

Login.gov

Program Roadmap







What is Login.gov?

Login.gov enables members of the public to create a single digital account that provides access to their benefits and services at over 50 federal and state agencies.

This “one account for government” is a key piece of national infrastructure – providing a secure, resilient platform that enables a seamless user experience while combating emerging security threats.

Key Benefits:

-  Saves users time and protects them from identity theft
-  Reduces costs, complexity, and fraud risks for agencies
-  Ensures consistent cross-agency security and anti-fraud practices
-  Creates government-wide efficiencies and saves taxpayer dollars

Login.gov's North Star:

Any member of the public can use their trusted Login.gov account to access all of their online government services.

About this Artifact

Transparency is a guiding principle for Login.gov, which can be seen in the many ways in which we work alongside our partners and the public to promote collaboration and accountability.

Plans

(e.g., program roadmap, partner webinars)

Program Roadmap – June 2025

	FY25 (May Sept) Start to deliver	FY26 (Oct March) Test on the market	FY28 (April Sept) Expanded direction
End User Needs	<ul style="list-style-type: none">Partners at evidence during identity verificationPersonalized user journey and managementEducational content on security identity theft threats	<ul style="list-style-type: none">Initiated proofing to meet other government agenciesMobile Driver's LicenseNew identity verification acceptance via government authoritative records checks	<ul style="list-style-type: none">New use cases supported (e.g., international travel)Mobile Driver's License for hard-to-verify populationsAt government line of dutyContinued US investments across the full user journey
Partner Support	<ul style="list-style-type: none">Self-service portal & improved reportingAuto fraud signal sharing API	<ul style="list-style-type: none">Expanded self-service portalCross-channel identity verification campaigns	<ul style="list-style-type: none">Shared research initiativesAdditional interagency working groups
Fighting Fraud	<ul style="list-style-type: none">Deeper anti-fraud analytics and investigative toolsAdditional identity vendors & provider sector partnerships	<ul style="list-style-type: none">Cross-agency threat intelligence modelingMore data sources to inform anti-fraud efforts	<ul style="list-style-type: none">NIJ 800-63 Revision 4 compliance (SAL & HLD)Cross-agency anti-fraud workshops

Last updated June 2025. These are initiatives and may be revised at the future Login.gov will be transparent with partners about when they happen.

Policies

(e.g., privacy impact assessment, FedRAMP)



Code

(e.g., open-source code, developer documents)



Collaboration

(e.g., partner / industry working groups)



The content presented in the Login.gov Program Roadmap is forward-looking and intended for informational purposes only. We will update and re-share this artifact regularly.

About Login.gov

Challenge of Identity in America

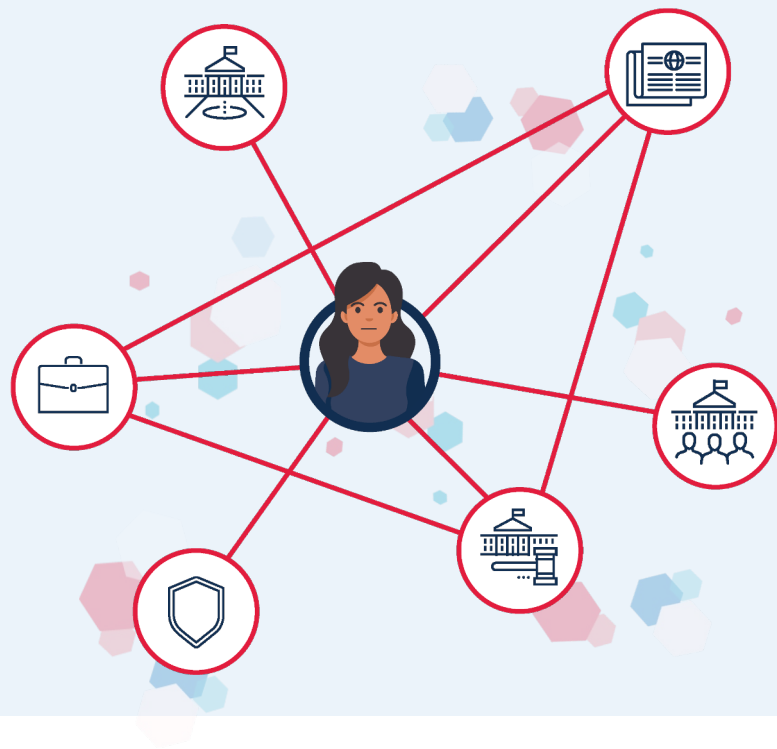
Fragmentation

Pain points for the public

- Managing multiple user accounts and passwords
- Entering the same information over and over
- Interacting with government systems with varying degrees of privacy / security protections
- Struggling to overcome barriers to access

Caused by fragmentation

- Level of government: Federal / State / County / Local
- Agency: Program, bureau, service, location
- Diverse stakeholders with varying requirements



Challenge of Identity in Government Services

Increasing access while preventing fraud

Access



340M+¹

Members of Public

Requiring varying degrees of access to government services

Fraud



\$233-521B²

Losses to Fraud

Estimated total direct annual financial losses to the government from fraud

¹Source: [Census](#)

