

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074  
MINORITY (202) 225-5051

<https://oversight.house.gov>

### Ranking Member Kweisi Mfume

#### Subcommittee on Government Operations and the Federal Workforce

#### Hearing on “Login.gov Doesn't Meet the Standard”

#### March 29, 2023

Thank you, Chair Sessions.

**Today, we convene an important hearing to discuss a topic that impacts millions of Americans who have engaged with the federal government’s secure online sign in service: Login.gov.**

**If you’ve received unemployment benefits through the Paycheck Protection Program, received a disaster loan from the Small Business Administration, or applied for a job through USAJOBS— you’ve used Login.gov to securely sign in and access the much-needed government services.**

**Americans trust Login.gov with their sensitive information, and the federal government relies on Login.gov to help root out potential fraudsters hoping to siphon money away from essential government programs. Today, unfortunately, we must reconcile with certain failures that have come to light.**

Just a few weeks ago, the General Services Administration Office of Inspector General released an alarming report that details how the General Services Administration—or GSA—misled customers on Login.gov’s compliance with the identity proofing standards that the National Institute of Standards and Technology (NIST) issued back in 2017.

Federal agencies must ensure that their identity proofing and authenticating services meet NIST standards.

For government services that may have a higher risk of fraud, agencies may require the service provider to meet higher identity proofing standards—for example, they may require more than a username and password. In these cases, individuals may need to prove who they say they are by visiting a federal facility in-person or by providing biometric data, like a “selfie” in an online environment.

Login.gov operates a high level of identity proofing—but it was not at the IAL2 standard, which requires biometric data. Login.gov failed to offer either an in-person or remote identity proofing option. Yet, GSA started to bill its customers, comprised of roughly 22 agencies, for non-compliant services for as many as two years.

The Report found that multiple key personnel informed the Login.gov team of its noncompliance with NIST’s IAL2 standards as early as January 2020, a few months after Login.gov began billing its customers.

That was not the last time Login.gov was informed of its non-compliance—and yet continued to mislead certain customers. It happened again in 2020, when a GSA consultant informed senior Login.gov staff of its lack of an IAL2 component.

But it was not until June 2021 that a senior official at GSA announced internally that GSA would cease its efforts to meet biometric requirements because of equity concerns. What is important to highlight here is that Login.gov has never met the IAL2 standard. It did not meet the standard then and it does not meet it today.

And still, Login.gov continued to mislead customer agencies about its lack of biometric comparison capabilities until January 2022, when the agency released its Equity Action Plan.

Finally, at the end of our five-year timeline, GSA notified customer agencies that the services they were paying for did not comply with NIST requirements published back in 2017.

**What the report does not show—and what is just as important to this conversation—are the decisive and immediate actions taken by GSA leadership when they were finally made aware of Login.gov’s shortfalls.**

**In February 2022, GSA leadership removed the Director of Login.gov and instituted a temporary Director. GSA then initiated a formal management inquiry to investigate the misrepresentations.**

**In March 2022, GSA leadership referred this matter to the Inspector General to undertake a nonpartisan and impartial review of the matter. It is rare for an agency actually to unilaterally request an Inspector General review, and I commend GSA for taking this important step.**

GSA leadership also created a new Technology Law Division to specialize in technology-focused legal services. This action is one that we should be looking to replicate across all federal agencies in the future to ensure there is adequate understanding of the technology that is deployed. I hope we can explore that today.

And lastly in October 2022, GSA leadership directed Login.gov to undertake a top-to-bottom review of the program. I look forward to hearing an update on the progress of this review.

Thank you to our witnesses, Commissioner Sonny Hashmi, Inspector General Carol F. Ochoa, and Acting Director Jim St. Pierre for testifying before us today and for their commitment to a more secure government.

Thank you, Chair Sessions. I yield back.

###