IDENTITY VERIFICATION
GSA Needs to Address Fraud Threats and Technical Issues

Statement of Marisol Cruz Cain, Director,
Information Technology and Cybersecurity

Testimony Before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery Expected at 2:00 p.m. ET

Wednesday, July 15, 2026

GAO-26-109261

United States Government Accountability Office

Accessible Version

GAO Highlights

IDENTITY VERIFICATION
GSA Needs to Address Fraud Threats and Technical Issues

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

GAO-26-109261

July 15, 2026
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 Adiministration (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.

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

I appreciate the opportunity to be here today to discuss our reports on federal efforts to improve identity verification and address related fraud threats. Data breaches at federal agencies, as well as in the private sector, have compromised millions of Americans' personally identifiable information (PII).[1] Given the significant role that stolen PII played in the large-scale identity fraud of pandemic programs, we have urged agencies to assume identity information has been compromised and develop and apply upfront verification controls.

Federal agencies use PII to verify the identity of individuals who access benefits and accounts on government websites. The increase in cyberattacks on these agencies and other organizations has led to a greater risk of stolen PII being used to commit fraud. For example, malicious actors have used PII to fraudulently obtain government benefits and commit tax- or wage-related fraud. Stolen PII also increases risks for financial fraud, including account takeovers and fraudulent credit card applications. These attacks can harm citizens, result in financial loss, and damage the reputation of federal agencies and financial institutions.

To address these issues, the General Services Administration (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. Login.gov uses a non-biometric three-step identity proofing process that results in the verification of an individual's identity, using guidelines established by the National Institute of Standards and Technology (NIST).[2] In addition, to protect users' PII, Login.gov uses security measures such as encryption, access restrictions, and monitoring capabilities. 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.

As we previously reported, Login.gov began providing identity proofing services in alignment with NIST Digital Identity Guidelines in October 2024.[3] Verification of a user's physical or biometric attributes, whether done in-person or remotely, is one of the NIST requirements for higher assurance that the user is who they claim to be. However, in May 2025, GSA issued a contract modification for Login.gov that indicated the program's Anti-

[1]Personally identifiable information is information that can be used to locate or identify an individual, such as names, aliases, Social Security numbers, biometric records, and other personal information that is linked or linkable to an individual.

[2]National Institute of Standards and Technology, *Digital Identity Guidelines*, Special Publication 800-63-4; and *Digital Identity Guidelines: Identity Proofing and Enrollment*, Special Publication 800-63A-4 (July 2025).

[3]GAO, *Identity Verification: GSA Needs to Address NIST Guidance, Technical Issues, and Lessons Learned,* GAO-25-106640 (Washington, D.C.: Oct. 16, 2024).

Fraud Team determined that fraudulent accounts passed the identity proofing services and that the sophistication of the attempts would increase exponentially in the future.[4]

My statement today will discuss findings from our prior reports on (1) identity-related fraud threats and (2) Login.gov capabilities and the progress GSA has made to implement our prior recommendations.

My statement is based primarily on reports we issued in October 2024 and June 2025, as well as our additional related work since 2019. These reports are listed on the related GAO Products page at the conclusion of this statement. To update the status of prior recommendations we made in those reports, we reviewed GSA documentation, including data backup testing reports, Login.gov's program roadmap, and lessons learned reports. More detailed information on the objectives, scope, and methodology of our prior work can be found within the specific reports on which this statement is based.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal agencies are responsible for ensuring that individuals are properly vetted before they access government services, benefits, and other resources. A key part of this process is verifying that the person who is attempting to interact for the first time with a federal agency is the individual they claim to be. This process is known as identity proofing.

Identity proofing may occur in-person or through a remote online process. In the case of in-person identity proofing, a trained professional verifies an individual's identity by making a direct physical comparison of the individual's physical features and other evidence (such as a driver's license) with official records. Verification of these credentials can be performed by checking electronic records in tandem with physical inspection.

