Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

May 4, 2023

Login.gov: Administration and Identity Authentication

In recent years, Congress and the executive branch have worked to digitize and streamline processes where members of the public interact with the federal government. In 2015, Congress required the General Services Administration (GSA) to develop and implement a *single sign-on trusted identity platform* for individuals accessing public agency websites (6 U.S.C. §1523(b)(1)(D)). As a result, GSA partnered with the United States Digital Services, a component of the White House Office of Management and Budget (OMB), to create Login.gov.

In an August 22, 2017, announcement, GSA described Login.gov as "a single sign-on solution for government websites that will enable citizens to access public services across agencies with the same username and password." Further, Login.gov aims to allow users to "securely sign in to participating government websites and securely verify their identity." Login.gov provides shared authentication and identity verification services for multiple federal organizations and is subject to implementation guidance from OMB and the National Institute of Standards and Technology (NIST). At the end of FY2022, GSA reported that Login.gov had 41 million active users.

However, questions remain regarding the ability of Login.gov to support shared services across agencies and state and local governments, the security of Login.gov's identity authentication, and oversight of GSA's implementation of the program. The following provides an overview of the management and funding mechanisms behind Login.gov, information on OMB and NIST requirements on conducting identity proofing and digital authentication, and information on Login.gov's adoption by federal and intergovernmental programs.

Management and Funding of Login.gov

GSA's Technology Transformation Services (TTS), a component of the Federal Acquisition Service (FAS), manages Login.gov. An overarching goal of FAS is to use the federal government's purchasing power to decrease duplication across agencies. TTS focuses on how agencies procure, use, and share information technology. The operations for TTS are funded via appropriations, reimbursable work, the Acquisition Services Fund (authorized by 40 U.S.C. §321), and agency contributions to the Federal Citizen Services Fund (authorized by 40 U.S.C. §323).

Login.gov as a Shared Service

Login.gov operates as a *shared service*, which is a business function that is provided for consumption by multiple organizations within or between federal agencies. GSA states that the goal of shared services is to promote standardization, reduce costs, and increase customer satisfaction. OMB Memorandum M-16-11, *Improving Administrative Functions Through Shared Services*, created a shared services governance model for executive branch agencies and made GSA's Office of Unified Shared Services Management responsible for providing implementation direction and guidance to shared service providers.

In the case of Login.gov, GSA executed 22 interagency agreements (IAAs) between 2018 and 2021, whereby GSA provides authentication services and agencies reimburse GSA for the services rendered. IAAs provide the terms, conditions, funding, and billing information under which GSA provides Login.gov services to other federal agencies.

Technology Modernization Fund (TMF)

In addition to GSA funding and agency reimbursements, Login.gov has also received over $187 million from the Technology Modernization Fund (TMF). The TMF awards federal agencies funds for IT modernization projects. Agencies submit project proposals for the TMF board to review and consider for funding. The board has used TMF funding in the American Rescue Plan Act of 2021 (P.L. 117-2) to prioritize modernizing high priority systems, cybersecurity, public-facing digital services, and cross-government collaboration services.

Identity Proofing and Digital Authentication

For Login.gov, OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access* requires agencies to comply with NIST guidance on identity proofing and digital authentication protocols. Further, Memorandum M-19-17 directs agencies to share proofing confirmations across agencies in order to reduce public burden for having to resubmit identity data. Guidance on these topics is contained in NIST Special Publication SP 800-63-3, *Digital Identity Guidelines*. NIST explains, "Identity proofing establishes that a subject is who they claim to be. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity" (NIST SP 800-63-3, p. iv).

NIST guidance requires agencies to select the appropriate levels of identity proofing and digital authentication based on risks to the individual of unauthorized disclosure of their information. GSA, in providing Login.gov, offers agencies a product that conforms to certain NIST digital identity components. These components include an Identity Assurance Level (IAL), referring to the identity proofing process, and an Authenticator Assurance Level (AAL), referring to the authentication process.

The three different IALs and AALs have different documentation and verification requirements and therefore present different levels of individual risk and security. Login.gov initially presented partners with the option of authentication at the AAL1 or AAL2 levels and identity proofing at the IAL1 or IAL2 levels. However, a March 2023 report by the GSA inspector general (IG) disputed Login.gov's ability to provide IAL2 identity proofing, and this option has since been removed.

