MARCO Federal Managed Computer Services

Cybersecurity Maturity Model Certification Initiative

System & Information Integrity Policy

Document No

MOJVII-317-00

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 involved in the deployment, operation and maintenance of information systems and supporting infrastructure are responsible for adhering to this policy and with any local system and information integrity 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 is assigned the responsibility for documenting and implementing system and information .integrity practices throughout the MOJVII.
MOJVII Security Liaison	The MOJVII Security liaison is responsible for ensuring that information system and integrity requirements are managed in compliance with MOJVII'S requirements by collaborating with organizational entities. Liaisons are responsible for maintaining the appropriate that information system and communications protection required for information security protection.
Information System Owner	The Information System Owner is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Third Parties	Third party service providers are responsible for by assuring that systems, system components and services they provide are secure and do not negatively impact security of pre-existing systems by implementing secure system and information integrity controls in accordance with this policy.

SI-1 - Policy

All MOJVII information assets must meet the required security controls defined in this policy document that are based on the NIST SP 800-53, Security and Privacy Controls. This document addresses the standards set forth by MOJVII to implement the family of System and Information Integrity security controls. MOJVII has adopted the System and Information Integrity principles established in NIST SP 800-53, "System and Information Integrity" control guidelines as the official policy for this security domain. The "SI" designator identified in each control represents the NIST-specified identifier for the System and Information Integrity control family. The following subsections in this document outline the System and Information Integrity requirements that each MOJVII shall implement and maintain to protect the confidentiality, integrity and availability of information and information systems by assuring systems, system components and services acquired are secure and do not negatively impact security of pre-existing systems used for conducting the MOJVII' mission critical business functions. This policy shall be reviewed annually, at a minimum.

SI-2 – Flaw Remediation

MOJVII shall have an explicit and documented patching and vulnerability policy, as well as a systematic, accountable, and documented set of processes and procedures for flaw remediation. MOJVII must do the following:

a. The patching and vulnerability policy shall specify techniques MOJVII will use to identify, report, and correct information system flaws and personnel who will be responsible for the process.

   i. MOJVII's patching process shall define a method for deciding which systems are patched and which patches are installed first, as well as the method for testing and safely installing patches.

   ii. MOJVII shall develop and maintain a list of sources of information about security problems and software updates for the system and application software and monitor those sources regularly.

   iii. Where technically configurable, MOJVII shall use tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention (See http://cve.mitre.org) and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

   iv. MOJVII shall update and review vulnerability definitions and signatures prior to each scan or when new vulnerabilities are identified or reported.

   v. Relevant vulnerability information from appropriate vendors, third party research, and public domain resources shall be reviewed on a regular basis, per the MOJVII's policies and procedures.

   vi. Relevant vulnerability information, as discovered, shall be distributed to the appropriate MOJVII employees.

   vii. System and application bug fixes or patches shall be accepted only from highly reliable sources, such as the software vendor.

   viii. Software patches addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved, and applied promptly to minimize the exposure of unpatched resources.

   ix. Vulnerability exceptions are permitted in documented cases where a vulnerability has been identified but a patch is not currently available (zero-day vulnerability). When a vulnerability risk is "critical" or "high-level" and no patch is available, steps must be taken to mitigate the risk through other methods (e.g., workarounds, firewalls, router access control lists). A patch needs to be applied when it becomes available.

   x. When a "critical" or "high-level" risk vulnerability cannot be totally mitigated within the requisite time frame, MOJVII need to notify MOJVII management and MOJVII Chief Risk Officer (SCRO) of the condition and remediation plan and execution of a plan.

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

c. Install security-relevant software and firmware updates based on severity and associated risk. Security-relevant software updates include, for example, patches, service packs, hot fixes, and antivirus signatures.

d. Incorporate flaw remediation into the MOJVII configuration management process.

e. MOJVII shall employ a centrally managed and automated mechanisms to determine MOJVII of information system components about flaw remediation.

