STATEMENT OF SONNY HASHMI, COMMISSIONER
FEDERAL ACQUISITION SERVICE
U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE SUBCOMMITTEE ON GOVERNMENT OPERATIONS AND THE FEDERAL WORKFORCE
OF THE
HOUSE COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
HEARING ON
"LOGIN.GOV DOESN'T MEET THE STANDARD"

March 29, 2023
2:00PM

Good afternoon, Chairman Sessions, Ranking Member Mfume, and members of the committee. Thank you for the opportunity to come before you to discuss the Login.gov program, a part of the U.S. General Services Administration's Technology Transformation Services, or TTS, a component of the Federal Acquisition Service (FAS). My name is Sonny Hashmi and I am the Commissioner of FAS. I am honored to testify before you alongside my colleagues from the National Institute of Standards and Technology (NIST) and the Inspector General (IG) at GSA.

I want to thank the Office of Inspector General (OIG) for their evaluation and thorough review of the matter at hand, based on a referral by GSA leadership in early 2022. I am committed to fully implementing all of the OIG's recommendations, and believe they reinforce and strengthen the corrective actions we have already taken since February 2022. Since its referral to the Inspector General, GSA has worked to improve and strengthen the management of the Login.gov program; it has also enhanced the service Login.gov provides, investing in an array of new security and anti-fraud practices used throughout industry and the financial sector.

Earning and maintaining the American people's trust through transparent and accountable actions is fundamental to the delivery of GSA's mission. That is why once we found out that Login.gov was out of compliance with a certain NIST identity assurance level that the program claimed to meet, our leadership immediately launched an internal review that uncovered that certain Login.gov employees may have knowingly misrepresented the program's capabilities to clients for years. GSA leadership then immediately took those internal findings to the OIG for further investigation. GSA also initiated disciplinary proceedings—and all those who we are aware of who knowingly misrepresented features of Login.gov are no longer employed by GSA. Again, I and the rest of GSA leadership have taken the misrepresentations made by members of TTS seriously, have taken a number of steps to improve our internal controls and strengthen the program, and are committed to fully implementing the IG's recommendations. However, before I dive into that further, I'd like to provide some background to the Committee about the Login.gov program and why a service like this is needed.

What Login.gov is and Why it is Important

Identity management is critical to the Federal government's successful delivery of mission and business promises to the American public and to preventing fraud. This has been a core competency of public institutions for much of the country's history, and this is still true in the digital age. Whether renewing a passport or applying for veterans benefits, Americans should be able to access government-provided digital services in the same way a physical government-issued ID allows for a member of the public to access government services in-person. They should also feel confident that their identity is not being fraudulently used. The need for this kind of government digital identity verification continues to grow, as more Americans expect to be able to simply and securely access services online.

Through Login.gov, GSA is working to develop a secure, scalable, trusted, and accessible authentication and identity verification solution that reduces burden and risk for our agency partners, and that helps the American people access the government services they need in a seamless and secure manner while promoting access, protecting privacy, and preventing fraud. As a shared service that agencies can use to provide simple and secure access, Login.gov not only benefits the public by providing a single account to access a range of government services, it also reduces duplication by providing a government-wide service rather than requiring each agency to develop and maintain separate systems.

In doing so, Login.gov focuses on:

- **Ensuring fairness and transparency in government service delivery:** Identity verification is the gateway to many government services and benefits, and it must work for all Americans. A government-managed option for identity verification ensures that people can access government services through a service that is subject to public oversight and accountability and has a strong obligation to ensure fair access to public services.
- **Making it simpler and more secure to work with the government:** The vast disparity in access to facilities and technologies can make it challenging for

citizens to get the support they need, and challenging for agencies to reach everyone that may be eligible. Login.gov helps address this by allowing the public to use a single secure digital account to access a multitude of services, while incorporating protections against cyber threats and fraud.

- **Protecting people's information**: The public should trust that the personal information they provide to the government is being protected and is not being leveraged by others for private gain. Login.gov will never be sold, nor will user data be leveraged for other uses not related to identity verification or fraud mitigation. In fact, Login.gov's unique encryption model ensures that users – not corporations - control access to their own sensitive information.
- **Leveraging market-leading capabilities and preventing fraud:** In developing a shared service, a government-wide approach creates the opportunity to establish high and consistent security practices across agencies versus each agency providing this service in their own way, which may not include the best tools or practices. This is critical because, in recent years and as reported by GAO and other auditing organizations, identity fraud perpetrated by criminal fraud syndicates has cost taxpayers billions of dollars. Creating a robust digital identity verification and authentication service is fundamental to preventing those threats. If the government wants to establish new standards or new protections, or adopt new market-leading capabilities, there is a benefit in one service where new capabilities can be integrated and immediately proliferate across a wide range of critical government activities.
- **Creating efficiencies and avoiding duplication:** Agencies have an obligation to be good stewards. For each agency that leverages Login.gov, the federal government avoids duplicative costs of having to build, procure, secure, and/or maintain a digital identity service. The more agencies that adopt a shared service, like Login.gov, the fewer agencies that need to develop their own identity authentication and verification solution.