Overview of the Remote Identity-Proofing Process

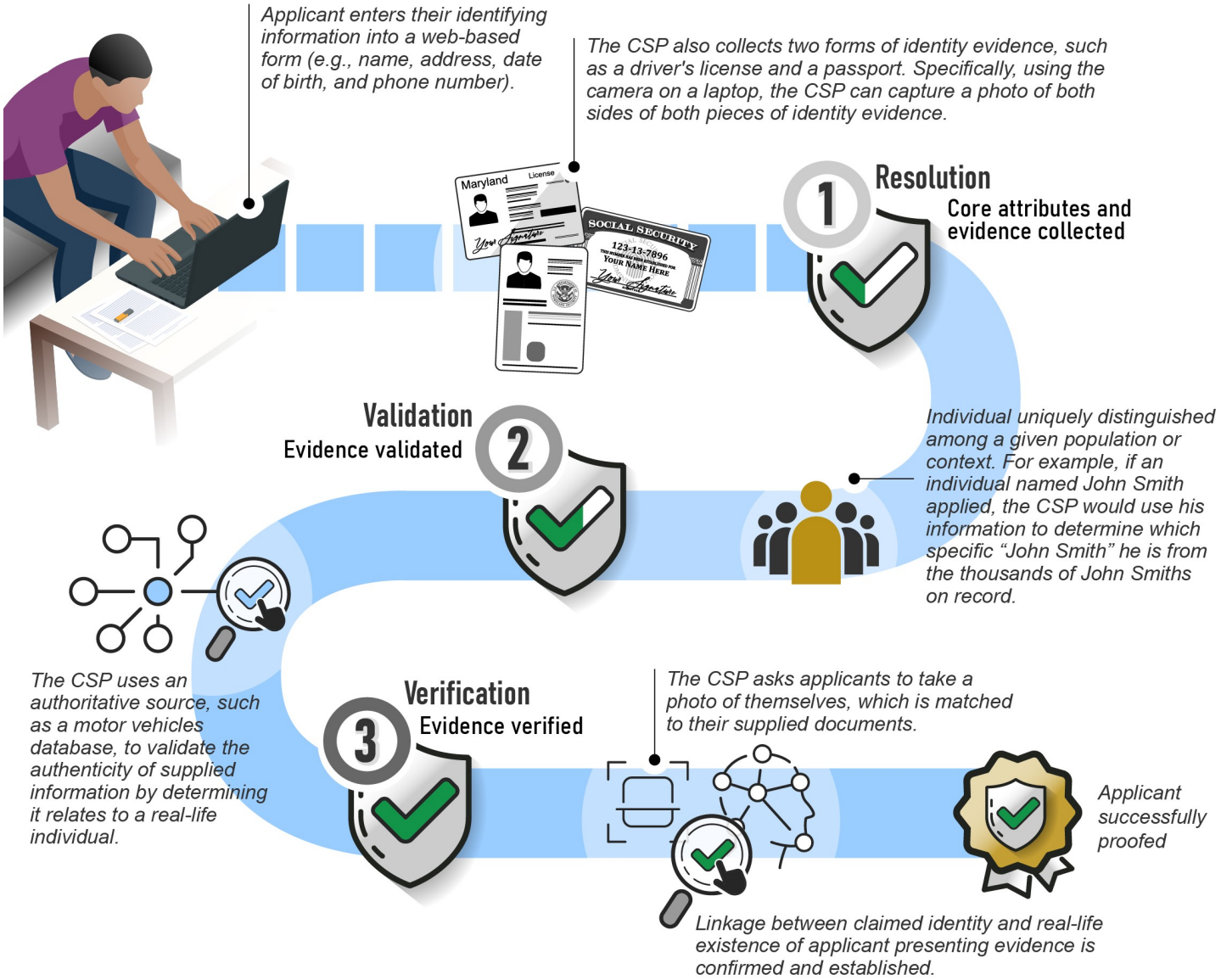
Remote identity proofing is the process of conducting identity proofing entirely through an online exchange of information. When remote identity proofing is used, the individual provides the information electronically or completes additional electronically verifiable actions to confirm their identity (e.g., transmitting selfies,[5] verification through virtual meeting, etc.). Since many federal benefits and services are offered broadly to large numbers of geographically dispersed individuals, agencies often rely on remote identity proofing to verify the identities of individuals. Remote identity proofing is also the process through which a credential service