Understanding IALs and AALs 1 and 2

NIST SP 800-63-3, Executive Summary and Section 5.2

Identity Assurance Level (IAL) conveys the degree of confidence that the applicant's claimed identity is their real identity.

- IAL1: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are considered self-asserted.
- IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically present identity proofing.

Authenticator Assurance Level (AAL) refers to the robustness of the authentication process itself and the binding between an authenticator and a specific individual's identifier.

- AAL1: Provides some assurance that the claimant controls an authenticator registered to the subscriber and requires single-factor or multi-factor authentication.
- AAL2: Provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at this level.

At the end of FY2022, GSA reported that it had three identity vendors and government data source providers to conduct identity verifications. GSA has also launched a partnership with the U.S. Postal Service that allows some users to begin the verification process online at Login.gov and complete it in person at post offices.

Federal Agency Use of Login.gov

Examples of agencies using Login.gov include the Office of Personnel Management (USAJOBS.gov and Retirement Services Online) and the Department of Homeland Security (Trusted Traveler Programs, including TSA PreCheck, Global Entry, and SENTRI). GSA also uses Login.gov for accounts created through SAM.gov, eSRS.gov, FSRS.gov, and FPDS.gov, all of which feed into federal financial information and reporting systems.

The Internal Revenue Service (IRS) announced in February 2022 that it would transition away from ID.me, a private sector identity verification company, and begin to explore using Login.gov. While the IRS did not deploy Login.gov for filings for the 2022 tax year, it does offer Login.gov and ID.me as options for accessing certain IRS services online.

Use by State, Local, and Territorial Governments

In 2021, GSA announced that it would make its Login.gov services available to state, local, and territory governments when related to federal programs. Such services are governed by Section 302 of the Intergovernmental Cooperation Act (ICA; P.L. 90-577). Under the ICA and related OMB Circular No. A-97 guidance, a federal agency may provide technical services to these other governments if it provides similar services for its own use, it is especially equipped and authorized to perform such services, and the requesting government cannot "reasonably or expeditiously" procure such services through ordinary business channels. In September 2022, the news website FCW reported that the Arkansas Division of Workforce Services is piloting using Login.gov to verify the identities of applicants for the unemployment insurance program using grant funding from the Department of Labor.

Issues for Congress

Login.gov recently came under scrutiny in a March 7, 2023, GSA IG report and as the subject of a March 29, 2023, House Committee on Oversight and Accountability hearing. Congress may continue to consider the role and ability of the federal government to provide identity authentication more broadly.

The GSA IG report noted challenges to obtaining and properly using biometric information to comply with the more stringent requirements of higher IALs. In addition to considering the ability of federal agencies to manage in-person verification processes, Congress might assess the appropriateness of government collection of the information versus agencies partnering with private entities, such as ID.me, to supply such a service.

Congress might examine whether NIST guidelines can be uniformly enforced across agencies while also keeping pace with technology updates and public expectations of privacy and security. While NIST issues criteria for identity authentication processes, legislators may explore how agencies enforce their implementation and if their ability to monitor their progress is adequate.

For example, the GSA IG report found that despite Login.gov not meeting the NIST criteria for IAL2, GSA continued to advertise and bill for IAL2 services. Relatedly, as NIST continues to revise SP 800-63, as it most recently did in April 2023, this may affect the ability of agencies to conform to the guidance. Policymakers could consider the ability of agencies to balance administrative consistency with the need to incorporate newer technologies and techniques for identity authentication.

Regarding implementation of Login.gov, Congress may examine the ability of the service to perform adequately for agencies with large numbers of public users. For example, during a May 3, 2022, Senate Appropriations Committee hearing, the IRS commissioner testified that Login.gov could not provide the transaction processing speed the IRS needs.

Dominick A. Fiorentino, Analyst in Government Organization and Management
Natalie R. Ortiz, Analyst in Government Organization and Management
Meghan M. Stuessy, Analyst in Government Organization and Management

Disclaimer