EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

August 31, 2026

M-26-18

MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Scaling Use of Login.gov to Deliver a Universal Sign-on for Public Services

On August 21, 2025, President Trump issued Executive Order 14338, *Improving Our Nation Through Better Design*, reaffirming the importance of delivering high-quality digital experiences.[1] Failure to do so comes at the expense of the American public, costing them time or even access to critical services. It also impedes Government efficiency by pushing the public to more costly and often less secure phone, in-person, or paper-based interactions.

Digital identity is a foundational element of digital service delivery. To access services online, users often begin by establishing their identity or signing into an account. In the absence of a clear Government-wide strategy, agencies have deployed a range of different solutions and taken inconsistent approaches for managing digital identity, creating unnecessary burden and inefficiencies for the public and Government alike. This policy enforces Login.gov as the universal sign-on for accessing public services online, enabling more seamless and efficient service delivery while safeguarding user privacy and supporting resilience against fraud and security threats.

Scope & Applicability

Except where otherwise stated, this memorandum applies to all agencies.[2]

This memorandum applies to the use of Login.gov and other digital identity solutions on public-facing[3] agency websites for services accessed by the public through user authentication.[4]

---

[1] Available at https://www.whitehouse.gov/presidential-actions/2025/08/improving-our-nation-through-better-design/.

[2] As used in this memorandum, "agency" has the meaning provided in 44 U.S.C. § 3502(1). See footnote 6 for exceptions to the requirement to use Login.gov.

[3] For the purposes of this memorandum, "public-facing" means intended to be accessed and used by members of the public, rather than by Federal Government employees or contractors acting on behalf of an agency.

[4] For the purposes of this memorandum, "authentication" refers to the process used to confirm that a previously established account subscriber holds one or more authenticators bound to the account (e.g., entering a username and

Agencies are encouraged to expand use of Login.gov and conform to the requirements of this memorandum for other digital channels (e.g., mobile applications), where appropriate.

This memorandum does not apply to public-facing websites for services accessed solely by: 1) organizations, or individuals acting on behalf of an organization (e.g., businesses, state and local governments); or 2) individuals acting on behalf of another individual. However, agencies are permitted and encouraged to expand the use of Login.gov and conform to the requirements of this memorandum for these other websites, where appropriate. Regardless of the use of Login.gov, agencies remain responsible for applying appropriate digital identity controls for enterprise identity and all of their public services, including those not covered by this memorandum.[5]

Policy

I. Enforcing Login.gov as the Universal Sign-on for Public Services

Agencies currently use a range of distinct digital identity solutions. This results in members of the public often needing to maintain multiple sign-ons to interact with agencies and services. It also results in agencies needlessly reverifying an individual's identity, often at a significant cost, where an existing verification could satisfy operational requirements. Further, agencies often pay commercial vendors to verify identity attributes for which the Federal Government may itself maintain an official data source.

Login.gov is purpose-built for public sector needs but integrates with leading private sector vendors and tools. Universal use of Login.gov for authentication gives the public one consistent sign-on to access public services. And as use of Login.gov for identity verification increases, the Government realizes cost efficiencies from economies of scale and a reduction in duplicative verification costs. Increased use of Login.gov also supports the Government's security posture, enabling deployment at scale of leading technologies and security practices to prevent and respond to emerging threats.

A. Use of Login.gov for Authentication

As required by law, agencies must offer Login.gov, the single sign-on identity platform developed by the Administrator of General Services, as a sign-on option for all in-scope public-facing websites, as described above.[6] In scenarios where an agency provides a service both to individuals acting on their own behalf and to organizations or representatives of a third-party,

---

password). *See* National Institute for Standards and Technology (NIST) Special Publication (SP) 800-63-4, *Digital Identity Guidelines*, Appendix B (https://pages.nist.gov/800-63-4/), for a formal glossary of digital identity terms.

[5] To manage digital identity, agencies should follow applicable law and existing Office of Management and Budget (OMB) policy, including OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*; OMB M-21-04, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act*; and OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.*

[6] 6 U.S.C. § 1523(b)(1)(D). The Login.gov statutory mandate and accompanying certification requirement do not apply to the Department of War (DoW), a national security system, or an element of the intelligence community, as provided by 6 U.S.C. § 1523(c). However, DoW is encouraged to offer Login.gov for public-facing websites that require user authentication to the extent practicable.

agencies must offer Login.gov for individuals acting on their own behalf but may choose whether or not to offer Login.gov for organizations or third-party representatives.