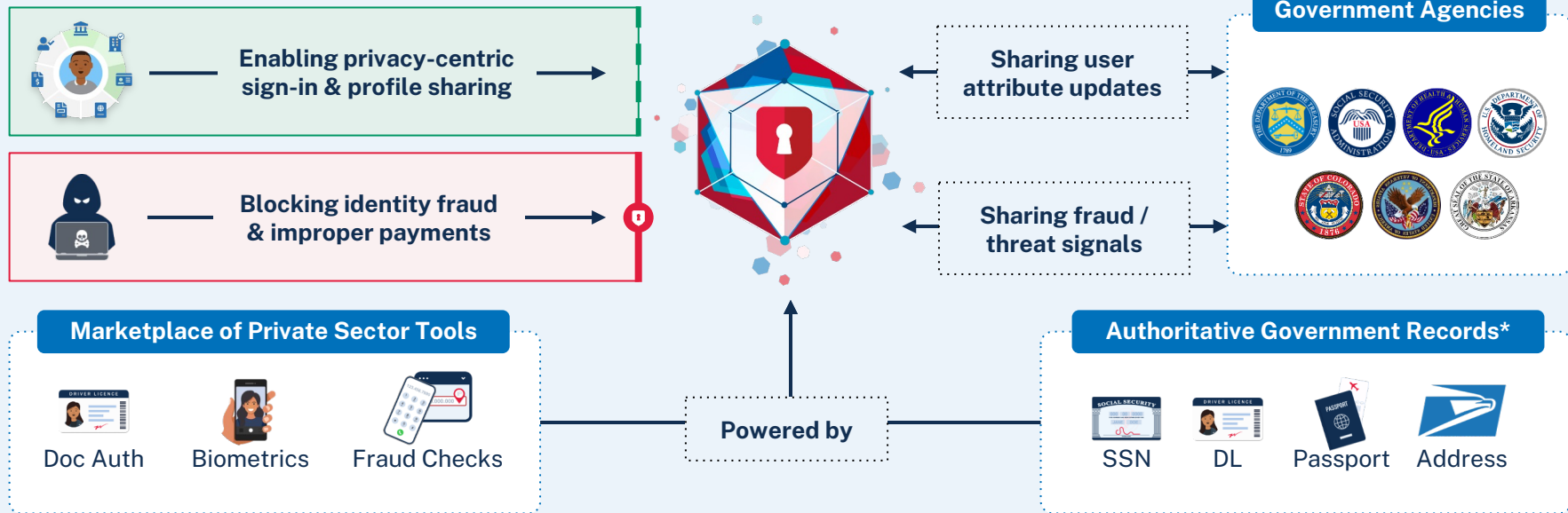
²Based on GAO Fraud Risk Management 2018-2022 which estimated fraud across government, including fraud attributed to identity issues

Login.gov Addresses These Challenges

Bringing together the best of public and private sector

Government-wide Identity Platform

Saves people time | Saves taxpayer dollars



*Includes current and planned

Value to Agencies

We're building a future where every agency can focus on their mission.

Simplifies Identity Management

- Cost and efficiency benefits of SaaS (software-as-a-service)
- Simple integration & agreements process
- A 24x7 contact center reduces agency burden
- “Pay for what you use” pricing that scales

Improves Access To Government Services

- Imperative to reach all members of the public
- Deep investments in user-centric capabilities
- Reliable platform that handles high usage
- Reusable credential reduces friction to service delivery

Prevents Fraud and Protects User Identity

- Multi-faceted anti-fraud program mitigating the threat of bad actors
- FedRAMP-authorized security controls
- Privacy-preserving encryption model
- Public-sector accountability & transparency

Value to the Public

We're building a future where every member of the public has seamless and secure access to government services.

Fewer Headaches

- Just one password to remember
- Proof once, use everywhere
- Easy-to-use web and mobile experience