[4]General Services Administration, "Contract Change to Login.gov's Identity Verification Solution for Functional Area 1-Document Capture, Authentication and Validation," Sam.gov (May 21, 2025), https://sam.gov/opp/8631751bf4a543b39d18471795fc7442/view.

[5]A "selfie" is a photograph one takes of oneself.

provider (CSP)—a trusted entity that issues electronic credentials to subscribers—collects and verifies information about an individual for the purpose of issuing credentials to that person, as illustrated in figure 1.[6]

Figure 1: Overview of the Remote Identity Proofing Process by Credential Service Providers (CSP)



Sources: GAO (license illustrations and analysis of National Institute of Standards and Technology information); Golden Sikorka/stock.adobe.com (person); stas111/stock.adobe.com (icons). | GAO-26-109261

Remote identity proofing involves three major steps: (1) resolution, (2) validation, and (3) verification.

[6]A credential service provider may be an independent third party or issue credentials for its own use.

- **Resolution:** The identity resolution process begins by having the applicant provide identifying information, typically through a web-based application form. Examples of information that an agency may collect for identity resolution include name, address, date of birth (DOB), and Social Security number (SSN). The CSP may also collect information from the applicant's driver's license or passport by having the applicant use a camera to capture screenshots of both sides of the document. The CSP then electronically compares the applicant's identifying information with electronic records maintained by an authoritative source, such as a state's department of motor vehicles, to determine (or "resolve") which identity is being claimed. For example, if an individual named John Smith applied, the CSP would use his identifying information to determine which specific "John Smith" he is from among the thousands of John Smiths that may be documented in the records of the authoritative source being used for this process.
- **Validation:** During this step, the agency electronically submits the information that the applicant provided to the CSP for validation. The validation process confirms that the evidence submitted is genuine and that the information is valid, current, and represents a real identity. Specifically, the CSP checks the image on the license and/or passport to determine that there are no alterations and that the identification numbers follow standard formats, among other things.
- **Verification:** In this step, actions are taken to verify whether the applicant is really who they claim to be. For example, in the case of John Smith, it is not enough simply to determine which "John Smith" is being claimed, because the applicant may not really be "John Smith" at all. During the verification, the CSP asks the applicant to take a photo of themself to match to the license and/or passport picture provided during the resolution step. Once the CSP matches the picture(s) on the license and/or passport to the applicant's picture and determines that the pictures match, an enrollment code is sent to the validated phone number of the applicant. The applicant provides the enrollment code to the CSP, and a match is confirmed, which verifies applicants are in possession and control of the validated phone number. After the applicant goes through these steps, they have been successfully proofed and the applicant is able to log into federal agencies' websites and applications to access their information or apply for federal services.

Federal Legislation and Guidance on Data Protection and Identity Proofing

Federal laws and guidance specify requirements for federal agencies to protect systems and data, including systems used or operated by a contractor or other organization on behalf of a federal agency.

- The Privacy Act of 1974 establishes agency responsibilities and protections for personal information accessed or held by federal agencies. For example, the Privacy Act places limitations on the collection, disclosure, dissemination, and use of personal information maintained in "systems of records," or groups of records under the control of any agency from which information is retrieved by individual name or identifier, such as those used to verify identification.[7]
- The Office of Management and Budget has published a zero-trust strategy that requires agencies to adopt specific cybersecurity standards and objectives that are intended to form a starting point to implementing

[7]5 U.S.C. § 552a. According to the Privacy Act, a ''record'' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, their education, financial transactions, medical history, and criminal or employment history and that contains their name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. A ''system of records'' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

zero trust architecture.[8] The strategy's requirements include integrating and enforcing multifactor authentication across applications involving authenticated access to systems by agency, staff, and partners.

