Statement of

The Honorable Carol Fortine Ochoa

Inspector General

U.S. General Services Administration

before the

U.S. House of Representatives

Committee on Oversight and Government Reform

Subcommittee on Government Operations and the Federal Workforce

concerning

The Technical and Operational Capabilities of Login.gov

March 29, 2023

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee:

Thank you for the opportunity to testify here today regarding the Office of Inspector General's (OIG) report issued earlier this month titled, *GSA Misled Customers on Login.gov's Compliance with Digital Identity Standards*.

Inspectors general across the U.S. Government exist within federal Executive Branch agencies as independent and objective units to conduct audits, investigations, and evaluations to promote economy, efficiency, and effectiveness and to prevent and detect waste, fraud, abuse, and mismanagement in government programs. We provide our findings and recommendations to the agencies where we are located and directly to Congress and the American public. My office performs this function inside the General Services Administration (GSA).

Initiation of OIG Evaluation

Our evaluation of this topic began in April of last year when we received a notification from the GSA's General Counsel identifying potential misconduct within the Login.gov program office. Organizationally, Login.gov is a component of GSA's Technology Transformation Services (TTS), which is part of the Federal Acquisition Service (FAS).

Background

Federal cybersecurity requirements obligate the GSA Administrator, in collaboration with the Secretary of Homeland Security, to develop a single sign-on trusted identity platform that federal agencies must implement for individuals accessing federal websites that require user authentication.

In 2016, the GSA Technology Transformation Service's 18F division initiated a project to build a multi-factor authentication login platform that would generate a single account for users interacting with the federal government online. In April 2017, GSA launched 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."

A few months after the launch, in June 2017, the National Institute of Standards and Technology (NIST) issued guidelines setting the standards and baseline requirements for digital identity services, and addressing risks associated with authentication and identify proofing errors. NIST updated the guidelines in March 2020.

NIST's Digital Identity Guidelines (Special Publication 800-63-3 et al.) provide technical requirements and guidance for identity proofing and authentication of users interacting with government information technology systems, such as Login.gov, over open networks. According to NIST:

> 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.

Implementation of the guidelines requires a two-component risk-based process – Identity Assurance Level (IAL) (identity proofing) and Authenticator Assurance Level (AAL) (authentication). For identity verification, the goal is to confirm and establish a link between the claimed identity and the real-life existence of the subject presenting the evidence.

The guidelines list three Identity Assurance Levels (IALs) which agencies may select from based on their risk profile and the potential harm caused by an attacker making a successful false claim of an identity. Importantly, identity verification at the second level, or IAL2, requires either a physical comparison to a photograph on the strongest piece of evidence provided, or a biometric comparison to the strongest piece of evidence provided. A biometric comparison measures both physical characteristics, such as a facial image (also referred to as a selfie), iris recognition, or fingerprints, and behavioral characteristics, such as typing cadence.

When identity verification is performed remotely and does not include a remote physical comparison, as in the case of Login.gov, the identity confirmation must also include a biometric comparison. Therefore, to achieve IAL2 in the Login.gov environment, there must always be a biometric comparison.

In May 2019, the Office of Management and Budget issued a memorandum requiring federal agencies to implement NIST digital identity guidelines. That OMB memo also required federal agencies to use shared services, such as those offered by GSA, to the extent available, to deliver these identity assurance and authentication services to the public.

OIG Findings

From September 2018 to January 2022, GSA executed interagency agreements with other federal government agencies to provide them with the OMB-mandated shared services. GSA claimed in those agreements that Login.gov met or was consistent with NIST digital identity requirements for identity proofing at the IAL2 level.

Despite these assertions, Login.gov has never met the technical requirements for identity proofing and authentication at NIST's IAL2 level, which include either a physical comparison or biometric comparison for identity verification.

At multiple points over the past three years, senior leaders in TTS and Login.gov learned that Login.gov did not comply with IAL2 requirements. They did not, however, notify customer agencies of the noncompliance.

On June 24, 2021, the TTS Director announced internally that TTS would suspend efforts to meet the biometric comparison requirement of the NIST standard, citing concerns about the discriminatory impact of facial recognition technology. However, TTS did not notify customer agencies when it made this decision.

