Login.gov

Program Roadmap

About This Artifact

The content presented here is forward-looking and intended for informational purposes only. We will be updating and re-sharing this artifact regularly.

Role in Government

The public's "one account for Government"
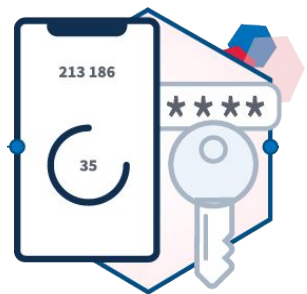

Each agency's "public option" for Identity

A key piece of national infrastructure

Services

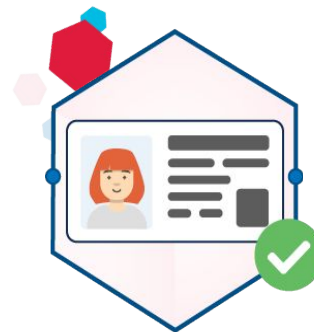Public-sector digital identity management as a service to Federal agencies and State governments

Authentication

Identity Verification

Strong Privacy Model ✚ Anti-Fraud Controls ✚ 24x7 Contact Center

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 1 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 and 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

Value to Agencies

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

Simplifies Identity Management	Expands Access To Government Services	Protects User Identity and System Integrity
• Benefits of SaaS (software-as-a-service) • Simple integration & agreements process • 24x7 user support • An account manager, integration support, etc.	• Platform that scales • Imperative to reach all members of the public • Reusable credential reduces friction to service delivery	• Privacy-preserving encryption model • FedRAMP compliant security controls • Anti-fraud program • Public sector accountability / transparency

Who We Serve

100 million user accounts

300+ million sign-ins annually

480+ live sites and services

48 agencies and states

Major Recent Announcements

New affordable pricing model going into effect on July 1st

In-person proofing recently graduated from the pilot phase

Login.gov will become fully compliant with the IAL2 level of NIST 800-63 in 2024

Learn more about these important milestones

Program Roadmap

	FY24 (Apr - Sep) Soon to deliver	FY25 Next on the docket	FY26 Expected direction
End User Impact	• Optional facial matching step for increased security and compliance • "Opt-In" for USPS in-person proofing • Additional languages	• Passports as evidence • Enhanced in-person proofing • Path to remote supervised • Equity study - targeted improvements via findings • A11y for low-vision / blind • Educational videos	• Mobile Driver's Licenses • New use cases supported (e.g. international users) • Enhanced multi-tiered IdV • Improved "My Account" experience / capabilities
Partner Support	• Improved dashboards • Identity working groups	• Self-service portal • Anti-fraud collaboration	• Expanded self-service portal • Shared research initiatives
Policy & Compliance	• NIST 800-63-3 compliance with Kantara TrustMark	• NIST 800-53 rev5 • Path to NIST 800-63-4	• Path to FedRAMP High • Deeper policy collaboration
Other	• Enhanced fraud controls* • Equity study notional results • Data infrastructure	• Enhanced fraud controls* • Additional identity vendors & targeted orchestration	• Enhanced fraud controls* • Ongoing platform improvements

Last Updated May 2024 – These are estimates and may be revised in the future; Login.gov will be transparent with partners about when / why this happens.