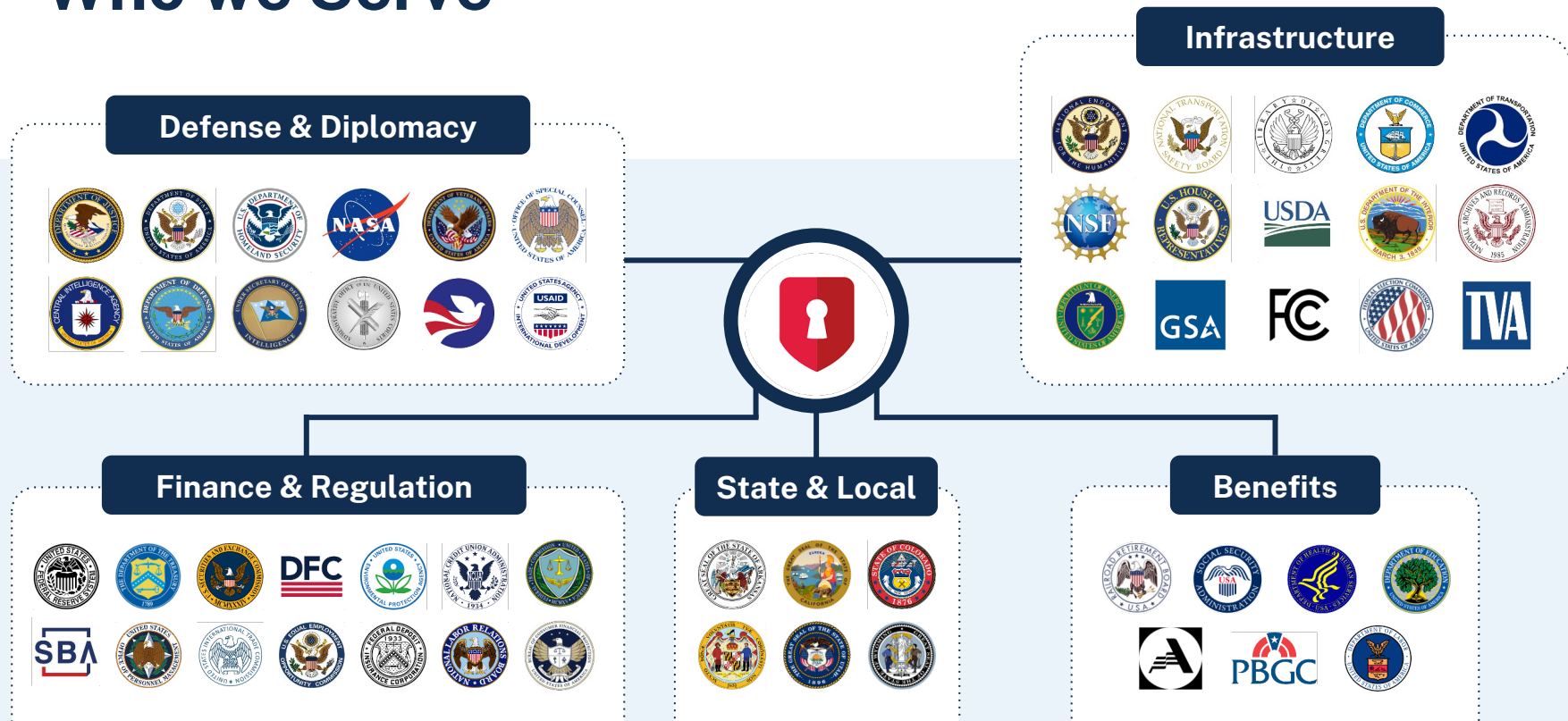
Better Support

- Multiple choices for MFA (multi-factor authentication), identity proofing, etc.
- A “serve everyone” mindset & mission
- 24x7 contact center

Identity Protection

- Strong security and anti-fraud controls keep your information secure
- User data is private by default and not used for any purpose unrelated to identity verification

Who we Serve



100+ million user accounts | 500+ million sign-ins annually | 700+ live sites and services | 54 agencies and states

Login.gov

Program Roadmap

Program Roadmap – December 2025

	2025 Jul-Dec Recently launched	2026 Jan-Jun Working on now	2026 Jul-Dec Expected direction
End User Impact	<ul style="list-style-type: none">• Passports as evidence during identity verification• Improved account recovery and management• Educational content on spotting identity theft threats	<ul style="list-style-type: none">• Mobile driver's licenses• New identity integrations via government + vendor sources• Inherited proofing to reuse existing proofing mechanisms (e.g., PIV/CAC)	<ul style="list-style-type: none">• New use cases supported (e.g., international users)• Alternative pathways for hard-to-verify populations• AI-powered live chat• Continued UX investments across the full user journey
Partner Support	<ul style="list-style-type: none">• Self-service portal & improved reporting• Anti-fraud signal sharing API	<ul style="list-style-type: none">• Expanded self-service portal• Cross-channel identity verification campaigns	<ul style="list-style-type: none">• Shared research initiatives• Additional interagency working groups
Fighting Fraud	<ul style="list-style-type: none">• Deeper anti-fraud analytics and investigative tools• Additional identity vendors & private sector partnerships	<ul style="list-style-type: none">• Cross-agency threat intelligence modeling• More data sources to inform anti-fraud efforts	<ul style="list-style-type: none">• NIST 800-63 Revision 4 compliance (IAL1 & IAL2)• Cross-sectoral anti-fraud forums

