is the individual with operational responsibility and authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. Provides input to information system owners regarding security requirements and security controls for the information system(s) where the information resides. Decides who has access to the information system and with what types of privileges or access rights.
Covered Personnel	Covered personnel must provide Configuration Management capabilities that meet MOJVII requirements. Configuration Management practices are subject to periodic review by the agencies.

CM-1 – Policy

All MOJVII information assets must meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls. This document addresses the requirements set forth by MOJVII to implement the family of Configuration Management security controls. This document provides requirements for the configuration management process which is required to assure that information systems are designed and configured using controls sufficient to safeguard MOJVII's information systems.

MOJVII has adopted the Configuration Management security principles established in NIST SP 800-53, "Configuration Management" control guidelines as the official policy for this security domain. The "CM" designator identified in each control represents the NIST-specified identifier for the Configuration Management control family. The following subsections in this document outline the Configuration Management requirements that each MOJVII must implement and maintain in order to be compliant with this policy. This policy shall be reviewed annually, at a minimum.

CM-2 – Baseline Configuration

MOJVII shall provide common security configurations that provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This requirement allows MOJVII to improve information system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of MOJVII data. MOJVII shall ensure the following is done:

a. A current baseline configuration must be developed, reviewed, approved, documented, and maintained under configuration control for each information system. The Department of Information Technology (DIT) shall be responsible for baseline configurations for enterprise solutions.

b. A baseline configuration must document and provide information about the components of an information system including the following:

    i. Standard operating system/installed applications with current version numbers

    ii. Standard software load for workstations, servers, network components, and mobile devices and laptops

    iii. Up-to-date patch level information

    iv. Network topology

    v. Logical placement of the component within the system and enterprise architecture

    vi. Technology platform

c. New baselines must be created as the information system changes over time in order to maintain the baseline configuration.

d. Ensure the baseline configuration of an information system is consistent with MOJVIIwide enterprise architecture. Product versions of security related technologies must be either N or at N-1 and must be kept up to date by applying the latest security patches.

e. Utilize best practice system hardening baselines for the operating systems. Refer to CM-6 Configuration Settings for a list of approved baselines.

f. In cases where a baseline security configuration does not exist for an operating system, MOJVII Chief Risk Officer (SCRO) or designee shall ensure a baseline security configuration is developed, documented and approved.

g. Document any exceptions to baseline security configurations and obtain approval by the SCRO or designee.

h. Maintain records confirming the implementation of baseline security configurations for each IT system they manage.

i. Retain previous versions of baseline configurations of the information system to support rollback, for example, hardware, software, firmware, configuration files, and configuration records.

j. Review and update the baseline configuration for information systems:

   i. Annually, at a minimum

   ii. When required due to system upgrades, patches, or other significant changes have occurred in the baseline configuration

   iii. As an integral part of information system component installations and upgrades

   iv. When an increase in interconnection with other systems outside the authorization boundary or significant changes in the security requirements for the system

CM-3 – Configuration Change Control

MOJVII shall manage changes to systems and application programs to protect the systems and programs from failure as well as security breaches. Adequate management of system change control processes shall require the following:

a. Safeguard production systems during modification, including emergency changes

b. Enforcement of formal change control procedures

c. Proper authorization and approvals at all levels

d. Successful testing of updates and new programs prior to their being moved into a production environment.

e. Determine the types of changes to the information system that are configuration controlled.

f. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.

g. Document configuration change decisions associated with the information system.

h. Implement approved configuration-controlled changes to the information system.

i. Retain records of configuration-controlled changes to the information system for the life of the system.

j. Audit and review activities associated with configuration-controlled changes to the information system.

k. Coordinate and provide oversight for configuration change control activities through a Configuration Control Board that convenes when configuration changes occur.

l. Test, validate, and document changes to the information system before implementing the changes on the system.

m. Ensure updates addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved, and applied promptly to minimize the exposure of unpatched resources. Vulnerability Management requirements are addressed in the System and

Information Integrity Policy SCIO-SEC-317, Section SI-2.

n. Integrate application change control and operational change control procedures. This effort should include the following processes, controls, and best practices:

   i Controls and approval levels for updating libraries.

