Identification and Authentication Standard

Effective Date: 12/19/2022
Creation Date: 12/16/2022
Version: 1.0

1. Purpose

The purpose of this Standard is to ensure that only authorized Arkansas DIS users and devices (or processes acting on behalf of users) are identified and authenticated in compliance with IT security policies, standards and procedures.

2. Applicability

This standard covers all systems developed by, or on behalf of the Arkansas Division of Information Systems (DIS). This includes all development, test, quality assurance, production and other ad hoc systems.

Notations of specific control items (e.g., CJIS, FTI, PCI) only pertain to the systems that are required to comply with such regulations.

3. Definitions

Refer to the DIS Regulatory Definitions.

4. Standard

4.1 Identification and Authentication (Organizational Users) IA-2 (NIST Moderate Control)

a. The use of shared accounts is prohibited within the AR DIS network.
b. Identification and authentication mechanisms shall be implemented at the application level, as well as the information system level.
c. Access to non-privileged accounts, privileged accounts, and all local accounts shall be authenticated with one or more of the following:
    - Passwords
    - Personal Identification Numbers (PINs)
    - Tokens
    - Biometrics

- Multi-factor Authentication (MFA)

4.2 Multi-factor Authentication to Privileged Accounts IA-2(1) (NIST Moderate Control)

MFA will be implemented for access to privileged accounts.

4.3 Multi-factor Authentication to Non-Privileged Accounts IA-2(2) (NIST Moderate Control)

MFA will be implemented for access to non-privileged accounts.

4.4 Individual Authentication with Group Authentication IA-2(5) (CJIS Only Control)

Users are required to be individually authenticated before granting access to any shared accounts or resources.

4.5 Access to Accounts — Replay Resistant Areas IA-2(8) (NIST Moderate Control)

Replay-resistant authentication mechanisms will be utilized for network access to privileged accounts. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

4.6 Acceptance of PIV Credentials IA- 2(12) (NIST Moderate Control)

Systems shall accept and electronically verify Personal Identity Verification (PIV) credentials.

4.7 Out-of-band Authentication IA- 2(13) (CJIS Only Control)

Advanced Authentication (AA) shall not be required for users requesting access to CJI from within the perimeter of a physically secure location, when the technical security controls have been met, or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services. In the event the security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. The intent of AA is to meet the standards of two-factor authentication. AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access.

4.8 Device Identification and Authentication IA- 3 (NIST Moderate Control)

Systems will uniquely identify and authenticate all devices before establishing a network connection.

4.9 Cryptographic Bidirectional Authentication IA- 3(1) (CJIS Only Control)

CJIS systems will authenticate devices before establishing defined connections using a type of bidirectional authentication that is cryptographically based.

4.10 Device Attestation IA- 3(4) (CJIS Only Control)

CJIS systems will ensure that identification and authentication of a device is based on its configuration and known operating state.

4.11 Identifier Management IA- 4 (NIST Moderate Control)

DIS manages information system identifiers by:

a. Receiving authorization from the information owner to assign an individual, group, role, service, or device identifier.

b. Selecting an identifier that identifies an individual, group, role, service, or device.

c. Assigning the identifier to the intended individual, group, role, service, or device.

d. Preventing reuse of identifiers as defined in the Regulatory Settings spreadsheet.

e. Disabling the identifier as defined in the Regulatory Settings spreadsheet

4.12 Identify User Status IA- 4(4) (NIST Moderate Control)

Individual identifiers are managed by uniquely identifying users (e.g., employee, contractor, agency user).

4.13 Authenticator Management IA- 5 (NIST Moderate Control)

a. DIS shall manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator.

b. Establish initial authenticator content for authenticators defined by the organization.

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

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

e. Change default authenticators prior to first use.

f. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators. These conditions shall be defined in the Regulatory Settings spreadsheet.

g. Change/refresh authenticators as defined in the Regulatory Settings spreadsheet.

h. Protect authenticator content from unauthorized disclosure and modification.

i. Require individuals and devices to implement specific security safeguards to protect authenticators.

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

4.14 Password-based Authentication IA- 5(1) (NIST Moderate Control)

a. Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.

b. Ensure passwords must contain characters from three of the five categories defined in the Regulatory Settings spreadsheet.

c. Require passwords to have a minimum length as defined in the Regulatory Settings spreadsheet.

d. Enforce at least one changed character when new passwords are created.

d. Store and transmit only cryptographically protected passwords.

e. Enforce password minimum and maximum lifetime restrictions as defined in the Regulatory Settings spreadsheet.

f. Prohibit password reuse as defined in the Regulatory Settings spreadsheet.

g. Allow the use of a temporary password for system logons with an immediate change to a permanent password

4.15 Public Key-based Authentication IA- 5(2) (CJIS Only Control)

a. Ensure that CJIS information systems, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

b. Enforce authorized access to the corresponding private key.

c. Map the authenticated identity to the account of the individual or group.

d. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

4.16 Change Authenticators Prior to Delivery IA- 5(5) (CJIS Only Control)

CJIS systems require developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.

