

# GAO Highlights

Highlights of [GAO-25-107000](#), a report to congressional requesters

## Why GAO Did This Study

The risk of identity theft and fraud has been increasing, and data breaches at federal agencies and in the private sector have resulted in the compromise of millions of Americans' personally identifiable information. The sensitive information obtained in those breaches could be used by malicious actors to commit identity fraud.

GAO was asked to examine how Login.gov compares to commercial solutions. This report, among other things: (1) compares Login.gov's capabilities to selected commercially available solutions; (2) identifies reported agency spending on Login.gov and commercial solutions; and (3) evaluates the extent to which Login.gov and other selected solutions protect the sensitive data they collect and manage.

GAO reviewed the commercial solutions' capabilities and compared them with Login.gov. GAO compared how much agencies spent on commercial solutions and Login.gov. GAO also analyzed and compared Login.gov and commercial vendors' privacy practices with industry best practices.

## What GAO Recommends

GAO is making one recommendation to GSA to ensure that Login.gov demonstrates that it fully implemented the policy to test its data backups. GSA concurred with the recommendation.

For more information, contact Marisol Cruz Cain at [cruzcaim@gao.gov](mailto:cruzcaim@gao.gov).

June 2025

## IDENTITY VERIFICATION

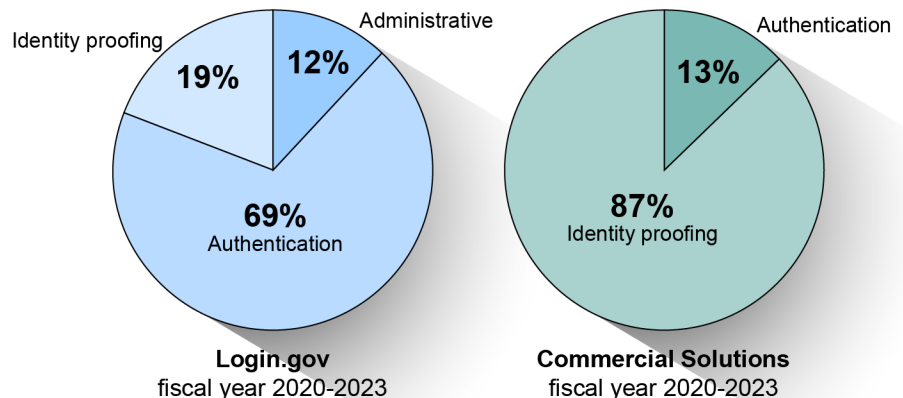
### GSA Should Demonstrate Its Implementation of Policies for Testing Data Backups on Login.gov

## What GAO Found

In 2017, the General Services Administration (GSA) launched Login.gov, which offers various capabilities. These include multi-factor authentication, identity-verification services, and fraud prevention measures. Authentication verifies the identity of a user, process, or device before allowing access to IT systems. Identity proofing verifies whether individuals are who they claim to be. However, from fiscal years 2020 to 2023, Login.gov offered fewer capabilities compared to commercial solutions (e.g. biometrics). For example, Login.gov did not provide identity proofing services in alignment with the National Institute of Standards and Technology's standards until October 2024.

Between fiscal years 2020 and 2023, federal agencies reported spending approximately \$209 million on commercial solutions while spending \$32.5 million on Login.gov.

Agencies' Login.gov and Commercial Solution Spending for Fiscal Years 2020 to 2023



Source: GAO analysis of agency documentation and Login.gov billing data. | GAO-25-107000

Note: For proprietary reasons, private vendors did not share detailed pricing information on their commercial solutions. As a result, we were not able to make a direct comparison.

Login.gov and selected commercial solutions largely implemented data protection categories in the "protect" function suggested by National Institute of Standards and Technology. Although Login.gov fully implemented four of five privacy practices, it did not fully implement policies and procedures for testing the integrity of its backup data.

According to GSA, the control was not fully implemented because Login.gov's security engineering team was not fully staffed until January 2024. At the conclusion of GAO's review, GSA reported that it had established a data protection policy; however, it has not yet demonstrated that the intended results of implementing this policy are being achieved.