   ii Requiring formal agreement and approval for any changes iii Restricting library content

   iv Restricting programmers' access to only those parts of the system necessary for their work

   v Version control for each application.

   vi Tying program documentation updates to source code updates

   vii Audit logs that track all accesses to libraries, copying and use of source code, and updates posted to libraries.

o. Define job responsibilities/restrictions and establishing authority levels for the following:

   i. Program librarian(s)

   ii. Developers (i.e., should neither test their own code nor promote it into production)

   iii. Other IT staff

p. Identify personnel authorized to make or submit changes to the source library (i.e., a program librarian) for each major application to control check-in/check-out.

q. Provide role-based training for business and technical users covering new features and security controls introduced by the upgrade.

r. Use rollback procedures designed to recover to previous stable version of programs.

CM-4 – Security Impact Analysis

When significant changes are planned for, or made to, a system, the system owners, MOJVII security liaison or business owners for systems shall conduct a security impact analysis to determine which controls shall be assessed for proper implementation and operation. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. The following security risk impact analysis activities shall be incorporated into the documented configuration change control process:

a. Identification of the Federal, State, and Local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for MOJVII functions or services.

b. Identification of restricted or highly restricted information, which are stored in the MOJVII 's files, and the potential for fraud, misuse, or other illegal activity. Data classifications are defined within MOJVIIwide Data Classification and Handling policy.

c. Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical MOJVII functions and services.

d. Identification of the processes used to monitor and report to management on whatever applications, tools and technologies the MOJVII has implemented to adequately manage the risk as defined by the MOJVII (i.e., baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.).

e. Identification of the MOJVII 's IT Change Management and Vulnerability Assessment processes.

f. Identification of the security mechanisms that are in place to conceal MOJVII data, for example the use of encryption, data masking, etc.

g. Changes shall be analyzed and evaluated for the impact on security, preferably before they are approved and implemented.

h. Security risk analysis requirements and definitions are addressed in the Risk Assessment Policy SCIO-SEC-314, Section RA-3.

CM-5 – Access Restrictions for Change

MOJVII shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system. MOJVII shall ensure the following:

a. Only qualified and authorized individuals can obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

b. All requests for local administrative rights must be documented and approved by MOJVII management.

c. Access records must be maintained to ensure that configuration change control is being implemented as intended and for supporting after-the-fact actions should MOJVII become aware of an unauthorized change to an information system.

d. Privileges to change information system components and system-related information within a production or operational environment shall be limited to avoid unintended changes to other systems and business processed.

e. Use two-person integrity to ensure that changes to MOJVII defined critical systems cannot occur unless both individuals implement such changes.

f. Restrict access to operating system and operational or production application software/program libraries to designated staff only.

CM-6 – Configuration Settings

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. MOJVII shall implement the following requirements:

a. A standard set of mandatory configuration settings must be established and documented for information technology products employed within the information system. Standard Configuration Documents (SCDs) must detail the configuration settings.

b. The selected configuration settings, whether MOJVII standards or designed specifically for the information system, must reflect the most restrictive mode consistent with operational requirements and must be derived from the following sources, listed in order of precedence:

   i. NIST recommended configurations and checklists: http://checklists.nist.gov/

   ii. Defense Information Systems MOJVII (DISA) security checklists and Standard Technical

Implementation Guides (STIGs): http://iase.disa.mil/stigs/stig/index.html and http://iase.disa.mil/stigs/checklist/index.html

iii. National Security MOJVII (NSA) configuration guides: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/index.cfm

iv. Center for Internet Security (CIS) benchmarks: https://benchmarks.cisecurity.org/downloads/benchmarks/

v. Safeguard Computer Security Evaluation Matrix (SCSEM): https://www.irs.gov/uac/safeguards-program, for systems that store, process, or transmit federal tax information (FTI).

c. Identify, document, and approve any deviations from established configuration settings for information systems.

d. Monitor and control changes to the configuration settings in accordance with MOJVII policies and procedures.