- NIST's privacy framework provides guidance to agencies on the selection and implementation of information security and privacy controls for systems.[9] Within the framework, functions organize foundational privacy activities at their highest level. The framework's "protect" function outlines the development and implementation of appropriate data processing safeguards.

In addition to laws and guidance focusing specifically on PII, agencies are subject to laws and guidance governing the protection of information and information systems. For example, the Federal Information Security Modernization Act of 2014 (FISMA) is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, as well as the effective oversight of information security risks. FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency, including those provided or managed by another entity.

FISMA also assigns government-wide responsibilities to key agencies. For example, NIST is responsible for developing comprehensive information security standards and guidelines for federal agencies. The act also requires agencies to comply with these federal information standards and guidelines.

To fulfill its FISMA responsibilities, NIST issues technical guidelines on many different aspects of information security, including, in 2017, on authentication and identity proofing. Specifically, NIST issued guidelines that outline how to authenticate a user's claimed identity.[10] The guidelines, among other things, define authenticator assurance levels (AAL) and methods. Specifically, AALs describe the degree of strength of authenticators (i.e., the stronger the authentication, the higher the AAL). Further, authentication methods such as passwords, tokens, and fingerprint scanning are assigned one of three AALs depending on the authentication requirements for federal systems.[11]

NIST also issued guidelines in 2017 on identity proofing that outline technical requirements for resolving, validating, and verifying an identity based on evidence obtained from a remote applicant. This guidance

[8]Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, M-22-09 (Washington, D.C.: Jan. 26, 2022). Zero trust architecture is a set of cybersecurity principles that are founded on the concept that no actor, system, network, or service operating outside of, or within, an organization's security perimeter should be trusted. Instead, the principles suggest that organizations must verify anything and everything that attempts to establish access to their systems, services, and networks.

[9]NIST, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, Version 1.0 (Gaithersburg, Md.: January 16, 2020).

[10]NIST, *Digital Identity Guidelines: Authentication and Authenticator Management*, Special Publication 800-63B-4 (Gaithersburg, Md.: July 2025).

[11]AAL1 requires either single-factor or multi-factor authentication. Factors could include memorized secrets (e.g. password) and physical authenticators (e.g. one-time password devices). AAL2 requires two different authentication factors, either (1) a physical authenticator and a memorized secret, or (2) a physical authenticator and a biometric that is associated with it (e.g. fingerprint scanner). AAL3 requires a hardware-based authenticator and an authenticator that provides verifier impersonation resistance. Hardware-based authenticators are typically public key infrastructure-based tokens, such as Personal Identity Verification cards.

defines identity assurance levels (IAL), which describe the degree of confidence that a user's claimed identity is their real identity (see table 1).

Table 1: Summary of the National Institute of Standards and Technology's Identity Assurance Levels (IAL)

IAL level	Description	Verification method
IAL1	There is no requirement to link users to a specific real-life identity. Any information provided by users should be treated as self-asserted and is neither validated nor verified.	No identity evidence is collected.
IAL2	The evidence provided supports the real-world existence of users' identities and verifies that users are appropriately associated with this real-world identity. This level introduces the need for either remote or physically present identity proofing.	Evidence may include a passport or driver's license, and supporting remote biometrics, such as a "selfie."[a]
IAL3	Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained credential service provider representative.	Evidence may include a passport and driver's license, as well as a physical or remote interaction supervised by a live operator.

Source: GAO analysis of National Institute of Standards and Technology Information. | GAO-26-109261

[a]A "selfie" is a photograph one takes of oneself.

In addition, NIST guidance requires applications to be assigned one of three IALs based on the sensitivity of information it holds, such as an SSN, and the potential harm caused if an attacker makes a successful false claim of an identity to gain system access.

GAO Has Reported on Identity-Related Fraud Threats

We have issued numerous reports on identity-related fraud threats and other risks.[12] As previously mentioned, the increase in cyberattacks on federal agencies and other organizations has led to a greater risk of the public's PII being used to commit fraud. These attacks can also be used to fraudulently obtain federal benefits or sensitive information, which can harm citizens and damage the reputation of federal agencies. We previously reported on fraud in the private and public sector, which can include:

- **new-account fraud,** in which thieves use identifying data, such as SSNs and driver's license numbers, to open new financial accounts without that person's knowledge.
- **existing-account fraud,** which is more common and entails the use or takeover of existing accounts, such as credit or debit card accounts, to make unauthorized charges or withdraw money.
- **government benefits fraud,** which can occur in many ways. One way is when thieves use stolen PII to fraudulently apply for or steal government benefits. For example, individuals or entities intentionally or knowingly providing false information (e.g., incorrect eligibility or identity information to receive a benefit

[12]GAO, *Identity Verification: GSA Should Demonstrate Its Implementation of Policies for Testing Data Backups on Login.gov*, GAO-25-107000 (Washington, D.C.: June 3, 2025) and GAO-25-106640.

from the federal government).[13] With respect to identity- related benefit theft, the Social Security Administration has reported that personal information of beneficiaries has been used to fraudulently redirect the beneficiary's direct deposit benefits.[14]

- **synthetic identity fraud,** which involves the creation of a fictitious identity, typically by using a combination of real data and fabricated information to apply for benefits or credit. As a result, individuals may face difficulties obtaining benefits or credit if their SSN has been used as part of a synthetic identity to commit fraud or may face health risks if their records are connected to someone else.[15]

The harms caused by exposure of PII or identity theft can extend beyond tangible financial loss, including the following:

- **Lost time.** Victims of identity theft or fraud may spend significant amounts of time working to restore their identities.
- **Emotional distress and reputational harm.** Exposed information also can cause emotional distress, a loss of privacy, or reputational injury.
- **Harm from state-based actors.** State-sponsored espionage can cause harm to individuals when nations use cyber tools as part of information-gathering, espionage, or other nefarious activities.

Increasingly, news reports and studies highlight the pervasiveness of fraud threats, including those from identity theft. As previously mentioned, in a May 2025 contract modification, GSA indicated that the Login.gov program was alerted that there were suspected fraudulent accounts that had passed Login.gov's IAL2 workflow. In response, the program's Anti-Fraud Team investigated all of the accounts and determined that fraudulent indicators were displayed. The team's assessment determined that the sophistication of these attempts would increase exponentially and that without the execution of an additional verification layer, the Login.gov platform would be at greater risk for fraud attacks.[16]

To combat these threats, the Login.gov program has taken and plans to take steps to prevent fraud. According to its December 2025 Program Roadmap, a cross-agency Threat Intelligence Working Group was introduced to collaborate on threat-related issues, such as coordinated fraud campaigns. The goal of the group is to share information on cybersecurity, digital identity, and fraud in order to improve the government's ability to detect and respond to fraud.[17]

[13]GAO, *Improper Payments and Fraud: How They Are Related but Different,* GAO-24-106608 (Washington, D.C.: Dec. 7, 2023). Improper payments are any payments that should not have been made or that were made in an incorrect amount, which can stem from various causes, including fraud. Fraud involves obtaining a thing of value through willful misrepresentation. Willful misrepresentation can be characterized as making material false statements of fact based on actual knowledge, deliberate ignorance, or reckless disregard of falsity. The extent of fraud government-wide will likely never be known with certainty because not all fraud will be detected, investigated, and adjudicated through judicial or other systems.

[14]For a related GAO report, see *Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display*, GAO-17-553 (Washington, D.C.: July 25, 2017).

[15]GAO, *Highlights of a Forum: Combating Synthetic Identity Fraud*, GAO-17-708SP (Washington, D.C.: July 26, 2017).

[16]General Services Administration, "Limited Sources Justification (FAR 8.4)," accessed July 12, 2026, https://sam.gov/api/prod/opps/v3/opportunities/resources/files/c5bb0654a100477d98fb9b332f2eb85a/download?api_key=null&status=archived&token=

[17]Login.gov Program Roadmap, December 2025, https://login.gov/docs/login-gov-roadmap-dec-2025.pdf.

Congress has also taken steps to address concerns about widespread fraud risks. For example, to help address the massive economic losses and security breaches tied to stolen identities, in January 2026 members of Congress introduced a bill that is aimed at strengthening U.S. digital identity infrastructure. Some of the key provisions of the legislation include: (1) establishing an identity fraud prevention grant program to help states build secure identity systems, (2) fostering the adoption of secure digital credentials, such as mobile driver's licenses, and (3) providing defenses against generative artificial intelligence[18] (AI)-related deepfake threats.[19] Efforts such as these may strengthen protections against identity fraud and could help to address some of the fraud risks outlined earlier in this statement by strengthening digital identity solutions.

GAO Has Reported on Login.gov Capabilities and Made Recommendations on Its Technical Challenges

Login.gov's Identity Proofing Process Collects, Shares, and Protects Personally Identifiable Information

As we reported in October 2024 and June 2025, GSA designed Login.gov to collect information from applicants who create an account to access federal websites.[20] Specifically, Login.gov requires users to create an account by entering their email address, create a password, and select a method of multi-factor authentication, such as using a text message, among other options. [21] After this process, users can choose to either continue with the online identity proofing processes or opt to go to a U.S. Post Office to finish the process.

After users create an account, Login.gov prompts them to upload an image of the front and back of their unexpired state-issued identification (ID) card. If users are able to successfully upload their ID, Login.gov reportedly encrypts the PII, and the data would be shared with third-party services for identity proofing. Specifically, users' PII goes through a series of checks with the following vendors:

- **LexisNexis' Document Authentication**:[22] The PII is to be sent to LexisNexis to check the authenticity of the ID by reviewing security features and checking for evidence of tampering to determine if there were any alterations to the image of the ID.
- **LexisNexis' Identity Validation**: Once a user's state-issued ID is deemed authentic, Login.gov sends the user's license data to LexisNexis to check that the data belongs to a single individual.

[18]Generative AI enables the creation of content, including text, images, audio, or video, when prompted by a user. This technology can be exploited by scammers to alter voices and images.

[19]Deepfake threats allow scammers to misrepresent themselves as reflecting a variety of backgrounds, languages, statuses, and genders to build rapport with a victim.

[20]GAO-25-107000 and GAO-25-106640.

[21]Multi-factor authentication is a method of authentication that requires more than one method, such as a password, and an additional means of verification, such as a code or token.

[22]Document authentication is a component of the LexisNexis® Risk Solutions which captures users' PII, including the front and back images of their state-issued ID.

- **Driver's License Data Verification Service**:[23] Once the users' state-issued ID is deemed authentic and the PII is verified to belong to one individual, Login.gov sends the user's license data to the driver's license data verification service.
- **LexisNexis' Phone Validation**: Login.gov also sends users' PII including name, SSN, DOB, and phone number to a LexisNexis service to verify that the phone number provided is associated with the user and that the user is the phone's account owner.

Login.gov then prompts users to re-enter the password created when the account was established. Once successful, the process is complete.

Users may also opt to have identity proofing done in person or may need to do so if they are unable to upload their ID online.