For all these reasons and more, we believe the United States needs a publicly provided shared service for digital identity.

GSA's Actions to Date and Moving Forward

In early 2022, GSA leadership first learned that, although Login.gov represented that it met a specific identity verification standard, it did not actually comply with that standard. Before I discuss the details of the issue, I want to provide some baseline information about the standard.

NIST has three Identity Assurance Level standards, ranging from IAL1 to IAL3, which seek to reflect the degree of confidence that “This person is who they say they are.” Each assurance level encompasses a detailed set of specifications with a progressively more rigorous set of criteria. Each agency evaluates its specific mission needs and balances the need for assurance with the need to provide seamless access to their constituents. For example, agencies could determine that the level of scrutiny required to apply for a fishing license or visit a national park should be different than that required to receive a US passport.

Login.gov was not compliant with the IAL2 level of assurance. Unfortunately, the problem went beyond one of noncompliance and into knowing misrepresentation. Specifically, GSA leadership learned there was a significant possibility that certain individuals within the Login.gov program, despite knowing that the product did not meet IAL2, misinformed customers by claiming that the product did, in fact, comply with IAL2. This misrepresentation included false statements in interagency agreements dating back to 2020 and, as the IG’s findings indicate, the issue went back even further - to at least 2018.

Once senior leadership became aware, we immediately took action by: 1) putting in place new leadership and launching an employee discipline inquiry; 2) implementing structural reforms to ensure greater compliance and internal controls within Login.gov; and 3) ensuring greater transparency with Login.gov partners.

With respect to personnel, in February 2022, the Director of the Login.gov program was removed from their role and a temporary Login.gov Director was put into place. A new permanent replacement was named in September. Additionally, after an internal review concluded that some GSA employees likely engaged in knowing misrepresentations regarding NIST standards, a GSA senior career executive was named to initiate an employee discipline inquiry and recommend discipline as appropriate. Today, all those we are aware of who knowingly misrepresented features of Login.gov are no longer employed by GSA.

GSA leadership also strengthened accountability and oversight practices within Login.gov and throughout TTS. In March 2022, GSA created a new Technology Law Division within the Office of the General Counsel, to provide specialized legal services to GSA’s technology-focused components, with an emphasis on ensuring compliance. GSA also started bringing TTS more into line with FAS’s overall management controls environment. For the Login.gov program, in June 2022, GSA created an executive steering committee to provide oversight for the program. Once a permanent Login.gov director was in place, I directed him to conduct a top-to-bottom review of the program to include a compliance roadmap, customer communications, internal controls environment, financial operations, human resources, and contracts review.

Finally, given prior misrepresentations, GSA leadership directed the Login.gov team to proactively communicate with partners. In February 2022, based on the information that was known at that time, GSA notified customers, the Technology Modernization Fund (TMF) Board, and GSA's Inspector General of Login.gov's non-compliance with IAL2 standards. GSA also began to execute revised customer agreements to accurately represent its status with respect to IAL2 compliance, and ensured that all new agreements were accurate. After the new permanent director was on board, GSA provided an extensive update on Login.gov's compliance status and product roadmap to customers, which was also shared with other stakeholders, including those in Congress.

Login.gov Provides Robust, and Continually Improving, Identity Authentication and Verification Services

While the IG report raises significant concerns with past *management* of the Login.gov program and management of TTS, it is important to recognize the strength of the existing Login.gov *service*. Login.gov has a robust suite of security features to prevent fraud, like mandatory multi-factor authentication, phone and address verification, and state-issued ID validation, and we continue to add more features targeting bad actors, bots, and more. Additionally, Login.gov has a strong encryption model to protect privacy, ensuring that users – not corporations – control access to their own information. And Login.gov is FedRAMP authorized, meaning that extensive controls are in place that are independently audited to ensure the system is secure from cybersecurity threats.

In addition, GSA has expanded its options for secure identity verification. GSA is now piloting a service in partnership with the U.S. Postal Service to allow certain users to complete their identity verification process in person at one of 18,000 locations around the country - about 95 percent of the public lives within 10 miles of a USPS location that partners with Login.gov. This offers a secure option for people who choose to verify their identity in person. GSA has further scaled up Login.gov's contact center capacity to provide 24/7 customer support, so that constituents can get help with the identity verification process from home at any time.

Together, these initiatives enable Login.gov to be a leading identity verification provider for the American public. GSA will continue to invest in anti-fraud protections, work with our federal partners to investigate identity theft, and expand secure access to government services.

Conclusion

GSA remains firm in its belief that the public deserves a secure identity verification option that prioritizes serving all Americans, while safeguarding their privacy and preventing fraud. We believe that the actions taken so far as a result of our internal reviews - along with fully implementing the recommendations made by the OIG and taking further steps coming out of the top-to-bottom review - will keep us on the path to deliver a more effective identity authentication and verification public option for the government into the future.

As we move forward, we are committed to being honest and transparent with our stakeholders, including our customer agencies, the Congress, and the public, on our efforts to improve Login.gov. We will continue to take all actions necessary to strengthen the management of the program and ensure that Login.gov delivers for our customers and for the public.

Thank you for your time. I look forward to your questions.