Program Roadmap

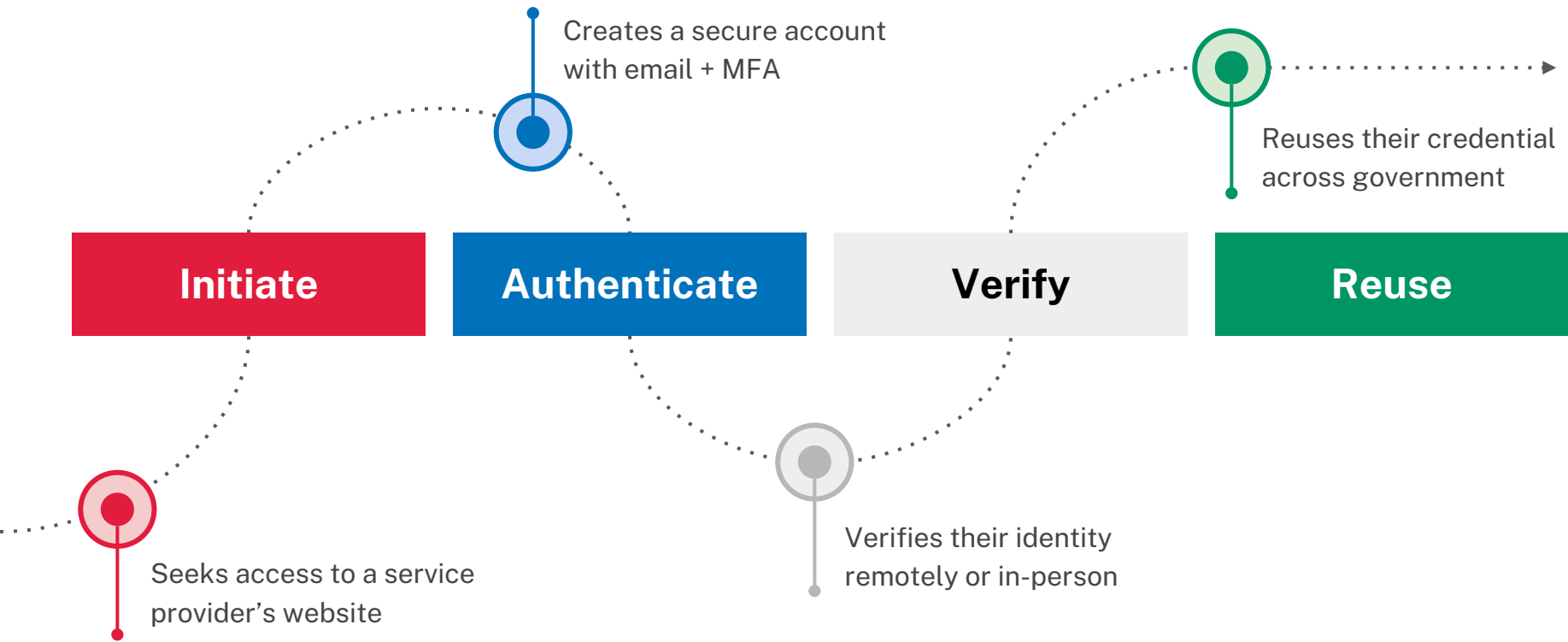
End User Impact

End User Impact

Partner Support

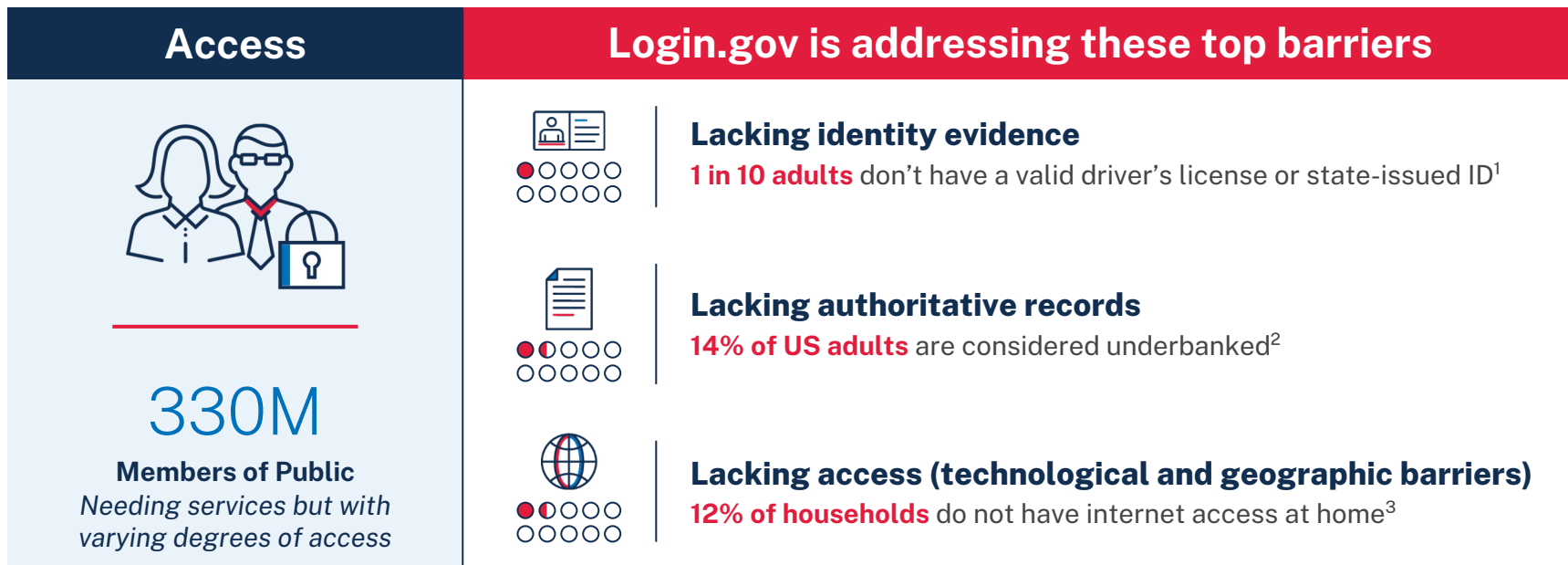
Fighting Fraud

The Login.gov User Journey



Importance of User Access

Login.gov's imperative is to serve all members of the public.



