GAO Highlights

IDENTITY VERIFICATION

GSA Needs to Address Fraud Threats and Technical Issues

GAO-26-109261 July 15, 2026

A testimony before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives

Contact: Marisol Cruz Cain at CruzCainM@gao.gov

What GAO Found

The proliferation of cyberattacks on federal agencies and other organizations has led to an increased risk of stolen personally identifiable information (PII) being used to commit fraud. For example, malicious actors have used the information to fraudulently obtain government benefits and commit tax fraud, among other things. The Social Security Administration has reported that personal information of beneficiaries has been used to fraudulently redirect the beneficiary's direct deposit benefits. Stolen PII also increases risks for financial fraud, such as fraudulent credit card applications. In this type of fraud, thieves use identifying data, such as Social Security numbers and driver's license numbers, to open new financial accounts without a person's knowledge. These types of attacks can result in financial loss and damage to the reputation of federal agencies and financial institutions.

To ensure that individuals accessing government services, benefits, and other resources are the individuals they claim to be, federal agencies use a variety of identity verification processes. To suppport these efforts, the General Services Administration (GSA) established Login.gov as a government-wide identity verification service. Login.gov uses a non-biometric, three-step process to verify an individual's identity. In addition, to protect users' PII, Login.gov uses security measures such as encryption, access restrictions, and monitoring capabilities.

GAO previously reported challenges in GSA's implementation of Login.gov. These challenges involved:

- ensuring that Login.gov data was backed up regularly to prevent data loss,
- aligning Login.gov with federal digital identity guidelines to provide an appropriate level of assurance when verifying users' identities,
- resolving technical challenges reported by agencies using Login.gov, and
- documenting and applying lessons learned from its Login.gov pilot programs.

To address these challenges, GAO made several recommendations in 2024 and 2025 to GSA. Since then, the agency has taken steps to implement all but one of these recommendations. For example, GSA took steps to ensure that Login.gov offers remote identity-proofing services that comply with federal digital identity guidelines. In addition, the agency provided evidence that it had begun testing processes for backing up Login.gov data. However, GSA still needs to take action to fully address one of GAO's recommendations. Specifically, GSA has not established time frames with its partners for addressing agency-reported technical challenges. Without GSA-proposed actions and time frames for addressing the challenges, agencies will continue to experience technical issues with the system.

Protecting PII and preventing identity theft is critical, as the harms can range from lost funds to emotional distress and damage to the reputation of federal agencies. Fully implementing GAO's remaining recommendation would help the federal government ensure PII is better protected and lessen the risk of identity theft. GAO will continue to monitor GSA's efforts to address the recommendation.

Why GAO Did This Study

The vast amount of PII that federal agencies collect from individuals to verify their identity may be vulnerable to breaches, which can result in identity theft, fraud, and other harms. Accordingly, it is critical that federal agencies implement effective ways to verify the identity of individuals who access government websites to prevent fraud and protect PII.

To address this issue, GSA launched Login.gov in 2017 to provide federal agencies with a single sign-on system to verify the identity of individuals seeking access to government websites. In 2021, GSA allocated about $187 million in technology modernization funds to enhance Login.gov's services, including strengthening its security and anti-fraud protections and improving ease of agency adoption.

This statement discusses (1) identity-related fraud threats and (2) Login.gov capabilities and the status of GSA efforts to address prior related GAO recommendations.

This statement is based primarily on GAO's October 2024 (GAO-25-106640) and June 2025 (GAO-25-107000) reports on Login.gov's identity proofing processes. This statement also includes updated information provided by GSA on efforts to address GAO's recommendations.