* Additional details are available upon request by agency partners

Program Roadmap
End User Impact

End User Impact

Partner Support

Policy & Compliance

The Login.gov User Journey

Creates a secure account with email + MFA

Reuses their credential across Government

| Initiate | Authenticate | Verify | Reuse |

Seeks access to a service provider's website

Verifies their identity remotely or in-person
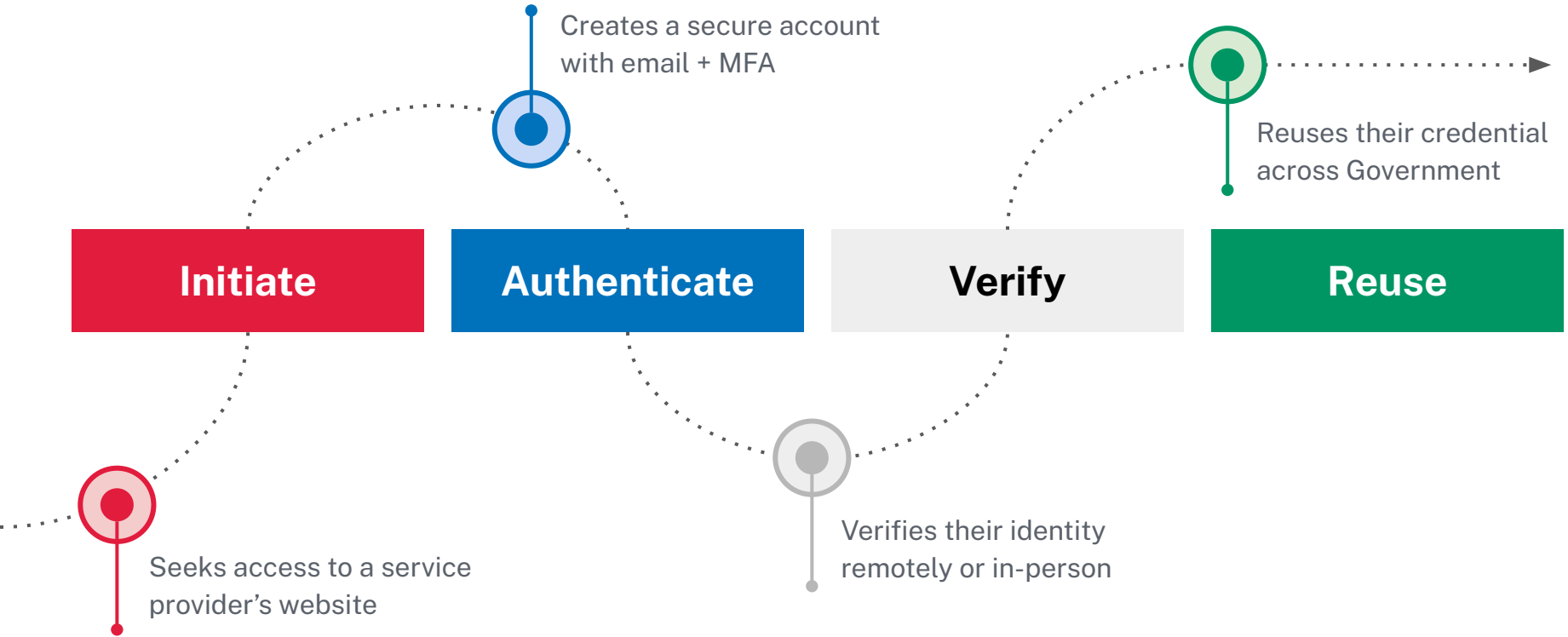
Importance of User Access

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

Access	Login.gov is addressing these top barriers
330M **Members of Public** *Needing services but with varying degrees of access*	**Lacking identity evidence** **1 in 10 adults** don't have a valid driver's license or state-issued ID[1] **Lacking authoritative records** **14% of US adults** are considered underbanked[2] **Lacking access (technological and geographic barriers)** **1 in 5 households** do not have internet access at home[3]

Sources: [1]CDCE [2]FDIC [3]NTIA

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.

99% **of the public live within 10 miles** of a USPS location[1].

While most people (97% during our pilot) prefer the convenience of remote proofing, IPP provides an accessible option to Login.gov users that need it.

We will be continuing to deepen our in-person proofing offering in FY25 and beyond.

[1]Source: <u>USPS</u>

Based on the IPP pilot findings:

More successful completions

81% Users followed through by visiting a USPS location after generating a barcode

16% Users that would have otherwise failed remote proofing were able to successfully verify their identity in-person

Security is still a priority

4% Users who visited a USPS location were turned away because of insufficient or invalid evidence, which is inline with expectations

Remote Supervised

- There are members of the public that want the opportunity to engage with a human during the identity verification process, but aren't able to visit an in-person proofing location to do so.

- We have begun exploring options that would enable a user to digitally verify their identity with a human agent, such as a **live video chat with a trained identity verification professional**.

- This channel presents interesting challenges, and we are pursuing this path while maintaining the program's high bar around security and privacy.
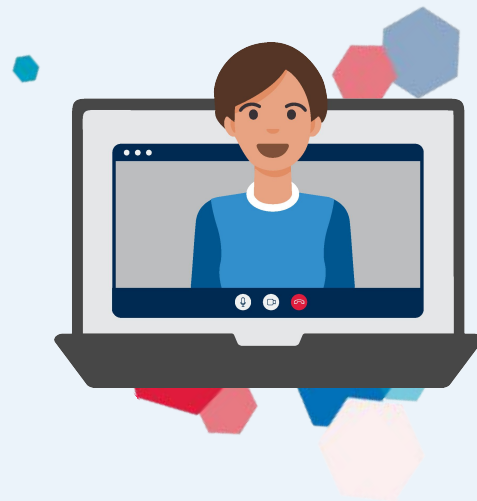
New Types of Identity Evidence

Challenge

The lack of reliable data sources that Login.gov can use to verify a person's identity for certain user populations.

The Login.gov program seeks to better understand use cases that are harder to support: international, unbanked, unhoused, minors, etc.

Next Up

- We'll be expanding our document collection process in order to accept and validate passports. 94% of U.S. adults have either a driver's license or a passport[1].

In Discovery

- We're collaborating with NIST and states via the NCCoE initiative to chart a path towards accepting mobile drivers licenses (mDLs)

- We're doing policy research around leveraging other types of identity evidence and proofing events (e.g. PIV cards).