Sources: ¹[CDCE](#) ²[FDIC](#) ³[NTIA](#)

U.S. Passports as Evidence

Login.gov has partnered with the U.S. Department of State to leverage their new API for validating passport attributes in a privacy-preserving manner. This is a “first of its kind” opportunity using Login.gov’s digital identity platform to combine private sector tooling with authoritative government records.

Benefits of Using an Authoritative Government Source

- More options for users to easily verify their identity
- Secure government-to-government data exchange
- Reliable, up-to-date information from issuing source
- Adherence to Login.gov privacy and data usage policies



94% of U.S. adults have either a driver's license or a passport¹



Over 400k passport validation attempts during initial launch phase

¹Source: [CDCE](#)

Unlocking the potential of Mobile Driver's Licenses

Login.gov is partnering with NIST, identity vendors, and states nationwide (via the [NCCoE Initiative](#)) on a demonstration project to integrate mDLs within Login.gov's online identity proofing process.



Benefits

- **Streamlined user experience:** Eliminates photo capture of identity document and selfie steps, reducing user friction and improving proofing rates.
- **Improved government efficiencies:** Drastically cuts costs associated with document authentication: ends the need for repeat document capture attempts while reducing user support needs.
- **Stronger digital defense:** Cryptographically-secure mDLs cannot be forged.
- **Aligned with the latest guidelines:** Meets NIST SP 800-63-4 digital identity guidelines.



What's Next



- NCCoE Initiative's Phase 2 launches in **December 2025**
- Login.gov is planning to begin accepting mDLs by **Summer 2026**

Providing More Options and a Better User Experience

Login.gov is leading the way with In-Person Proofing

In-person proofing (IPP) gives Login.gov users the option to complete identity verification in-person at one of over 18,000 USPS locations across states and U.S. territories.

IPP provides a convenient and secure identity verification option for those that prefer it, and is available as part of both basic (non-IAL2) and enhanced (IAL2) identity verification workflows.

Source: ¹[USPS](#)

Increasing access



99% of the public live within 10 miles of a USPS location¹

Prioritizing security



1% of users who visited a USPS location were turned away due to **insufficient or invalid evidence, which is in line with expectations**

We are continuing to invest in our in-person offerings in FY26 and beyond.

New Identity Integrations to Increase Proofing Rates

We continue to work on integrating best-in-class private sector technologies alongside credible and authoritative government sources with the goal to increase accessibility and boost the proofing pass rates.

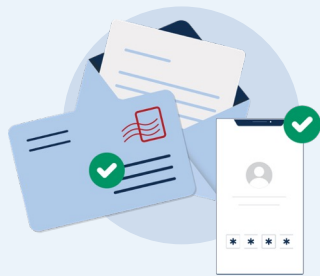
Benefits:



Improve the proofing rate
among "hard to match"
legitimate users



**Enhance protection against
fraudulent activity** while reducing
friction for legitimate users



**Ensure we provide compliant
IAL2 level proofing**, which today
requires address verification

Working on the Future of Digital Identity Verification

Government records are at the heart of identity, and Login.gov is collaborating with agencies and industry partners to develop common-sense approaches to incorporating these as part of the identity verification process of the digital age.



NIST

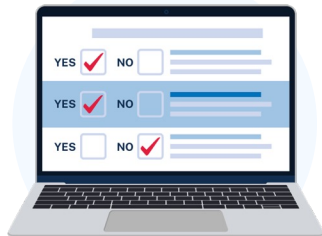
NIST Rev4

We're incorporating the new NIST guidelines into our planning to expand identity verification options and reduce friction for users.



Inherited Proofing

We're working with agencies to reuse existing government proofing mechanisms (e.g., PIV/CAC) for identity verification.



Attribute Validation

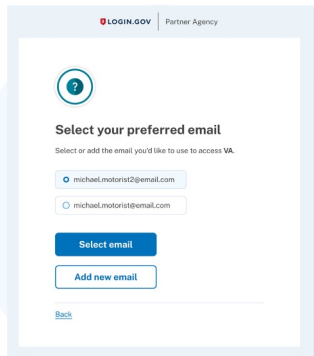
We're integrating privacy-preserving APIs that confirm information accuracy based on agency records and with the user's consent.

Investing in Alternative Pathways for Hard-to-Verify Individuals

- Some members of the public will not be able to verify their identity following standard identity verification processes and aren't able to visit a USPS location to do so.
- We're investing in expanded proofing channels that allow a user to complete the identity verification process through an alternative workflow.
- Given quickly evolving generative AI capabilities in the world, our solution must maintain a high bar around security and privacy in order to protect against fraud threats like deep fakes and social engineering tactics.



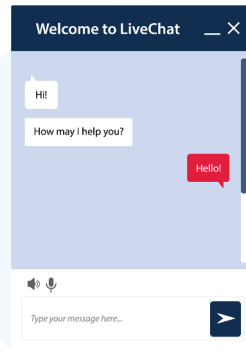
Continually Developing New User-Centric Capabilities



Account Management & Recovery

We recently released a new feature that provides users with the **flexibility to select the email address** they wish to share with each partner agency.