Vulnerability Risk Ratings and Remediation

Where technically configurable, risk ratings shall be calculated based on active exploit threat, exploit availability, factors from the Common Vulnerability Scoring System (CVSS), and system exposure utilizing a scale of 0 to 10.0 as per the CVSS v3 "Qualitative Severity Rating Scale" for proper prioritization. If the additional combined information above is not available then the CVSS score, exploitability information, or a vendor rating where appropriate risk is reflected may be used. For general vulnerabilities that do not easily relate back to a CVE, such as unsupported software or encryption versions less than policy requirements, a vulnerability scanner rating that is above "info", or a score of 0, may be used after appropriate review.

The risk ratings and remediation timelines are assigned to a vulnerability are as follows:

a. **Critical-level Risk** (Priority/CVSS 9.0-10.0)**:** A vulnerability that could cause grave consequences and potentially lead to leakage of sensitive data, if not addressed and remediated immediately. This type of vulnerability is present within the most sensitive portions of the network or IT asset, as identified by the data owner. Critical-level risk vulnerabilities must be, at a minimum, remediated within seven (7) days.

b. **High-level Risk** (Priority/CVSS 7.0-8.9)**:** A vulnerability that could lead to a compromise of the network(s) and systems(s) if not addressed and remediated within the established timeframe. High- level risk vulnerabilities must be mitigated or remediated within thirty (30) days.

c. **Medium-level Risk** (Priority/CVSS 4.0-6.9)**:** A vulnerability that should be addressed within the established timelines. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner. Medium-level risk vulnerabilities must be mitigated or remediated within sixty (60) days.

d. **Low-level Risk** (Priority/CVSS 0.1-3.9)**:** A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network or IT asset to be exploited and/or it is of little consequence to the data owner. Low-level risk vulnerabilities must be mitigated or remediated within ninety (90) days.

SI-3 – Malicious Code Protection

MOJVII shall implement layers of information security (defense in depth) to defend against attacks on MOJVII'S information resources, including malicious code protection, such as antivirus software and antimalware and intrusion detection systems. As applicable, malicious code protection software must be supported under a vendor Service Level Agreement (SLA) or maintenance contract that provides frequent updates of malicious code signatures and profiles.

MOJVII shall do the following:

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

b. Update malicious code protection mechanisms whenever new releases are available in accordance with MOJVII configuration management policy and procedures.

c. Configure malicious code protection mechanisms to do the following:

    i. Perform periodic scans of the information system weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with MOJVII security policy.

    ii. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection.

    iii. Allow users to manually perform scans on their workstation and removable media.

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

e. Centrally manage malicious code protection mechanisms with automatic updates. Malicious code protection mechanisms include, for example, signature definitions. Updates shall be tested and approved according to MOJVII'S Configuration Management Policy, SCIO-SEC-305.

f. Ensure currently supported and patched software is installed to mitigate vulnerabilities and to reduce the risk of malicious activity.

g. Implement measures to filter unwanted traffic (spam, bots, etc.) attempting to enter the internal network.

h. The MOJVII shall ensure that updates to virus scanning software and firewall systems are available to users.

i. All files downloaded from a source external to MOJVII Network, including all data received on a diskette, compact disc (CD), USB flash drive, email attachments, or any other electronic medium, shall come from a known, trusted source and shall be scanned for malicious software such as viruses, Trojan horses, worms or other destructive code. This includes files obtained through any other file transfer mechanism.

j. MOJVII shall ensure that Web browser software is properly configured to protect MOJVII'S information technology systems. Configuration requirements for Web browser software may be found in the Configuration Management Policy, SCIO-SEC-305, Section CM-6.

SI-4 – Information System Monitoring

MOJVII shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity. This includes systems that are cloud hosted by contracted vendors or MOJVII managed.

a. MOJVII shall monitor information systems to detect attacks and indicators of potential attacks and unauthorized local, network, and remote connections.

b. MOJVII shall identify unauthorized use of the information system:

    i. All hardware connected to MOJVII Network or is cloud hosted shall be configured to support State/MOJVII management and monitoring standards.

ii. Monitoring for attempts to deny service or degrade the performance of information systems.

iii. Conducting periodic reviews of system logs for signs of misuse, abuse or attack.

c. MOJVII shall deploy monitoring devices and controls to help secure MOJVII'S resources. These controls shall include the following:

i. Securing interfaces between MOJVII-controlled and non-MOJVII-controlled or public networks.