If an agency cannot meet this requirement by the deadlines indicated in the Appendix, the agency must submit a notice to the Office of Management and Budget (OMB) by the applicable deadline identifying the operational requirements that prevent the agency from meeting the requirement. The notice must contain a personal certification from the head of the agency that satisfies the requirements of 6 U.S.C. § 1523(b)(2), and it must be shared with the required Congressional committees.[7] OMB will provide subsequent reporting instructions to agencies, specifying the expected format, contents, and delivery channel for this notice.

Agency implementation of Login.gov should follow the best practices set out by the General Services Administration (GSA), as specified in the Appendix.

B. Use of Login.gov for Identity Verification

For public-facing websites that require identity verification[8] in addition to authentication, agencies must use Login.gov's identity verification service unless they determine that Login.gov does not meet requirements specific to the user base, risk profile, or operations of a given service or transaction.

C. Use of Other Identity Solutions

When use of Login.gov is required under Section I.A or I.B, agencies may also offer other authentication or identity verification solutions in order to: 1) meet specific use cases that Login.gov is unable to fully meet (e.g., a particular user population or operational requirement), or 2) avoid imposing additional burden on a significant population of users (e.g., users that rely on an existing sign-on option).[9] For example, certain user populations such as young people or members of the public living abroad may have limited official records which can make identity verification more challenging and may warrant the use of other solutions.

Agencies must phase out identity solutions that do not meet this description and should routinely reevaluate the need for continued use of solutions other than Login.gov, including by assessing each solution's volume of active users. When offering other solutions, agencies must promote Login.gov as the default option for new account creation for any user population that Login.gov is able to serve. When using other solutions in addition to Login.gov for a given service or transaction, agencies must seek to maximize parity in assurance level selection for authentication and identity verification between Login.gov and the other solution(s).[10]

---

[7] 6 U.S.C. § 1523(b)(2)(B).

[8] For the purposes of this memorandum, "identity verification" refers to the process of confirming that a claimed identity is valid and that the person making the claim is who they say they are. While technically verification is a specific outcome of the "identity proofing" process as defined by NIST SP 800-63-4, this memorandum uses "identity verification" as an overarching term, synonymous with "identity proofing."

[9] This policy supersedes Section V.5 of OMB Memorandum M-19-17, which required agencies to "use Federally provided or commercially provided shared services, to the extent available, to deliver identity assurance and authentication services to the public."

[10] See assurance levels outlined in NIST SP 800-63A-4, Section 4, and SP 800-63B-4, Section 2.

II. Considering Customer Experience as a Component of Risk Management

Effective digital identity management requires both the credential service provider (CSP) (e.g., Login.gov) and relying party (agency providing the service) to balance needs and outcomes related to customer experience, mission effectiveness, privacy, and threat resistance. Use of Login.gov supports agencies' needs across these dimensions, but agency-specific risk management processes are also critically important to ensure the overall effectiveness of digital identity programs.

Consistent with the guidelines on digital identity risk management issued by the National Institute for Standards and Technology (NIST),[11] in deciding whether to require identity verification as a condition for accessing an online service and selecting appropriate assurance levels and any supplemental controls, agencies must consider the impact of those decisions on users and avoid friction that is unjustified by the risk profile of the service or transaction. Agencies must adequately document their risk-based decisions in order to effectively evaluate the outcomes of these decisions over time.

On an ongoing basis, agencies must monitor the performance and outcomes of digital identity programs, leveraging metrics from their CSP(s) and any additional, directly relevant data that agencies gather, to identify and inform potential changes to selected assurance levels and any supplemental controls.[12] Performance metrics such as pass rates, abandonment rates, and completion time can be particularly helpful in identifying user burden or limitations on user access. These user-focused metrics should be considered alongside fraud and security metrics, as well as privacy considerations, for a balanced, multi-disciplinary view of the overall performance of digital identity programs.

III. Accepting Previously Verified Credentials

As use of Login.gov for identity verification increases, agencies benefit from being able to reuse previously verified credentials, which reduces the need to verify an individual's identity more than once. Users also benefit from not needing to complete duplicative and potentially burdensome verification processes. However, these benefits hinge on agencies accepting common standards for verification at any given assurance level.