This year, we will release an improved process for managing and recovering accounts.



AI-powered Live Chat

We are exploring AI-powered tools that will **assist and empower users** to quickly find the answers to questions they have about Login.gov.

These tools will complement our amazing human agents, and we will use AI responsibly.

Help Center Update

Based on user input and research, we upgraded our Help Center for a more intuitive, user-friendly experience, to quickly support the public.

Updates include:



Streamlined navigation (fewer clicks)



Clearer, more detailed article titles (e.g., specific authentication methods like Face or Touch Unlock)



Content organized around real-life user questions

Since launching the redesigned Help Center:



43+ million visitors

to the new Help Center



Login.gov will continue to add new content and features based on evolving public needs.

User-focused Educational Video Series

Login.gov launched a new [YouTube channel](#) with educational videos covering basic identity concepts such as identity verification, multi-factor authentication, spotting identity theft threats, and more.

Benefits & Features:



Provides helpful tips for setting up, managing, and protecting Login.gov accounts



Helps users troubleshoot common issues and enhance their user support experience



Complements outreach materials that agency partners provide their users



Tip: Subscribe to the channel to receive alerts when new content is added.
Login.gov YouTube channel: www.youtube.com/@loggingovgsa



Program Roadmap

Partner Support

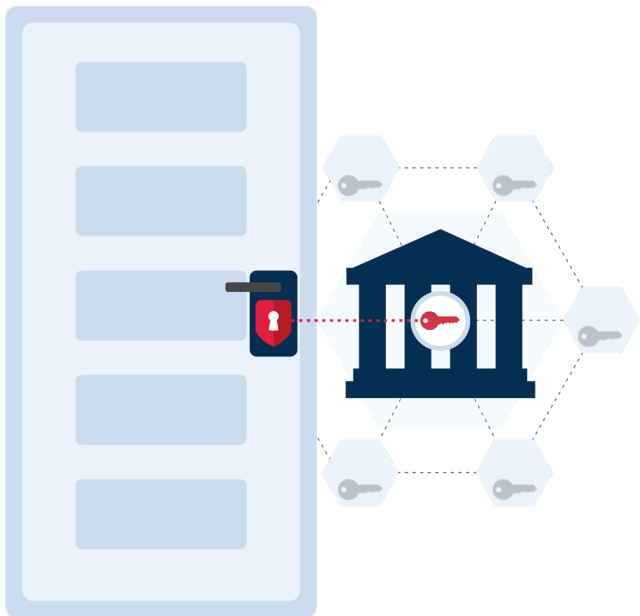
End User Impact

Partner Support

Fighting Fraud

Partner Support

Login.gov is the front door to government services, and we work closely with agencies to help them achieve their mission.



Login.gov's Commitment to Partners



Help you focus on your mission by handling scalability and customer support



Mitigate unauthorized access with a multi-faceted fraud prevention program



Save you money through transparent and cost-recoverable pricing



Protect your users' information through a privacy-preserving encryption model



Constantly improve systems with best practices and tools from industry



Help you learn best practices from other agencies and identity experts



Help you launch successfully through change management tools and resources

Our Service Offerings

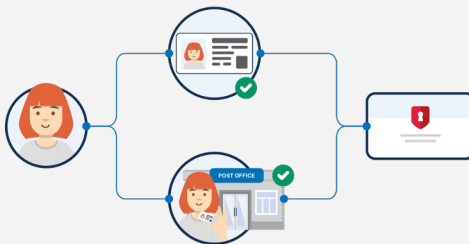


We successfully completed the independent Kantara assessment for National Institute of Standards & Technology (NIST) SP 800-63-3 compliance (IAL2 and AAL2). We are now working toward compliance with the newly-released NIST SP 800-63-4 guidance, demonstrating Login.gov's commitment to secure partner integration and user access.

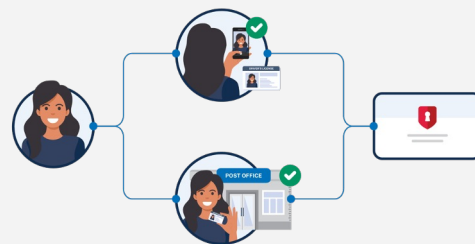
Authentication-only



Basic identity verification



Enhanced (IAL2) identity verification



Strong Privacy Model



Anti-Fraud Controls



24x7 Contact Center

Our Transparent Pricing Model

Login.gov conducted an extensive analysis in order to restructure pricing so that accelerated adoption could be translated into increased affordability for agency partners.

1

Authentication

Authentication prices are based on Monthly Active Users (MAUs) and decrease as volume increases.

\$0.10 per MAU* (starting price)

Savings as your agency scales

2

Identity Verification

Identity verification prices are oriented around a user's "credential lifecycle" and are substantially more affordable than before.

\$3 per active user if your agency is first to proof a user in a credential cycle (year 1)*

\$1 per active user per year if the user is already proofed*

*Based on a five year credential lifecycle of a user being proofed at your desired assurance level.

