MARCO Federal Managed Computer Services

Cybersecurity Maturity Model Certification Initiative

Identification & Authentication Policy

Document No

MOJVII-307-00

Effective Date	*Review Date*	*Version*	*Page No.*
02/15/2021	02/01/2021	3	1 of 10

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, MOJVII, or other organization on behalf of MOJVII. This policy applies to all employees, contractors, and all other users of information and information systems that support the operation and assets of MOJVII. This is a living document subject to change in accordance with NIST SP 800-53 and CMMC v

Responsibilities

All covered personnel accessing or using IT resources are responsible for adhering to this policy and with any local Identification and Authentication requirements.

Role	Definition
Management	The Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated officials at the senior leadership level are assigned the responsibility for the continued development, implementation, operation and monitoring of the Identification and Authentication process.
Security Liaisons	Security liaisons are responsible for ensuring that adequate user identification and authentication controls are present in all computing environments including those managed by agencies or by third parties.
Information System Owner	The Information System Owner (SO) is responsible for ensuring that identification and authentication controls for the system are implemented in coordination with agencies, information owners, security system administration, and 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 (ISO)s 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 are responsible for following the approved identification and authentication processes and the supporting controls.
Third Parties	Third party service providers with systems interconnected to the network are responsible for managing identification and authentication actions in accordance with this policy.

IA-1 - Policy

All 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 MARCO-

ONOPA JVII to implement the family of Identification and Authentication security controls. This policy provides requirements for the identification and authentication process which is required to assure that information systems are designed and configured using controls sufficient to safeguard MARCO-ONOPA JVII's information systems.

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

IA-2 - Identification and Authentication Authorized Users

Information systems and those operated on behalf of MOJVII shall be configured to uniquely identify and authenticate users (or processes acting on behalf of users). Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or

processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal access).

a. System Owners shall not allow the use of shared accounts (credentials used by more than one individual) within their system unless a risk assessment determines that the confidentiality, integrity or availability of information or information systems is not at risk. The use of shared user accounts makes it difficult to uniquely identify individuals accessing an information system, as well as provide detailed accountability of user activity within an information system.

b. Identification and authentication mechanisms shall be implemented at the application level, as determined by a risk assessment, to provide increased security for the information system and the information processes. This shall be in addition to identifying and authenticating users at the information system level (e.g., when initially logging into a desktop, laptop, or mobile device).

c. Access to non-privileged accounts, privileged accounts, and all local accounts shall be authenticated with passwords, personal identification numbers (PINs), tokens, biometrics, or in the case of multifactor authentication (MFA), some combination thereof. **Note:** See IA–5 - Authenticator Management for definitions of privileged and non-privileged accounts.

d. Information systems shall use MFA for the following conditions:

    i. Remote access to information systems using privileged accounts.

    ii. Remote network access with privileged and non-privileged accounts for information systems that receive, process, store, or transmit federal tax information (FTI) or other Highly Restricted data.

    iii. Remote access with privileged and non-privileged accounts such that one of the factors

is provided by a device separate from the system gaining access. The purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system.

e. Information systems shall implement replay-resistant authentication mechanisms for network access to privileged accounts, if technically configurable. Authentication processes resist replay attacks if it is impractical for an attacker to replay previous authentication messages and thus achieve unauthorized access. Replay-resistant techniques include, for example, protocols that use challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators (one-time passwords).

IA-3 - Device Identification and Authentication

To protect MARCO-ONOPA JVII Network from vulnerabilities that can be introduced when users access the network with unmanaged devices, such as personal computing devices, agencies shall require that all users accessing MARCO-ONOPA JVII Network adhere to required security configurations for their devices, including required patches and updated anti-virus signature files on those devices.

a. Procedures that verify node authentication measures shall be developed.

b. Agencies shall use only approved procedures, mechanisms, or protocols for host or device authentication. Approved mechanisms and protocols include, but are not limited to, the following:

   i. Media Access Control (MAC) address filtering, which provides basic filtering based on Open Systems Interconnection (OSI) Layer 2 (Data Link Layer) address information.

   ii. Vendor-specific solutions which provide basic identification and authentication for devices in a wired network on a per-port basis.

   iii. Wi-Fi Protected Access 2 (WPA2) in combination with MAC filtering.

   iv. Institute of Electrical and Electronics Engineers (IEEE) 802.1x.

   v. Network Access Control (NAC) technology, which is most built on the foundations of 802.1x.

c. Network routing controls should be implemented to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal sub networks (“subnets”).

