State of Maryland

STANDARD

IDENTIFICATION & AUTHENTICATION

Document No.	Last Updated	Prepared By
MD-STD-307-IA-01	02/18/2026	DOIT OSM

Identification and Authentication (I&A), as a core principle of Zero Trust Architecture (ZTA), is fundamental to security and access control for digital systems by enforcing continuous verification, adaptive authentication, and least privilege access to prevent unauthorized access.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed to verify the identities of users, devices, and systems before granting access to State systems.
Scope	This standard provides an organizational approach for ensuring that only authorized users gain access to systems and data.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
Related Policy	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
Baseline	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
Distribution	This document is approved for public distribution and may be shared with external stakeholders, partners, and regulatory bodies. It reflects the State's commitment to transparency, compliance, and operational excellence. Unauthorized modifications or misrepresentation of this document are strictly prohibited.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWORD

Agencies that use Department of Information Technology DoIT-managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services, such as hosting platforms, identity management, and network infrastructure, are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

Throughout this document, informational call-out boxes are utilized to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible”, “encouraged”, or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

STANDARDS

307 State Strategy

These standards establish a baseline of identification and authentication practices that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

307-1 Develop Agency-Level Procedures (IA-1)

In alignment with this standard, develop and document agency-level Identification & Authentication procedures. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on changes and risk at least every **3 years**. At a minimum, the procedures must address purpose, scope, roles and responsibilities, and guidelines.

307-2 Implement Identification and Authentication (Organizational Users) (IA-2)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users. Require multi-factor authentication (MFA) for all access to State systems and where feasible phishing-resistant MFA particularly for High Value State Systems (HVSS) and systems housing non-public data (Data Classification Level 2 or above). Short Message Service (SMS)-based text code, a short numeric or alphanumeric code sent via SMS to a user's mobile phone, shall not be used for authentication or verification purposes.

Phishing-Resistant Multi-Factor Authentication

Phishing-resistant MFA uses authentication methods that cannot be easily intercepted, replayed, or socially engineered. Unlike traditional MFA (e.g., SMS codes or app-based prompts), phishing-resistant MFA relies on cryptographic techniques and device-bound credentials that validate both the user and the device. Common methods include: a) Public-key cryptography bound to a specific device (e.g., Yubi Keys, biometric authenticators); b) Smart Cards that require physical possession and personal identification number (PIN) entry; and c) Passkeys, which are device-bound credentials that replace passwords entirely (e.g., Apple, Google, Microsoft ecosystems).

IA-2(1): Implement phishing-resistant MFA for access to privileged accounts.

IA-2(2): Implement MFA for access to non-privileged accounts.

IA-2(8): Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

Replay-Resistant Authentication

Designed to prevent attackers from capturing and reusing valid authentication data (like passwords or tokens) to gain unauthorized access. Replay-resistant techniques include, for example, one-time passwords (OTPs), time-based tokens, challenge-response protocols, Nonce-based Application Programming Interface (API) Authentication.

307-3 Implement Device Identification and Authentication (IA-3)

Uniquely identify and authenticate all endpoint devices (especially those that receive, process, store, or transmit non-public information) before establishing a connection to State resources (i.e., on prem or cloud-based). Where device authentication cannot be enforced (i.e., contractors using non-Maryland managed devices) the MFA token expiration shall be at most **12 hours**.

Identifying & Authenticating Endpoint Devices

To uniquely identify and authenticate devices prior to accessing state-owned or cloud-hosted resources, every device shall have a registered ID (such as a serial number or certificate) and go through a secure login process, often using tools like device certificates or management software. To check device health and identity automatically before allowing access, a mix of hardware, software, and network-based tools are required. Examples include: a) Certificate-based authentication (e.g. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)); b) Endpoint management platforms (e.g., Microsoft Intune); c) Network access control (e.g., Cisco Identity Services Engine (ISE)); d) Security & Monitoring Tools (e.g., Microsoft Defender); e) Hardware authentication devices (e.g., Yubi Key, Trusted Platform Module (TPM)); and f) Biometric & Behavioral Authentication (e.g., Windows Hello, Apple FaceID).

307-4 Manage System Identifiers (IA-4)

Manage system identifiers by: a) Receiving authorization from a designated official (supervisor, security monitor, or system administrator) or agency designee to assign an individual, service, or device identifier; b) Selecting an identifier that identifies an individual, service, or device; c) Assigning the identifier to the intended individual, service, or device; and d) Preventing reuse of identifiers for at least **2 years** or as defined in agency level procedures based on risk, business needs, and audit retention timelines (whichever is greater); and e) Disabling identifiers after **30 days** of inactivity.