CM-7 – Least Functionality

MOJVII shall implement the following requirements to provide least functionality:

a. Configure information systems to provide only essential capabilities and specifically prohibit or restrict the use of functions, ports, protocols, and/or services that are not required for the business function of the information system.

b. Where technically configurable, the MOJVII will limit component functionality to a single function per device (e.g., email server, web server, etc.).

c. Disable any functions, ports, protocols, and services within an information system that are deemed to be unnecessary and/or non-secure. MOJVII can either make a determination of the relative security of a function, port, protocol, and/or service or base a security decision on the assessment of other entities. The use of the following functions, ports, protocols, and/or services, at a minimum, must be specifically prohibited or restricted:

i. ARINC-GATEWAY Port 55210 / TCP

ii. Background File Transfer Protocol (BFTP) Port 152 / TCP

iii. Border Gateway Protocol (BGP) Port 179 / Transmission Control Protocol (TCP)

iv. Courier Port 530 / TCP, User Datagram Protocol (UDP)

v. Domain Name System be (DNS) Port 53 / TCP, UDP

vi. File Transfer Protocol (FTP) Ports 20, 21 / TCP

vii. Finger Port 79 / TCP

viii. Hypertext Transfer Protocol (HTTP) Port 80 / TCP; 443 / TCP

ix. HTTP-MGMT Port 280 / TCP

x. Identification Protocol (IDENT) Port 113 / TCP, UDP

xi. Internet Control Messaging Protocol (ICMP) - block incoming echo request (ping and Windows traceroute) block outgoing echo replies, time exceeded, and destination unreachable messages except “packet too big” messages (type 3, code 4). **Note:** Blocking ICMP will restrict legitimate use of PING to restrict malicious activity.

xii. Internet Message Access Protocol (IMAP) Port 143 / TCP, UDP

xiii. Internet Relay Chat (IRC) Port 194 / UDP

xiv. Lightweight Directory Access Protocol (LDAP) Port 389 / TCP, UDP

xv. Line Printer Daemon (LPD) Port 515 / TCP

xvi. LOCKD Port 4045 / TCP, UDP

xvii. Network Basic Input Output System (NetBIOS) Ports 135, 445 / TCP, UDP; 137-138 / UDP; 139 / TCP

xviii. Network File System (NFS) Port 2049 / TCP, UDP

xix. Network News Transfer Protocol (NNTP) Port 119 / TCP

xx. Network Time Protocol (NTP) Port 123 / TCP

xxi. Oracle Names (ORACLENAMES) Port 1575 / TCP, UDP

xxii. Port Mapper (PORTMAP/RPCBIND) Port 111 / TCP, UDP

xxiii. Post Office Protocol 3 (POP3) Ports 109-110 / TCP

xxiv. r Services Ports 512-514 / TCP

xxv. Secure Shell (SSH) Port 22 / TCP

xxvi. Session Initiation Protocol (SIP) Port 5060 / TCP, UDP

xxvii. Shell Port 514 / TCP

xxviii. SIDEWINDER-COBRA, (S) Port 2809 & 9002 / TCP

xxix. Simple File Transfer Protocol (SFTP) Port 115 TCP, UDP

xxx. Simple Mail Transfer Protocol (SMTP) Port 25 / TCP

xxxi. Simple Network Management Protocol (SNMP) Ports 161-162 / TCP, UDP

xxxii. Snare Port 509 / TCP, UDP

xxxiii. Socket Secure (SOCKS) Port 1080 / TCP

xxxiv. SOFTWAREAGWEBMETHODS Port 6849 / TCP

xxxv. Structured Query Language (SQL) Port 118 / TCP, UDP; Port 156 / TCP, UDP

xxxvi. Super Duper Telnet Port 95 / TCP

xxxvii. SYMANTEC-ITA Port 3833-3836 / TCP

xxxviii. Syslog Port 514 / UDP

xxxix. Telnet Port 23 / TCP

xl. TIME Port 37 / TCP, UDP

xli. TIMBUKTU Port 407 / TCP, UDP

xlii. Trivial File Transfer Protocol (TFTP) Port 69 /

UDP xliii. VNC-SERVER Port 5900 / TCP

xliv. X Windows Ports 6000-6255 /

TCP xlv. YAK-CHAT Port 258 /

UDP

d. Identify and remove/disable unauthorized and/or non-secure functions, ports, protocols, services, and applications.

e. An information system shall prevent program execution in accordance with MOJVII -defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.