4.17 Protection of Authenticators IA- 5(6) (NIST Moderate Control)

Authenticators shall be commensurate with the security category of the information to which use of the authenticator permits access. For example, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.

4.18 No Embedded Unencrypted Static Authenticators IA- 5(7) (CJIS Only Control)

Ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

4.19 Multiple System Accounts IA- 5(8) (CJIS Only Control)

Implement safeguards for CJIS systems to manage the risk of compromise due to individuals having accounts on multiple information systems.

4.20 Dynamic Credential Binding IA- 5(10) (CJIS Only Control)

CJIS information systems will dynamically provision identities.

4.21 Authentication Feedback– IA- 6 (NIST Moderate Control)

Ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

4.22 Cryptographic Module Authentication IA- 7 (NIST Moderate Control)

Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

4.23 Identification and Authentication (non-organizational Users) IA-8 (NIST Moderate Control)

Ensure that information systems uniquely identify and authenticate non-agency users or processes acting on behalf of non-agency users.

4.24 Acceptance of PIV Credentials from Other Agencies - IA- 8(1) (NIST Moderate Control)

Ensure that information systems accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies.

4.25 Acceptance of External Authenticators IA- 8(2) (NIST Moderate Control)

Approved third-party credentials will meet or exceed the minimum FICAM approved requirements.

4.26 Use of Defined Profiles IA- 8(4) (NIST Moderate Control)

Information systems shall conform to FICAM-issued profiles.

4.27 Acceptance of PIV-I Credentials IA- 8(5) (CJIS Only Control)

a. Ensure that the CJIS information systems accept and electronically verify Personal Identity Verification (PIV) credentials from other government agencies.

b. Ensure that the CJIS information systems accept only Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved third-party credentials.

c. Ensure that the CJIS organization employs only FICAM-approved information system components to accept third-party credentials.

4.28 Service Identification and Authentication IA- 9 (PCI & FTI Only Control)

Uniquely identify and authenticate DIS defined system services and applications before establishing communications with devices, users, or other services or applications.

4.29 Adaptive Authentication IA- 10 (PCI Only Control)

Employ specific pre-defined techniques or mechanisms and establish protocols to assess suspicious behavior when individuals are accessing an information system. Adaptive authentication does not replace and is not used to avoid the use of multi-factor authentication mechanisms but augments the implementation of multi-factor authentication.

4.30 Re-authentication IA- 11(CJIS Only Control)

In addition to the re-authentication requirements associated with device locks, CJIS systems will require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

4.31 Identity Proofing IA- 12 (NIST Moderate Control)

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.
b. Resolve user identities to a unique individual.
c. Collect, validate, and verify identity evidence.

4.32 Identity Evidence IA- 12(2) (NIST Moderate Control)

Require evidence of individual identification be presented to the registration authority. The forms of acceptable evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

4.33 Identity Evidence Validation and Verification IA- 12(3) (NIST Moderate Control)

Require that the presented identity evidence be validated and verified. Acceptable verification methods must be consistent with the risks to the systems, roles, and privileges associated with the user's account.

4.34 In-person Validation and Verification IA- 12(4) (CJIS Only Control)

CJIS require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

4.35 Address Confirmation IA- 12(5) (NIST Moderate Control)

Require that an identity proofing process be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

5. Authority

Refer to the DIS Regulatory Definitions document.

6. Compliance

This control shall take effect upon publication. Compliance is expected with all DIS controls. Employees not following this DIS control are subject to the standard DIS disciplinary procedures.

If compliance with this control is not feasible or technically possible, or if deviation from this control is necessary to support a business function, applicable entities shall request an exception through the DIS Exception Request Procedure.

7. Related Documentation

Identification and Authentication Procedures
Policy_Identification and Authentication
Procedure_Exception Request
Regulatory Definitions
Regulatory Settings spreadsheet

8. Revision History

This standard shall be subject to review according to the Regulatory Settings spreadsheet to ensure relevancy.

Date	Description of Change	Reviewer
12/16/2022	Moved from Draft to Final	Greggari Tucker, Deputy Chief Information Security