IA–4 - Identifier Management

Agencies shall ensure that all information systems, to include cloud provided services, do the following:

a. Receive authorization from a designated representative (e.g., system administrator, technical lead or system owner) to assign individual, group, role, or device identifiers.

b. Select and assign information system identifiers that uniquely identify an individual, group, role, or device. Assignment of individual, group, role, or device identifiers shall ensure that no two users or devices have the same identifier.

c. Prevent reuse of identifiers for seven (7) years.

d. Disable identifiers after 120 days of inactivity, except as specifically exempted by management.

e. Delete or archive identifiers that have been disabled more than 365 days.

f.

IA–5 - Authenticator Management

Agencies shall manage information system authentication requirements. Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Agencies shall require the following:

a. Develop secure log-on procedures to be applied to all network components, operating systems, applications, and databases that implement a user identification and authentication mechanism. These procedures shall be designed to minimize the risk of unauthorized access.

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

c. Establish initial authenticator content for authenticators defined by MARCO-ONOPA JVII.

d. Ensure that authenticators have sufficient strength of mechanism for their intended use.

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

f. Change default content of authenticators, for example, the default password, prior to information system installation.

g. Require individuals to take, and have devices implement, specific security safeguards to protect authenticators from unauthorized disclosure and modification.

h. Change authenticators for group/role accounts when membership to those accounts changes.

i. Information systems shall display a message to users before or while they are prompted for their user identification and authentication credentials that warns against unauthorized or unlawful use. Refer to the Access Control policy AC-8 - System Use Notification for the standard MOJVII approved banner.

j. The log-on process should not be validated until all log-on data is input. Failing the process as each input field is completed will provide an attacker with information to further the attack.

k. Only generic "log-on failed" messages should be displayed if the user does not complete the log- on process successfully. Do not identify in the message whether the user identification, password, or other information is incorrect.

l. Agencies shall configure systems to limit the number of consecutive unsuccessful log-on attempts. If the number of consecutive unsuccessful log-on attempts exceeds the

established limit, the configuration shall either force a time delay before further log-on

attempts are allowed or shall disable the user account such that it can only be reactivated by a system or security administrator or an authorized service desk staff member.

m. For systems that store, transmit, or process FTI, the MARCO-ONOPA JVII shall password-protect the system initialization (boot) settings.

n. All newly assigned passwords shall be changed the first time a user logs into the information system.

o. Where technically configurable, passwords shall be at least eight (8) characters long for access to all systems and applications.

p. Passwords shall have at least one numeric, at least one special character, and a mixture of at least one uppercase and at least one lowercase letter.

q. Passwords shall not contain number or character substitutes to create dictionary words (e.g., d33psl33p for deepsleep).

r. Account passwords shall not traverse the network or be stored in clear text. All passwords stored shall be encrypted using FIPS-140-2 encryption.

s. Passwords shall not be inserted into email messages or other forms of electronic communication without proper encryption.

t. Information systems may allow the use of a temporary password for system logons as long as the temporary password is immediately changed to a permanent password upon the next logon attempt.

u. Passwords shall be different from all other accounts held by that user.

v. Agencies may use password management tools approved by the Enterprise Security and Risk Management Office (ESRMO). Approved password managers must be installed and managed locally on the user's machine (not offsite or in the "cloud"), must securely store passwords with a master key or key file, and must encrypt the password list with FIPS 140-2 encryption.

w. Passwords shall not be revealed to anyone, including supervisors, help desk personnel, security administrators, family members or co-workers.

x. Users shall enter passwords manually for each application or system, except for simplified/single sign-on systems that have been approved by MARCO-ONOPA JVII CIO.

y. Passwords shall be changed whenever there is the suspicion or likelihood that the password or system is compromised.

z. Agencies shall validate the identity of an end user who requests a password reset. Initial passwords and subsequent password resets shall utilize a unique password for each user account.