CM-8 – Information System Component Inventory

MOJVII shall update the inventory of information system components as an integral part of component installations, removals, and information system updates. MOJVII shall do the following:

a. Develop, document, and maintain an inventory of information system components that accurately reflects the current information system environment.

b. Verify that all components within the authorization boundary of the information system arenot duplicated in other information system component inventories.

   Inventory all components within the authorization boundary of the information system (this may inter-connected systems). The inventory includes information deemed necessary to achieve effective property accountability and is at the level of granularity for tracking and reporting, for example, the following:

   i. hardware inventory specifications (manufacturer, type, model, serial number, physical location),

   ii. software license information,

   iii. information system / component owner(s),

   iv. associated component configuration standard,

   v. software/firmware version information, and

   vi. for a networked component/device, the machine name and network address,

c. Review and audit information system component inventory,

d. Include assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory,

e. Review and update the information system component inventory annually, at a minimum.

CM-8 (3) – Information System Component Inventory – Automated Unauthorized Component Detection (Moderate Control)

MOJVII shall employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system. MOJVII may take one or more of the following actions when unauthorized components are detected:

i. Disable network access to such components.

ii. Isolates the components.

iii. Notify MOJVII -defined personnel.

This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices.

CM-9 – Configuration Management Plan

MOJVII shall develop, document, and implement a configuration management plan for information systems that does the following:

a. Addresses roles, responsibilities, and configuration management processes and procedures,

b. Defines the configuration items for the information system and when in the system development life cycle (SDLC) the configuration items are placed under configuration management,

c. Establishes the means for identifying configuration items throughout the SDLC and a process for managing the configuration of the configuration items,

d. Assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development. In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process,

e. Defines detailed processes and procedures for how configuration management is used to support SDLC activities at the information system level,

f. Describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated,

g. Creates a step-by-step implementation plan for every configuration change,

h. Requires that software implementation plans follow change control procedures,

i. Protects the configuration management plan from unauthorized disclosure and modification,

j. The configuration management approval process must include the following:

    i. Designation of key management stakeholders who are responsible for reviewing and approving proposed changes to the information system.

    ii. Designation of security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.

CM-10 – Software Usage Restrictions

MOJVII shall ensure the following:

a. Provide employees, contractors and other third parties with guidelines for obeying software licensing agreements, to include open-source software, and shall not permit the installation of unauthorized copies of software on technology devices that connect to MOJVII Network.

    i. Persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.

    ii. Employees, contractors and other third parties shall use software and associated documentation in accordance with contract agreements and copyright laws.

    iii. Employees, contractors and other third parties who make, acquire, or use unauthorized copies of software shall be disciplined as appropriate. Such discipline may include termination.

    iv. Open-source software must adhere to a secure configuration baseline checklist from the U.S. Government or industry.

b. Inform their users of any proprietary rights in databases or similar compilations and the appropriate use of such data.

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

d. Establish procedures for software use, distribution, and removal within the MOJVII to ensure MOJVII use of software meets all copyright and licensing requirements. Procedures shall include the development of internal controls to monitor the number of licenses available and the number of copies in use.

CM-11 – User Installed Software

Only standard approved software shall be installed on MOJVII owned assets with any deviations being pre-approved by MOJVII management and reviewed by an MOJVII security liaison assigned to perform the review. MOJVII shall ensure the following for user installed software:

a. Establish policies governing the installation of software by users.

b. Enforce software installation policies through automated methods, if available and technically configurable.

c. Monitor policy compliance quarterly, at a minimum.

d. Ensure only software programs that are from validated media are installed and are free of harmful code or other destructive aspects.

e. Refer to MOJVIIwide Acceptable Use Policy (AUP) for additional requirements.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Material Superseded

This current policy supersedes all previous versions of the policy. All MOJVII and vendors of MOJVII are expected to comply with the current implemented version of this policy.

APPROVAL SIGNATURES PAGE
Information Technology Department (ITDEPT)

MOJVII OFFICERS	SIGNATURE	DATE
CIO		
CSO		
CEO		
IASO:		

CYBERSECURITY MATURITY MODEL CERTIFICATION