Instead, GSA continued to mislead and withhold information from customer agencies about Login.gov's lack of biometric comparison capabilities until February 3, 2022. On that date, 7 months after its internal announcement to suspend efforts to meet the biometric requirement, GSA finally notified customer agencies that the IAL2 service included in their interagency agreements, for which they were paying, did not comply with NIST requirements.

Although GSA had never met the NIST standards, the February 3, 2022, notification to customer agencies cited the decision not to use facial recognition technology as the basis for Login.gov's failure to meet the NIST standards. This led customer agencies to believe that GSA's decision to not use facial recognition technology due to equity concerns was the basis for Login.gov's noncompliance with IAL2 requirements, and that Login.gov had been compliant prior to that decision. The notification did not reveal that Login.gov had never complied with NIST IAL2 digital identity standards, and that the noncompliance began long before GSA announced an equity-based rationale for the decision not to deploy facial recognition.

Starting in 2019, Login.gov began charging customer agencies for IAL2 services that did not meet the NIST digital identity requirements. GSA knowingly billed 22 customer agencies more than $10 million for services, including alleged IAL2 services that did not meet IAL2 standards. Even after notifying customer agencies in February 2022 that their services were not compliant with NIST IAL2 standards, Login.gov continued to bill agency customers for IAL2 services.

Further, GSA made inaccurate statements about Login.gov's compliance with IAL2 to the Technology Modernization Board in securing funding for Login.gov. The board, which includes GSA, provides awards from the Technology Modernization Fund (TMF) to agencies to help them improve, retire, or replace existing systems. In its September 2021 proposal seeking TMF funding for use on Login.gov, GSA stated:

> Login.gov is currently used in production and complies with NIST's …standard for … identity verification (IAL2).

The Board awarded just over $187 million from the fund to GSA for Login.gov.

More than 4 months later, on February 7, 2022, the GSA Deputy Administrator notified the Technology Modernization Board that Login.gov's TMF proposal made statements "that could be interpreted to say Login.gov's service meets NIST guidelines for identity verification." In fact, Login.gov identity proofing services did not meet the IAL2 standard at that time and, as quoted above, GSA's funding application expressly stated unequivocally that Login.gov "complies with NIST's standard" for IAL2.

GSA's FAS exercised inadequate oversight and management controls over Login.gov's day-to-day operations, and thus bears responsibility for these derelictions by Login.gov and its parent organization, the TTS.

The FAS Commissioner acknowledged that TTS's failure is rooted in its historic, ongoing culture that considered oversight burdensome. Previously, in 2016 and 2017, the OIG issued two reports finding significant deficiencies in the management and oversight of 18F, the office within TTS where Login.gov originated.

Despite GSA's assurances to fix these deficiencies, FAS allowed TTS's culture to continue unchecked. The former TTS Director told us the Login.gov team retained significant autonomy, and a culture in which teams believed they did not need to escalate decisions to leadership or that escalating was worthwhile. As one person working in Login.gov told us, "no one was at the wheel" for IAL2 decisions, enforcement, responsibility and accountability. There also were no clear policies, management controls, or checks and balances for Login.gov.

The Federal Acquisition Service's failure to establish management controls empowered Login.gov to mislead customer agencies. FAS bears ultimate responsibility for any consequent harm to TTS's credibility with federal customer agencies.

To address these findings, our report included a set of five recommendations.

OIG Recommendations

We recommended that FAS:

- Establish adequate management controls over TTS;
- Ensure adequate documentation of policies, decisions, procedures, and essential transactions involving TTS programs, including Login.gov, and records management in accordance with GSA standards;
- Implement a comprehensive review of Login.gov billings for IAL2 services;
- Establish a system for internal reviews of TTS programs to ensure that they comply with relevant standards; and
- Adopt a policy to clearly notify each customer agency seeking identity and authorization assurance services whether Login.gov meets all

applicable NIST published standards and the services specified in the interagency agreements.

GSA agreed with our recommendations and offered comments in a reply memo which we appended to our report.

Conclusion

This concludes my overview to the committee regarding our report on the misleading actions by government officials inside GSA's Login.gov office. I appreciate the opportunity to appear before the Committee today.