Password Management Standards – Non-Privileged Accounts

A non-privileged account is generally defined as a standard user account that does not have elevated privileges, such as administrator access to a system. For instance, non-privileged accounts cannot make configuration changes to an information system or change the security posture of a system. Information systems that use password-based authentication shall do the following:

a. Passwords shall have a minimum lifetime of one (1) day and a maximum lifetime of ninety 90 days. Password lifetime restrictions do not apply to temporary passwords.

b. Passwords shall not be reused until twenty-four (24) additional passwords have been created.

c. Passwords for citizens and business users are recommended to be changed at least annually.

Password Management Standards – Privileged Accounts

A privileged account is generally defined as a system administrator account. Privileged accounts have elevated permissions than those of a non-privileged user account. Examples of privileged accounts include those that have root access, system administrator access, and accounts associated with database ownership and router management.

a. Privileged accounts are generally used for performing administrative functions, such as configuration changes, system/software upgrade, patch installations, and/or developing software.

b. Privileged accounts shall have passwords with a minimum lifetime of one (1) day and a maximum lifetime of thirty (30) days whenever technically configurable but must not exceed sixty (60) days.

Password Management Standards—Service Accounts

A service account is a non-interactive account created by system administrators for automated use by an application, operating system, or network device for their business purpose. Service accounts shall be managed by the following:

a. Service accounts shall only be granted the minimum level of access required to run a process.

b. Service accounts must be dedicated solely to their business purpose and not shared by an end user.

c. Service accounts shall be separate from privileged and non-privileged accounts.

d. All service accounts must have appropriate logging as specified by the MARCO-ONOPA JVII of account activity. The application/device owner must audit the service account usage semi-annually, at a minimum.

e. Whenever technically configurable, service account passwords must have change intervals appropriate to the level of risk posed by a potential compromise of the system.

f. At a minimum, change intervals shall not exceed 364 days (1 year).

g. A service account password must be changed immediately after any potential compromise or any individual who knows the password leaves the MARCO-ONOPA JVII or changes roles within the MARCO-ONOPA JVII.

h. In the special case where an application or system is *specifically designed* for service accounts to use 'non-expiring' passwords to complete their business purpose, these accounts must be.
preapproved by MARCO-ONOPA JVII management and the MARCO-ONOPA JVII's

security liaison. MARCO-ONOPA JVII approved controls, policies, and procedures must be in place to closely monitor and mitigate the risk of non-expiring passwords.

IA-6 - Authenticator Feedback

Agencies shall ensure that all information systems including those operated on behalf of MOJVII do the following:

a. Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

b. Mask passwords upon entry (e.g., displaying asterisks or dots when a user types in a password) and not displayed in clear text.

IA-7 - Cryptographic Module Authentication

a. Agencies shall ensure that mechanisms are implemented for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

b. Validation provides assurance that when MARCO-ONOPA JVII implements cryptography, the encryption functions have been examined in detail and will operate as intended.

c. All encrypted electronic transmissions must be encrypted using FIPS 140-2 validated cryptographic modules. NIST maintains a list of validated cryptographic modules on its website at http://csrc.nist.gov/.

IA-8 – Identification and Authentication (Non-MARCO-ONOPA JVII Users)

This control typically applies to MARCO-ONOPA JVII information systems that are accessible to the general public, for example, public-facing websites. Agencies shall ensure the following for all non-MARCO-ONOPA JVII users accessing information systems, including those operated on behalf of MOJVII.

a. Approved third-party credentials must meet or exceed the set of minimum requirements, security, privacy, and MARCO-ONOPA JVII maturity requirements.

b. MARCO-ONOPA JVII information systems shall be configured to uniquely identify and authenticate non- MARCO-ONOPA JVII users or processes acting on behalf of non-MARCO-ONOPA JVII users.

c. MARCO-ONOPA JVII information systems shall uniquely identify and authenticate non-MARCO-ONOPA JVII users for all access other than those accesses explicitly identified and documented as exceptions in the MARCO-ONOPA JVII Access Control Policy MOJVII-301-00 regarding permitted actions without identification and authentication.

IA-9 - Service Identification and Authentication (Optional)

This control is optional for Low and Moderate risk information systems.

IA-10 - Adaptive Identification and Authentication (Optional)

This control is optional for Low and Moderate risk information systems.

IA-11 - Re-Authentication (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 agencies and vendors of MARCO-ONOPA JVII 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: