

**Statement of Congressman Gerald E. Connolly (VA-11)**  
**Committee on Oversight and Government Accountability**  
***Login.gov Doesn't Meet the Standard***  
**Wednesday, March 29, 2023**

I condemn misrepresentations by General Service Administration (GSA) officials about Login.gov's compliance with NIST digital identity guidelines. There must be accountability for these wrongful actions, but we cannot throw the baby out with the bathwater. As top Democrat of the Cybersecurity, Information Technology, and Government Innovation Subcommittee, I understand the value proposition of Login.gov as a critical tool to cut fraud in federal programs, cut costs to taxpayers, and improve customer experience for government services.

Login.gov is a well-intended effort to improve government services. As government agencies move their processes and operations to digital channels, the shared service provides a consistent, easy to use and secure platform where people can authenticate and verify their digital identity across Federal, State, and local entities. To date, Login.gov has served 60 million users, and supports vital government services across more than 30 agencies that include veteran health care, unemployment benefits, and social security services.

Unfortunately, a recent GSA Office of the Inspector General (OIG) Report found Login.gov's compliance with National Institute of Standards and Technology's (NIST) Identity Assurance Level 2 (IAL 2) standard was continually misrepresented by GSA officials as far back as 2019. IAL 2 requires identity proofing, for example a person can provide a passport or driver's license number as evidence they are the owner of the identity they are claiming. The report further uncovered the primary reason for continued non-compliance was based on the decision not to implement facial recognition/biometric verification, due to significant and persistent concerns regarding equity and access. While equity and access should be embedded within every service delivery program, these misleading actions by GSA officials are reprehensible because they erode trust between the federal government and the people it serves. Public trust is a critical cornerstone of our democratic republic, so let's work together to earn back the people's trust.

To right this wrong, Congress must ensure Login.gov meets necessary digital identity proofing standards and that federal agencies, more generally, are better equipped to procure technology needed for digital identity verification. I welcome the actions by GSA leadership once they learned about Login.gov's noncompliance and misrepresentation of the service in January 2022. These strong, consequential decisions include referring the matter to the OIG and removing the Login.gov Director. I also support the structural reforms, which include the creation of a new Technology Law Division within the Office of General Counsel; directing the new Login.gov Director to conduct a top-to-bottom review of the program; and enforcing greater transparency with Login.gov's federal partners. Finally, I am eager for the continued oversight over these past initiatives including GSA's plan to audit Login.gov for future compliance with necessary NIST standards.

I am an unapologetic champion of the potential for IT to improve federal customer experience and deliver services to taxpayers. We have made a significant investment in Login.gov to do just that, but in this case the program is coming up short of our expectations for transparency and service delivery. This subcommittee must ensure these issues are addressed

immediately and that the original purpose of the program, to streamline access to government services, is realized.