- In-person proofing as an initial verification option: Users can initially select the "verify in person" option, allowing users to conduct the identity proofing process in person. Users would select a U.S. Post Office to visit, then enter information from their state-issued ID, such as name, address, DOB, and unexpired ID number, in addition to their SSN and phone number. After Login.gov performs the verification checks described above, the system is to then generate a barcode that users can print or download to present along with their state-issued ID to the post office.[24]
- In-person proofing after failing to upload ID: As described above, as part of its online proofing process, Login.gov prompts users to upload an image of the front and back of their unexpired state-issued ID. If a user's ID image fails to upload, the user is to have the option to verify their identification at their local participating U.S. Post Office. To do this, users will need to enter information from their ID, including their name; DOB; unexpired state-issued ID number; and address, in addition to their SSN and phone number.

After successful verification at the post office, users receive an email from Login.gov to sign back into the system. Login.gov confirms that the user has had their identity verified and obtains consent to share their PII with the relevant federal agency.

In addition to its identity-proofing functionality, Login.gov also provides its customers with tools to monitor and prevent fraud. These tools can be used to monitor users through behavioral biometrics during the identity proofing process to determine if a fraudulent participant was involved during this process. Behavioral biometrics analyzes a user's digital, physical, and cognitive behavior to distinguish between cybercriminal activity and legitimate use. It also provides GSA with the ability to collect and analyze risk signals based on how users interact with their devices when accessing the Login.gov website, such as how they touch and move their devices.

[23]The Driver's License Data Verification Service is offered by the American Association of Motor Vehicle Administrators.

[24]Users must use this barcode within 30 days.

GSA Took Steps to Improve Login.gov and Made Progress to Address Most of GAO's Recommendations

In recent years, we have reported on Login.gov's alignment with federal guidelines for identity verification and data protection and fraud prevention measures.[25] In our June 2025 report, we reported that Login.gov and selected commercial solutions largely implemented recommended data protection categories in the "protect" function suggested by NIST.[26] More specifically, we reported that while Login.gov implemented four out of the five data protection practices, it did not fully implement policies and procedures for testing the integrity of its backup data that NIST recommends. Data loss—whether through a ransomware attack, hardware failure, or accidental or intentional data destruction—can have catastrophic effects on the confidentiality, integrity, and availability of any IT assets, services, and sensitive data. For example, if Login.gov's backup data was not tested to ensure that its integrity was not compromised, then it could result in complete loss of data if a breach were to occur. As a result, we recommended that GSA ensure that Login.gov demonstrates that it fully implemented the policy to test its data backups.

In July 2026, we verified that GSA's procedures and test output from June 2025 and 2026 demonstrate that the agency has begun testing its data backups, and doing so on an annual basis as required by policy. By taking action to ensure that data backups are maintained and testing that the integrity of the backups is not compromised, GSA has helped to reduce the impact of data loss incidents.

In October 2024 we reported that GSA had not fully completed actions needed to ensure Login.gov was secure, reliable, and aligned with federal requirements in several areas. Specifically, GSA had not yet completed the work necessary to ensure Login.gov met the requirements of NIST guidelines on identity proofing, particularly IAL2. For example, GSA has been taking steps to align Login.gov with NIST guidelines, including (1) completing a pilot on in-person identity proofing in March 2024 and (2) beginning a separate pilot on remote identity proofing. However, at the conclusion of our audit work, the remote identity proofing functionality was not yet available because GSA had not established an expected completion date for the pilot. Accordingly, we recommended GSA establish a completion date for the remote identity-proofing pilot.

In March 2025, GSA took action to address the recommendation. Specifically, Login.gov completed its remote identity-proofing pilot and a third-party reviewer assisted GSA in confirming the functionality worked as intended. As a result, Login.gov began offering IAL2 remote identity-proofing services to all users. Having completed the pilot and confirmed the functionality works as intended, GSA is better able to ensure that Login.gov users are linked to a specific real-life identity, as required by NIST guidelines.

Additionally, in October 2024, we reported GSA had not resolved agency-reported technical challenges or established timelines for addressing many of the concerns. In particular, twelve of 21 agencies reported challenges related to Login.gov's noncompliance with NIST IAL2 guidelines at the time. In addition, nine agencies reported challenges involving technical issues, such as not having visibility into authentications, high failure rates, and lack of fraud controls, among others. Further, at the time of our audit work, eight agencies reported challenges related to Login.gov's pricing structure. As a result, we recommended GSA propose

[25]GAO-25-107000 and GAO-25-106640.