For cloud services, identifier management should also include supplemental controls provided by the cloud provider to prevent duplicate identifiers from being stored.

IA-4(4): Manage individual identifiers by uniquely identifying each individual as either a State employee, or Contractor. Administrative accounts must be distinct in nomenclature as well.

Where feasible, implement dynamic identity management with continuous validation using identity governance solutions that monitor and revoke access based on real-time risk assessments.

307-5 Manage System Authenticators (IA-5)

Manage system authenticators (e.g., tokens, public key infrastructure (PKI) certificates, smart cards) by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual, service, or device receiving the authenticator;
- Establishing initial authenticator content for any authenticators;
- Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
- Changing default authenticators upon system installation or prior to first use;
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
- Terminating application sessions (i.e., forced log out) to require reauthentication at least once per **12 hours** during an extended usage session, regardless of user activity;
- Requiring reauthentication following any period of inactivity lasting more than **30 minutes** or shorter duration commensurate with risk;
- Protecting authenticator content from unauthorized disclosure and modification;
- Requiring individuals protect authenticators;
- Changing authenticators for group or role accounts when membership to those accounts changes;
- Changing the passwords at least **annually,** ideally using automated mechanisms (i.e., PAM tool), on service accounts and non-human identities which use elevated privileges; and
- Implementing secure password storage standards in alignment with the NIST SP 800-63B-4 Digital Identity Guidelines.

For public facing systems that require user identification and authentication, E-authentication or Digital Identity Risk Assessment (DIRA) criteria should be used to address authentication requirements along with the policy and procedures documented under this security control.

Digital Identity Risk Assessment (DIRA)

DIRA is a systematic evaluation of risks associated with digital identities and authentication processes that helps implement NIST SP 800-63 Digital Identity Guidelines. It helps organizations determine whether their authentication methods (passwords, MFA, biometrics, passkeys, etc.) provide the right level of assurance for protecting data and services. Refer to the Digital Identity Risk Assessment Playbook for more information[2].

IA-5(1): For password-based authentication:

- Maintain a list of commonly used, expected, or compromised passwords and update the list annually and when organizational passwords are suspected to have been compromised directly or indirectly;
- Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords;
- Transmit passwords only over cryptographically protected channels;
- Store passwords using an approved salted key derivation function (e.g., keyed hash);
- Require immediate selection of a new password upon account recovery;
- Employ automated tools (i.e., approved password generators or managers) to assist the user in selecting strong password authenticators;
- Do not permit the use of null passwords;
- Create individual user accounts for each authorized user;
- Do not permit user accounts without passwords or duplicate accounts;
- Do not use shared accounts unless operationally required, justification documented, and approved by the apprporiate AO; and

Employ the following standards:

Password Standards

Subject	Description*
Length	Require a minimum of 15 characters in length; and maximum of 64 characters.
Characters	Permit all printing ASCII [RFC20] characters; space character; and Unicode [ISO/ISC 10646] characters.
Truncating	Request the password to be provided in full (not a subset of it) and verify the entire submitted password (e.g., not truncate it).
Composition	Accept spaces and Unicode characters.

[2] DIRA Playbook: https://www.idmanagement.gov/playbooks/dira/

Subject	Description*
Verification	Check new passwords against known compromised lists.
Complexity	**Do not** impose additional composition rules (e.g., requiring mixtures of different character types)
Expiration	**Do not** require subscribers to change passwords periodically, unless there is evidence that the authenticator has been compromised.
Hint	**Do not** permit the subscriber to store a hint (e.g., a reminder of how the password was created) or knowledge-based questions (e.g., "first pet").
Security Questions	**Do not** prompt subscribers to use knowledge-based authentication (KBA) (e.g., “What was the name of your first pet?”) or security questions when choosing passwords.

** Adapted from NIST SP 800-63B-4*

IA-5(2): For public key-based authentication:

- Enforce authorized access to the corresponding private key; and
- Map the authenticated identity to the account of the individual or group.

When PKI is used:

- Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
- Implement a local cache of revocation data to support path discovery and validation.

Public-Key Based Authentication

Public key-based authentication uses a cryptographic key pair, where the public key is shared and the private key is kept secret, to prove identity without transmitting secrets, offering stronger security and resistance to common attacks. While passwords are easier to deploy, public key methods (like certificate-based login or Secure Shell (SSH) keys) are more secure and better suited for high-assurance environments. PKI based access enables passwordless access but requires more complex infrastructure for key management and revocation.