Because Federal programs vary widely in their missions and operate within a broad range of threat environments, consistent with NIST guidelines, agencies should directly weigh their specific risks, the unique aspects of their user populations, and their desired outcomes to set an appropriate Identity Assurance Level (IAL) to safeguard their services and transactions.[13] For those agencies that use Login.gov for identity verification per Section I.B., agencies should accept all suitable Login.gov service offerings at the requisite IAL, as set by agencies for a given service or transaction. Login.gov should maintain an independent assessment of its credential processes and service offerings to validate the level of assurance provided to agencies. Where

[11] See the Digital Identity Risk Management (DIRM) methodology for assurance level selection outlined in NIST SP 800-63-4, Section 3.
[12] See sample performance metrics for consideration in NIST SP 800-63-4, Section 3.5.2.
[13] See the DIRM methodology for assurance level selection outlined in NIST SP 800-63-4, Section 3.

agencies determine that supplemental anti-fraud controls are required on top of controls implemented by the Login.gov service offering, agencies should implement these controls within their respective system boundaries whenever practical, rather than rejecting Login.gov credentials outright**.**

IV. Unlocking More Integrated Experiences

Many members of the public interact with more than one public service, but interactions across services are often disjointed and repetitive. For individual services, user accounts already facilitate more customized experiences, often enabling users to set personal preferences (e.g., communication preferences), manage their personal information, and even use that information to pre-populate tasks for easier completion. Universal use of Login.gov unlocks the potential to deliver these benefits at scale, greatly reducing the number of times that users need to provide the same information across agencies and services.

Consistent with OMB Memorandum M-23-22, *Delivering a Digital-First Public Experience*, agencies should leverage data previously provided by users, where appropriate, to reduce the burden of duplicative interactions.[14] If the user consents, and consistent with applicable law, agencies should use user-provided information passed by Login.gov to agencies to populate and update an individual's account information and to pre-populate relevant forms or other tasks that can be completed within the authenticated experience. Agencies should consider privacy risks when assessing whether to pre-populate user data, particularly if users provided that data for a different purpose, and ensure incorporation of appropriate privacy safeguards.

Appendix

[14] OMB M-23-22, *Delivering a Digital First Public Experience*, Section 7.

Appendix: Actions and Deadlines

Agencies:

1. Within 60 days, report to OMB an inventory of all existing public-facing websites that have authentication. Agency Chief Information Officers will be responsible for coordinating this reporting requirement. OMB will provide subsequent reporting instructions to agencies.
2. Within 240 days, conduct a Digital Identity Risk Management (DIRM) process for public-facing digital services that have authentication and/or verification, including selection of assurance levels, consistent with the process outlined in NIST SP 800-63-4.
3. Within one year, to the extent practicable, adopt best practices from GSA's Login.gov implementation guide for existing public-facing websites that offer Login.gov.
4. Within one year, deploy Login.gov on all existing in-scope websites of OMB-designated High Impact Service Provider (HISP) services,[15] or submit a notice to OMB as described in Section I.A.[16]
    a. Within 18 months, report to OMB on the user volume and relevant performance metrics of Login.gov and any other identity solution offered on these websites.
5. Within two years, deploy Login.gov on all existing in-scope websites, or submit a notice to OMB as described in Section I.A.[17]

General Services Administration (GSA):

1. Within 90 days, and on an ongoing basis (no less frequently than quarterly), convene a cohort of agency customers to collect input on the Login.gov product.
2. Within 180 days, in coordination with OMB, publish a guide on best practices for implementing Login.gov and incorporate relevant best practices into the U.S. Web Design System.
3. Within 180 days, host an industry day to solicit information on leading commercial digital identity technologies that Login.gov could consider leveraging.
4. Within 180 days, provide a report to OMB assessing opportunities related to digital identity to further improve customer experience, such as the creation and use of verifiable digital credentials (e.g., veteran's status) and other opportunities to reduce duplicative information collection from the public.
5. Within one year, in coordination with NIST, and based on agency customers' DIRM results, explore opportunities to expand Login.gov's service offerings, such as the inheritance of credentials from commercial CSPs and ability to progressively increase identify verification based on the relative risk of specific transactions.

National Institute of Standards and Technology (NIST):

1. Within 120 days, publish a DIRM resource that helps agencies implement NIST SP 800-63- 4, *Digital Identity Guidelines.*

---

[15] The term "high impact service provider" is defined in 5 U.S.C. § 321.

[16] This action is not required of DoW or elements of the intelligence community, or with respect to any national security system.

[17] This action is not required of DoW or elements of the intelligence community, or with respect to any national security system.