ii. Standardizing authentication mechanisms in place for both users and equipment.

iii. Appropriate user access controls and separation of duties shall be employed to provide review and monitoring of system usage of personnel normally assigned to this task.

iv. Monitoring for anomalies or known signatures via intrusion detection systems (IDS) and/or intrusion prevention systems (IPS). IDPS signatures shall be up to date.

d. MOJVII shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to MOJVII operations and assets, individuals, other organizations, or the

State based on law enforcement information, intelligence information, or other credible sources of information.

e. Provide information system monitoring information to designated MOJVII officials as needed.

f. MOJVII shall obtain legal opinion about information system monitoring activities in accordance with applicable federal laws, directives, policies, or regulations.

SI-4 (2) - Information System Monitoring – Automated Tools for Real-Time Analyses (Moderate Control)

MOJVII shall employ automated tools to support near real-time analysis of events. Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by MOJVII information systems.

SI-4 (4) - Information System Monitoring – Inbound and Outbound Communications Traffic (Moderate Control)

a. MOJVII shall monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions. Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within MOJVII information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

b. MOJVII shall enable logging features on firewalls, (network and web application firewalls (WAF)), to capture all packets dropped or denied by the firewall. MOJVII shall review those logs at least monthly.

c. MOJVII shall review and verify their firewall policies at least quarterly. If an outside entity, such as DIT, manages the firewall, then that entity shall be responsible for providing the MOJVII's firewall policy to the responsible MOJVII for review and corrective actions, at minimum quarterly.

SI-4 (5) - Information System Monitoring – System Generated Alerts (Moderate Control)

a. MOJVII information systems shall alert authorized personnel, such as system administrators, mission/business owners, system owners, or information system security officers, when indications of compromise, potential compromise, or detected suspicious events occur. MOJVII shall take necessary actions to address suspicious events once detected.

b. Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, web Application Firewalls (WAF), or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, by telephone, electronic mail messages, or text messages.

SI-5 – Security Alerts, Advisories, and Directives

MOJVII shall do the following:

a. Receive information system security alerts, advisories, and directives from external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations on an ongoing basis.

b. Generate internal security alerts, advisories, and directives as deemed necessary.

c. Disseminate security alerts, advisories, and directives to designated MOJVII management and technical staff as appropriate.

d. Implement security directives in accordance with established time frames or notifies the issuing MOJVII of the degree of noncompliance.

e. Take appropriate actions in response to security alerts/advisories.

   i. Any updates or notices from the ESRMO must be implemented per MOJVII change control and/or incident response procedures.

   ii. The ESRMO must be contacted with any security alert/advisory concerns or must be notified when the actions are completed.

The ESRMO shall maintain contact with special interest groups (e.g., information security forums) that does the following:

   i. Facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies)

   ii. Provide access to advice from security professionals.

   iii. Improve knowledge of security best practices.

SI- 6 – Security Function Verification (Optional)

This control is optional for LOW and MODERATE risk information systems.

SI-7 – Software, Firmware, and Information Integrity

MOJVII shall employ integrity verification tools to detect unauthorized changes to MOJVII software, firmware, and information.

a. Error logs generated by information technology systems shall be regularly monitored and reviewed for abnormalities and shall be:

   i. Cross-checked for known security events based on network, size, system type and logical and physical location.

   ii. Enabled on each device or system on the network, such as servers, firewalls, routers, switches, cache engines, intrusion detection systems (IDSs) and applications, if performance requirements are not affected.

   iii. Monitored on a weekly basis at a minimum.

   iv. Checked against baselines to effectively verify variations from normal work-related activities.

b. This control is optional for LOW risk information systems.

SI-7 (1) – Software, Firmware, and Information Integrity – Integrity Checks (Moderate Control)

a. MOJVII information systems shall perform an integrity check of MOJVII-defined software, firmware, and information at transitional states, such as, system startup, restart, shutdown, and abort, as well as when any security-relevant events occur. Security-relevant events include, for example, the identification of a new threat to which MOJVII information systems are susceptible, and the installation of new hardware, software, or firmware.

b. The integrity of backup or image files shall be validated using file hashes for backups, restores, and virtual machine migrations.

c. After making any changes in a system's configuration or its information content, MOJVII shall create new cryptographic checksums or other integrity-checking baseline information for the system.