[26]According to NIST's Privacy Framework, the "protect" function focuses primarily on data protection. NIST describes the function as practices that address privacy and cybersecurity risk management and are intended to prevent cybersecurity-related privacy events.

actions to address the technical challenges that the agencies identified related to Login.gov and develop mutually agreed-upon time frames for taking those actions.

In response to this recommendation, in December 2024, GSA developed a public Login.gov roadmap outlining planned and ongoing efforts to address agency-reported technical challenges and improve system functionality. GSA also established a Partner Advisory Group to engage participating agencies in structured discussions regarding fraud prevention, enhanced Login.gov features, and identity-related challenges. However, these actions alone do not fully demonstrate that the specific technical challenges identified by the agencies we interviewed have been addressed, or that mutually agreed-upon timeframes were established for resolving those challenges, as recommended. Without GSA-proposed actions and time frames for addressing the challenges, agencies will continue to experience technical issues with the system. We will continue to monitor GSA's actions to implement this recommendation.

In October 2024, we reported that GSA had not documented lessons learned from its Login.gov pilot efforts. Specifically, the agency conducted a pilot that resulted in Login.gov offering users the option to conduct in-person proofing at post office facilities at the start of the identity-proofing process. GSA also conducted an additional pilot to provide remote identity proofing. We found that GSA's two identity proofing pilots met most of the leading practices for pilot programs. However, we found that for the in-person proofing pilot, GSA did not identify and document lessons learned nor did it have plans on how it was going to document lessons learned for the remote identity proofing pilot. Accordingly, we recommended GSA develops and document a plan for identifying lessons learned for Login.gov's remote identity-proofing pilot program.

As of June 2025, GSA has taken actions to address the recommendation by establishing a process to capture and document lessons learned from its remote identity-proofing pilot program. GSA provided a lessons learned template and supporting examples demonstrating that the process has been used in collaboration settings. GSA has demonstrated that it has a mechanism in place to capture insights from pilot activities and document lessons learned from pilot activities.

In conclusion, identity fraud threats are pervasive and likely to continue to escalate. 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. Our work has identified actions that GSA can take to protect PII and help prevent identity theft. Fully implementing our remaining recommendation would help the federal government ensure PII is better protected and lessen the risk of identity theft.

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee, this concludes my prepared statement. I would be happy to answer any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Marisol Cruz Cain at CruzCainM@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this statement.

GAO staff who made key contributions to this testimony are Elena Epps (Assistant Director), Sher'rie Bacon (Analyst-in-Charge), Kami Brown, Chris Businsky, Jillian Clouse, Jonnie Genova, Keith Kim, Lee McCracken, and Evan Nelson Senie.

Related GAO Products

Identity Verification: GSA Should Demonstrate Its Implementation of Policies for Testing Data Backups on Login.gov. GAO-25-107000. Washington, D.C.: June 3, 2025.

Fraud Risk in Federal Programs: Continuing Threat from Organized Groups Since COVID-19. GAO-25-107508. Washington, D.C.: July 10, 2025.

Identity Verification: GSA Needs to Address NIST Guidance, Technical Issues, and Lessons Learned. GAO-25-106640. Washington, D.C.: October 16, 2024.

COVID-19: Insights and Actions for Fraud Prevention. GAO-24-107157. Washington, D.C.: Nov 14, 2023.

Improper Payments and Fraud: How They Are Related but Different. GAO-24-106608. Washington, D.C.: December 7, 2023.

Employment-Related Identity Fraud: Improved Collaboration and Other Actions Would Help IRS and SSA Address Risks. GAO-20-492. Washington, D.C.: May 06, 2020.

Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services. GAO-19-230. Washington, D.C.: March 27, 2019.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

Related GAO Products

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us