WaTech
Washington Technology Solutions

Identification and Authentication Background

New, Update or Sunset Review? Sunset Review

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

This standard expands on and replaces the current 141.10 (6.2, 6.3) requirements. Based on workgroup and community feedback, changes were made to improve clarity for agency adoption and accountability.

This policy's updates draw from the NIST 800-63 series publications: Digital Identity Guidelines, Enrollment and Identity Proofing, Authentication and Lifecycle Management, and Federation and Assertions.

What is the business case for the policy/standard?

This standard requires controls for identification and authentication of all organizational and non-organizational users and devices necessary to securely conduct of state business.

What are the key objectives of the policy/standard?

- Aligning the processes and tools used to link user and device identities to an account.
- Ensure authentication mechanisms are appropriate to the level of risk associated with the data category processed by the resource the user or device is authenticating to.
- Requiring detailed documentation of authentication methods and processes in the annual application inventory and the agency's security program, ensuring transparency and compliance.
- Managing user, group, role, service, and device identifiers to ensure unique and secure access controls, preventing unauthorized access and privilege escalation.

How does policy/standard promote or support alignment with strategies?

Enterprise Strategic Plan
The digital trust pillar upholds and is interwoven in all of the 2023-2025 Enterprise IT Strategic plan goals.

This standard supports “Creating a Government Experience that Leaves No Community Behind” (Goal 2) by considering barriers to public access to data and security concerns when selecting authentication controls.

This standard also supports Goal 3 “Innovative Technology Solutions Create a better Washington” by emphasizing secure and inclusive access, leveraging secure technology, addressing systemic societal challenges, and supporting data-driven decision-making.

What are the implementation considerations?

To ensure a smooth transition to the new authentication standards, it is essential to ensure that existing systems and applications are compatible with them, including MFA and encryption requirements. This involves assessing the current infrastructure to support new authentication mechanisms, such as additional servers or network upgrades.

Additionally, it is crucial to enhance helpdesk capabilities to assist users with the transition, including support for password resets and MFA enrollment. Detailed risk assessments are necessary to identify and mitigate potential threats related to the new authentication methods.

Creating channels for users to provide feedback on the new authentication processes will allow continuous improvement. Staying updated with the latest advancements in authentication technologies and incorporating them into the security framework as needed will help maintain their effectiveness and security.

How will we know if the policy is successful?

Specific: Implement robust credential management and authentication policies to enhance security by reducing credential sharing incidents, achieving password security compliance, increasing MFA adoption, ensuring proper identity verification, minimizing credential exposure, and securing service accounts.
Measurable: Response. Enhance security by eliminating fraudulent identity incidents, attaining compliance with password policies, implementing MFA for all high-risk scenarios, verifying the identity of all IT systems users, minimizing temporary authenticator exposure, and ensuring all service accounts comply with duplicate account and password documentation requirements.
Achievable: Implement strict policies and provide education to prevent credential sharing; deploy tools and training for managing complex passwords; roll out MFA solutions with necessary support; establish a standardized identity verification process; automate the expiration of temporary credentials; and conduct regular audits to ensure service accounts meet security standards.
Relevant: Enhancing credential security reduces the risk of unauthorized access, identity fraud, and security vulnerabilities. Ensuring compliance with password policies, implementing MFA, verifying user identities, minimizing temporary authenticator exposure, and securing service accounts are critical measures to protect systems and data.
Timely: We will review the progress toward the objectives at the three-year sunset review mark.
Equitable: Ensure all employees, regardless of role or department, have equal access to security tools, training, and support. Apply security policies and processes consistently across the organization to maintain fairness and inclusivity.