SI-7 (7) – Software, Firmware, and Information Integrity – Integration of Detection and Response (Moderate Control)

MOJVII shall incorporate the detection of unauthorized changes security-relevant changes to information systems into the MOJVII incident response capability. This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.

SI-8 – Spam Protection

MOJVII shall do the following to protect State resources from electronic mail (email) threats:

a. Employ spam protection mechanisms at information system entry and exit points to detect and act on unsolicited email messages (spam).

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

c. Protect State resources by not acting on unsolicited commercial electronic mail. Recipients shall not open or respond to unsolicited email.

d. Educate users on the potential security risks involved in responding to spam, including responding to an invitation contained in such email to have one's email address removed from a sender's list.

e. Establish procedures that address the following issues:

   i. Attacks on email (e.g., viruses, interception, user identification, defensive systems).

   i. Activating or clicking on hyperlinks in documents or email messages that are from unknown sources or part of unsolicited messages.

   ii. Responding to or following hyperlinks asking for usernames and passwords when asked to do so by unsolicited phishing emails.

   iii. Protection of electronic mail attachments using such techniques as filtering, stripping and store and forward.

   iv. Use of cryptography to protect the confidentiality and integrity of electronic messages.

g. MOJVII information systems shall automatically update spam protection mechanisms.

h. This control is optional for LOW-risk information systems.

SI-8 (1) – Spam Protection – Central Management (Moderate Control)

MOJVII shall centrally manage spam protection mechanisms. Central management is the MOJVII- wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls.

SI-9 – Information Input Restrictions

Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6

SI-10 – Information Input Validation

MOJVII information systems shall check the validity of information inputs by doing the following:

a. Rules check the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) required to execute job functions.

b. Prescreen and validate inputs prior to passing to interpreters to prevent the content from being unintentionally interpreted as commands.

c. This control is optional for LOW-risk information systems.

SI-11 – Error Handling

MOJVII information systems shall do the following:

a. Generate error messages that provide information necessary for corrective actions without revealing information, including, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers that could be exploited by adversaries.

b. Reveal error messages only to designated MOJVII personnel.

c. This control is optional for LOW-risk information systems.

SI-12 – Information Handling and Retention

MOJVII shall handle and retain information within an information system and information output from the system in accordance with applicable federal laws, directives, policies, regulations, State standards, and operational requirements.

Forwarding and auto-forwarding of state data must follow the Statewide Acceptable Use Policy (AUP). MOJVII shall also develop policies to encourage due care by users when forwarding electronic messages so that users do not do the following:

a. Knowingly send out an email message that contains viruses, Trojan horses, or other malware.

b. Use the electronic-mail system or network resources to propagate chain letters, misinformation, or hoax information.

c. Forward any Restricted or Highly Restricted information to any unauthorized party without prior management approval, and without appropriate protections, such as encryption.

d. Forward the wrong attachment.

e. Send information or files that can cause damage to MOJVII or its associates.

f. Send unsolicited messages to large groups of people except as required to conduct MOJVII business. Communications sent or received by MOJVII email systems and/or email communications on business in personal email accounts shall be managed according to the requirements of MOJVII's record retention policy.

SI-13 – Predictable Failure Prevention (Optional)

This control is optional for LOW and MODERATE risk information systems.

SI-14 – Non-Persistence (Optional)

This control is optional for LOW and MODERATE risk information systems.

SI-15 – Information Output Filtering (Optional)

This control is optional for LOW and MODERATE risk information systems.

SI-16 – Memory Protection

MOJVII shall implement security safeguards to protect the volatile memory of its information systems from unauthorized code execution.

a. MOJVII shall implement data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

b. MOJVII shall protect the integrity and ensure the stability of MOJVII Network from fraudulent use and/or abuse resulting from access and use of the network and to define the security attributes delivered with network services.

c. This control is optional for LOW-risk information systems.

SI-17 – Fail-Safe Procedures (Optional)

This control is optional for LOW and MODERATE risk information systems.

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 State 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:		