[1]Source: CDCE

Accessibility

1 in 4 adults in the U.S. have some type of disability[1]

Login.gov is consistently **exploring new ways in which to perform testing and reporting of the accessibility of our product.** For example, we are assessing updated guidance in M-24-08 (Strengthening Digital Accessibility and the Management of Section 508 of the Rehabilitation Act)

Login.gov is in the **process of updating its Voluntary Product Accessibility (VPAT) Template** for its Authentication and Identity Verification services, which will be published on our website.

?

What's next?

Login.gov will explore new capabilities around **accessibility for low-vision and blind users** and others based on the findings from our ongoing testing and validation.

[1]Source: CDC

Language Support

Login.gov currently supports 3 languages:

English	**Spanish**	**French**

The program plans to expand the set of languages it supports in FY24 via:

- Login.gov website
- Help center articles
- Contact center support

Login.gov is working with the Department of State to **increase language support** and **simplify the translation process**.

Soon this will be reflected in **improved quality** of existing languages, and a **new language of Chinese (Simplified)**.

This will allow us to **accelerate the expansion to new languages**, which we'll share in a future update.

Educating the Public About Identity Issues

Login.gov will be investing in educational resources and tools to help users and encourage adoption. These include:

Videos explaining basic identity concepts and how to use Login.gov

Guidance for protecting their identity and what to do to mitigate fraud risks

GSA's Equity Study on Remote Identity Proofing

About

GSA is committed to investing in equitable service delivery. The GSA study on Remote Identity Proofing aims to understand how different methods to verify your identity relate to this goal. Login.gov will be thoughtfully incorporating the findings of this study into our processes and tools.

What's new

The **Equity Study on Remote Identity Proofing** asked participants to test five different vendor solutions. Participant recruitment ended in April 2024. The study will enable GSA to identify statistically significant differences in proofing failures that may be correlated with demographic bias in identity-proofing systems.

Next steps

GSA and an academic partner will be performing analysis to understand potential biases and areas of improvements for each step of the identity verification process. The peer-reviewed results, set to be released in FY25, will provide guidance to GSA and agencies government-wide in how they build to deliver better for the public.

Learn more about GSA's Equity Study on Remote Identity Proofing.

Program Roadmap
Partner Support

New Pricing Model (Available July 2024)

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

Goal

Develop a pricing model that is as affordable as possible, anchored in a sustainable financial model, and embodies our core values of equity, privacy, and transparency.

Fully Registered Login.gov Accounts
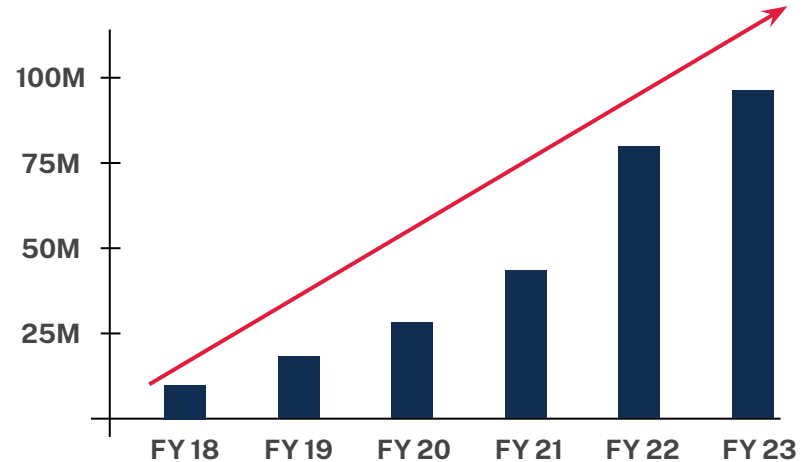
What's Changing?

1 Authentication

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

$0.10 per MAU* (starting price)

Savings as your agency scales

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

2 Identity Verification

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

$3 per user in a "proofing" year
$1 per user in a "non-proofing" year*

Savings up to 72%

*Based on a five year credential lifecycle

3 Base Price

The monthly base price will be lower than current plans, and more aligned with agency usage.

$2,500/month*

Savings up to 50%

*Transactional costs now count towards minimum, providing additional savings

Streamlined Partner Tools

During FY24, we will be making improvements to our existing dashboards, as well as beginning to build a new partner portal that will consolidate various partner-facing resources.

In Place Today
(Reporting & Dashboards)

Create and manage sandbox applications

Configure apps and request launches to production

Receive summary reports (e.g. # of users, billing costs)

Receive detailed reports (e.g. funnel drop-offs)

Submit tickets and read documentation

What's Next
(Self-Service Portal)

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

Manage access-control permissions

Drill into self-serve reports

Streamline the deployment process

View relevant alerts, tickets, etc.