IA-5(6): Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

307-6 Protect Authentication Information (IA-6)

Obscure feedback of authentication information (i.e., mask system responses) during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

307-7 Implement Cryptographic Module Authentication (IA-7)

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication. Minimum encryption standards are defined in MD-STD-318-SC System and Communication Protection Standard, Section 318-6.

307-8 Implement Identification and Authentication (Non-Organizational Users) (IA-8)

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users using federated identity solutions and enforcing least privilege access for third-party users. All public users accessing State systems must be required to authenticate using MFA.

IA-8(2): Accept only external authenticators that are approved third-party credentials; and Document and maintain a list of accepted external authenticators. Third-party credentials are those credentials issued by non-Federal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative[3].

IA-8(4): Conform to FICAM-issued profiles for identity management (as applicable).

307-9 Require Re-authentication (IA-11)

Require users to re-authenticate regularly, and when not feasible, require re-authentication when credentials change, when security categories of systems change, or when the execution of privileged functions occurs. Where feasible, use behavioral analytics and Artificial Intelligence (AI)-driven anomaly detection to adjust authentication requirements dynamically.

Enhanced Authentication

In modern identity and access management systems, it is increasingly feasible to enhance authentication by integrating behavioral analytics and AI-driven anomaly detection. These technologies monitor user behavior (e.g., login times, device types, geographic location, access patterns) and establish a baseline of normal activity. When deviations from this baseline occur, such as a login attempt from an unusual location or device, the system can dynamically adjust authentication requirements. This might involve triggering MFA, requiring certificate-based login, or temporarily restricting access.

[3] https://www.idmanagement.gov/arch/

307-10 Perform Identity Proofing (IA-12)

Identity proof users who require accounts for logical access to systems based on appropriate identity assurance level requirements below; Resolve user identities to a unique individual; and Collect, validate, and verify identity evidence.

Identity Assurance Levels

Level	Definition	Typical System Type	Examples
IAL1	No identity proofing required; self-asserted identity	Low-risk public access systems	Public portals, newsletters, anonymous surveys
IAL2	Requires validated identity evidence (e.g., government ID); remote or in-person proofing	Moderate-risk systems handling non-public or personal information	Health portals, benefits enrollment, tax filing
IAL3	Requires in-person proofing and verified biometric match	High-risk systems with legal, financial, or national security impact	Law enforcement databases, financial systems

*Based on NIST SP 800-63A-4

IA-12(3): Require for all users (e.g., employees, contractors, vendors, third-party providers) that the presented identity evidence be validated and verified either through document-based verification (i.e., official documents like passports, driver's licenses, or national ID cards, which are checked for authenticity) or third-party verification (i.e., external identity providers (IdPs) that verify and vouch for a user's identity, such as government or banking).

IA-12(5): Require that a notice of proofing be delivered through an out-of-band channel to verify the user’s address (physical or digital) of record.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cybersecurity Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*
NIST SP 800-63B-4	Digital Identity Guidelines	This is a three-volume publication covering identity proofing, authentication, and federation.	*csrc.nist.gov (LINK)*
CISA Bulletin *Oct 2022*	Implementing Phishing-Resistant MFA	This fact sheet is intended to provide for IT leaders and network defenders an improved understanding of current threats against accounts and systems that use MFA.	*CISA: Implementing Phishing-Resistant MFA*

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID	Standard	Compliance
307-1	**Develop Agency-Level Procedures (IA-1)**	☐ Yes ☐ No
307-2	**Implement Identification and Authentication (Organizational Users) (IA-2)**	☐ Yes ☐ No
307-3	**Implement Device Identification and Authentication (IA-3)**	☐ Yes ☐ No
307-4	**Manage System Identifiers (IA-4)**	☐ Yes ☐ No
307-5	**Manage System Authenticators (IA-5)**	☐ Yes ☐ No
307-6	**Protect Authentication Information (IA-6)**	☐ Yes ☐ No
307-7	**Implement Cryptographic Module Authentication (IA-7)**	☐ Yes ☐ No
307-8	**Implement Identification and Authentication (Non-Organizational Users) (IA-8)**	☐ Yes ☐ No
307-9	**Require Re-authentication (IA-11)**	☐ Yes ☐ No
307-10	**Perform Identity Proofing (IA-12)**	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system's documented security posture.