3

Minimum Billing Amount

The minimum billing amount is lower than previous plans, and more aligned with agency usage.

\$2,500/month*

Savings up to 50%

*Transactional costs now count towards minimum, providing additional savings

* Billed at the agreement level, so that agencies see savings when a user accesses multiple applications

Login.gov Partner Portal

We are adding features to the portal to improve application and team management.



In Place Today

Create and manage sandbox applications

Configure apps and request launches to production

Create and manage teams in sandbox

Streamlined deployment process

Submit tickets and read documentation

View relevant alerts, updates, etc.



What's Coming

What's available today in a single place, plus:

Manage production applications and teams

Improved team management workflow

Self-serve reports and data access

At-scale user management

Email notifications

Tackling Government-wide Identity Challenges Together

One way Login.gov engages agencies is through our Partner Advisory Group where we gather feedback from agency partners in a small group discussion setting.

Goals

1

“Voice of the Customer” input into the Login.gov roadmap and planning process

2

A forum for cross-agency collaboration and discussion around shared Identity needs

3

An avenue for recommendations on program decisions that impact government at-large

PAG Membership

This is an interagency group with rotating representation from agencies of all sizes across key Login.gov user segments, as well as partners representing state / local / territorial / tribal entities using Login.gov.

Working with a diverse representation of agencies helps Login.gov prioritize features and support that meet partners’ and the public’s evolving needs.

Coming Soon!

State Working Group

Similar to the PAG, but focused on State & Local issues, the SWG will include representatives from our current State & Local partner agencies.

Breaking Down Information Silos to Fight Fraud



Login.gov has introduced a cross-agency **Threat Intelligence Working Group (TIWG)** in order to **collaborate on threat-related issues** including dark web trends, spoofed sites, coordinated fraud campaigns, and more.

Because **our platform is connected to 50+ agencies**, it is well-positioned as a cross-government first line of defense in identifying trends and sophisticated attacks targeting our most-valuable resources in ways that break down traditional information silos.

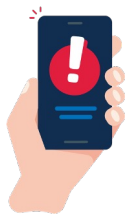
The goal of the TIWG is to **share intelligence across the cybersecurity, digital identity, and fraud domains**, strengthening interagency coordination, and improving the government's ability to **detect and respond to fraud**.

Other interagency groups

Login.gov's security team hosts a monthly **Continuous Monitoring (ConMon) Meeting** with agency partners to review Plan of Action and Milestones, Deviation Requests, and Significant Change Requests in order to make better risk-based decisions through collaboration.

Collaborating with Partners in Various Ways

By leveraging existing touchpoints, data, and shared insights



Signal sharing

Deployed a new API for sharing real-time security and fraud-related events with agency partners to help them fight fraud



Cross-channel identity verification campaigns

Help users setup and reuse their Login.gov credential across more agencies and channels to realize the full benefits of “one account for government” (e.g., in-person signup events)



Shared research opportunities

Continue to work with NIST, DHS S&T, and various agency, industry, and academic partners to further the identity space

Partner / Industry Events

FY25 Events

Login.gov engaged in key conferences this year, taking an active role in the evolving conversation around identity verification, its opportunities and challenges.

- ✓ **NASCIO Midyear Conference**
- ✓ **Identiverse**
 - *Balancing Access & Security at Scale*
 - *Ain't No Party Like a Relying Party: Verifiable Digital Credential Edition*
- ✓ **Federal mDL Industry Day**
- ✓ **Identity Week**
 - *Stronger Together: Public-Private Partnerships at Login.gov*
- ✓ **Federal Identity Forum and Expo**
 - *Breaking silos: IdAM Across the Government*
 - *Business Model of Credential Providers & Leveraging MDLs*
 - *What's New in U.S. Government Identity*
 - *AI for HISPs: An Identity-First Approach to the Action Plan*



FedID 2025 Panel

Know of an upcoming event that Login.gov should participate in?

**Contact us at
partners@login.gov**

Program Roadmap

Fighting Fraud

End User Impact

Partner Support

Fighting Fraud

Login.gov as a Foundational Anti-Fraud Tool

Login.gov implements a variety of fraud controls and investigative techniques to provide a holistic defense against fraudulent actors. In this way, we are partnering with government agencies in order to help protect the integrity of government systems and members of the public from identity theft.



We are continuing to invest significant resources into adding new controls and collaborative signal sharing techniques.

Additional details are available upon request by agency partners.



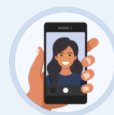
State ID / Driver's license



Social Security number



Phone number



Facial matching



Mailing address



Device / IP address



Other controls

Protecting Users Against Identity Theft

Anti-fraud isn't just about protecting agency systems, it's about preventing the devastating human impact of identity theft.



Financial Loss

In 2024, over 18 million American adults lost a total of \$47 billion to identity fraud¹ with a disproportionate affect on older populations. People in their 60s claimed a total of \$1.18 billion lost through fraud and those in their 30s \$810 million.²

Significant Increase in 2025

748,555 cases of identity theft were reported in the first half of 2025³, up over 196,000 year over year.

Credit Impacts

Fraudulent accounts can take months or years to remove from a credit report and if not caught on time, the victim can be liable for the debt incurred

Psychological Impact

Per ITRC, 83.3% reported feeling worried or anxious, 75.4% felt vulnerable and 73% felt angry.⁴

Sources: ¹[AARP](#), ²[AARP](#), ³[The Motley Fool](#), ⁴[ITRC](#)

A Dedicated Team for Preventing Fraud

● Data Analysis and Engineering

Looks at suspicious user behavior and data to find fraud patterns, develops new fraud detection measures, and collects insights to guide program decisions.

● Case Investigations

Investigates high-risk account setups, manages redress cases, and reports broader trends for deeper analysis.

● Special Investigations

Carries out detailed studies on large, suspicious datasets, using the results to suggest improvements in fraud controls.

● Quality Assurance

Makes sure investigations follow set procedures, fixes any mistakes, and creates feedback systems to avoid future issues.



Threat Intelligence, Detection, and Evaluation (TIDE) ●

Identifies and reports on complex fraud risk and cyber threats to the program and its partners. Passes findings to other teams for investigation and remediation of risks.

Fraud Risk Assessment ●

Uses a structured approach to identify vulnerabilities in new product lines, making sure strong fraud prevention is built in from the start.

Partner Fraud Support ●

Looks into suspected fraud cases sent by partners, shares results internally to improve controls, and tells partners about the findings, including linked accounts, if fraud is confirmed.

NIST Compliance Path Forward

Login.gov is developing new capabilities in accordance with NIST SP 800-63 Revision 3, and we are building towards the recently-published NIST SP 800-63 Revision 4.

We created a cross-functional working group to review the over 400 pages of requirements and recommendations in NIST SP 800-63-4 to incorporate into Login.gov's planning.



Login.gov

NIST Compliance Status



800-53-5 Compliance



800-63-3 Compliance



800-63-4 In Progress

Login.gov and NIST Rev4 Compliance*

Based on the working group's analysis, Login.gov identified how it is already delivering on NIST Rev4 guidance and how it will incorporate NIST Rev4 into its planning.

Login.gov currently **MEETS** many NIST Rev4 compliance areas (Examples)

- ✓ Has a mature cross-functional fraud program
- ✓ Implements valuable anti-fraud checks
- ✓ Recommends partners offer alternative IdV channels for access to services
- ✓ Provides biometric protections
- ✓ Offers phishing-resistant authenticators

While continuing to **IMPLEMENT** other areas identified in NIST Rev4 (Examples)

- ⌚ Using new forms of identification (i.e., mDLs)
- ⌚ Aligning with the new IAL1 and IAL2 requirements
- ⌚ Exploring alternative pathways for hard-to-verify individuals
- ⌚ Updating trust agreements
- ⌚ Standardizing our continuous improvement metrics

*Login.gov is in compliance for IAL2 with NIST Rev3

Anti-Fraud Investments in FY26 and Beyond



Tools & Data

Continued investments in efficiently and effectively performing fraud detection and prevention



Collaboration

- Additional identity vendors and private sector partners
- Cross-agency threat intelligence modeling
- Cross-sectoral anti-fraud workshops

Partnering with Industry to Accelerate Innovation

Login.gov harnesses best-in-class private sector technologies to stay ahead of evolving threats. As a government-wide identity platform, we work with multiple vendors across our various components to bring cutting-edge solutions to the public faster and more efficiently.



Market research: We use Requests for Information, product demonstrations, industry-wide testing frameworks, and studies as appropriate to understand how technology can enable a secure user experience for the public.



Contracting: We partner with numerous cloud platform, technology service, and identity verification companies in order to power key components of our service.



Industry participation: We attend conferences, working groups, and other forums to collaborate with our digital identity peers.



Private sector best practices: We leverage agile software development processes, perform user research, adopt leading anti-fraud and customer success practices, and more.

Login.gov's Biometric Promise

Providing those interacting with government with a way to verify their digital identity that protects their security and privacy while ensuring access is critically important

To protect users, Login.gov will:

Always protect user data by ensuring it will never be used for any purpose unrelated to verifying your identity by Login.gov or its vendors

Use a privacy-preserving matching approach that is built on clear consent and other privacy-preserving measures

Leverage best-in-class facial matching algorithms that, based on testing in controlled environments, have been shown to offer high levels of accuracy and reduced algorithmic bias

Continue to engage agency partners via anti-fraud collaboration, incorporate private sector best practices, and invest in academic-quality research to use emerging technologies responsibly

Looking Forward

Human-Centered Iteration

Login.gov is **built by digital service experts** with substantial government and industry experience.

We **listen to the public and agencies** alike to develop new capabilities and fix issues.

Our team **follows agile practices** and deploys code to production frequently.

We believe in **continuous improvement** and employ a variety of methods to learn and grow.

We **quickly adopt emerging technologies and federal policies** to confront evolving threats from bad actors.



We Value Your Feedback

We update and re-share this artifact regularly, and use your feedback to adapt our plans.

Please let us know:

- What use cases would you like us to support?
- What capabilities would improve service delivery?
- How can we continue to improve collaboration?

Contact us at partners@login.gov



Thank you.