Partner Advisory Group

This past year, Login.gov launched a new partner engagement channel called a "Partner Advisory Group" in order to garner 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.

Membership

This is an interagency group with rotating representation from the following stakeholders:

- **5-7** cabinet or large independent agencies representing key Login.gov user segments
- **1-2** small agency partners representing the needs of small agencies using Login.gov
- **1-2** SLTT partners representing the needs of State / Local / Territorial / Tribal entities using Login.gov

Each partner is expected to send **2-3** representatives to quarterly in-person meetings.

Future

- We are in the process of chartering a "Login.gov Working Group" concept in order to collaborate on specific Identity topics, starting with a Cybersecurity & Fraud focus.
- This will start out as part of the Partner Advisory Group, but we will be evaluating how to expand the scope to a broader audience.
- We are exploring other partner engagement channels, e.g. "Login.gov user groups".

Partner / Industry Outreach

Upcoming Speaking Events

- **ACT-IAC Emerging Technology and Innovation** *Digital Identity at the Speed of Change* panelist (5/20)

- **Identivation Summit** *Unlocking Secure and Seamless Service Delivery: Strategies for Digital Portals* panelist (5/21)

- **Identiverse**
    - *Fireside Chat with the Login.gov Director* (5/29)
    - *Providing and Quantifying Equitable Opportunities in Digital Identity* moderator (5/30)

- **Federal Identity Forum and Expo**
ID Infrastructure in a Hybrid World panelist (6/25)

Interested in participating in a panel or know of an upcoming event that Login.gov should participate in?

———————

Contact us at partners@login.gov

Program Roadmap
Policy & Compliance

End User Impact

Partner Support

Policy & Compliance
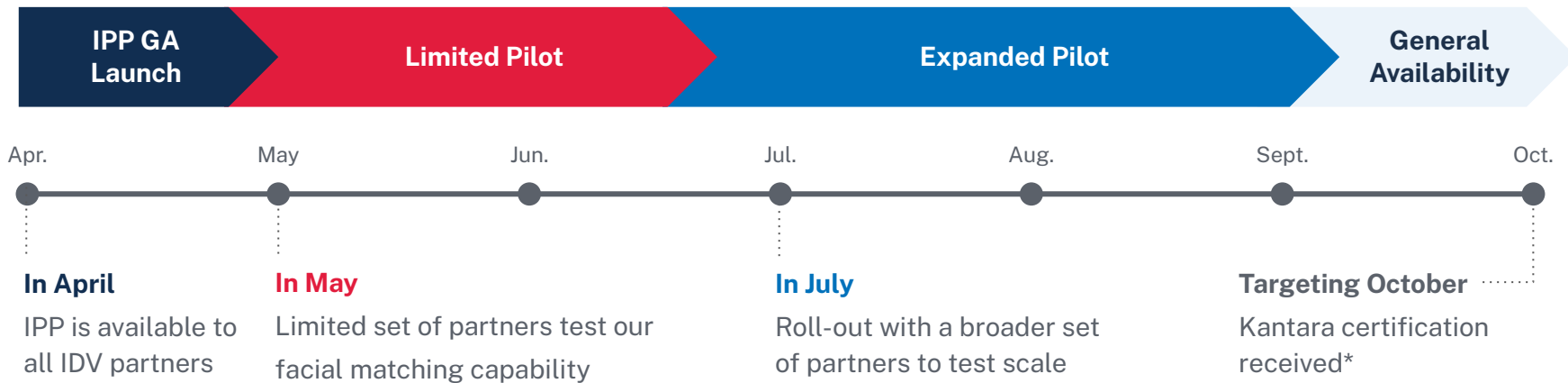
NIST 800-63-3 IAL2 Compliance

Login.gov has begun the Kantara assessment process for NIST SP 800-63-3 compliance at the IAL2 and AAL2 levels. The Kantara Initiative is a non-profit organization that operates an identity assurance program for assessing conformance against the NIST 800-63 standards. Once Login.gov receives the Kantara trust mark, the program will formally claim IAL2 compliance, and agencies will have the option of configuring a given application in one of three ways:

		Online-only Proofing Via your phone or computer	In-person Proofing Via a USPS location
A.	Authentication-only (i.e. no identity verification)	N/A	N/A
B.	Non-IAL2 identity verification (i.e. the existing Login.gov solution)	✔ (without a facial-matching step)	✔
C.	IAL2-compliant identity verification (i.e. the new service offering)	✔ (with a facial-matching step)	✔

This approach gives more integration options to partners and more access options for users

IAL2 Launch Plan

Login.gov will launch a pilot using proven facial matching technology, allowing users to match a live selfie with the photo on a self-supplied form of photo ID, such as a driver's license.

| IPP GA Launch | Limited Pilot | Expanded Pilot | General Availability |

Apr. — May — Jun. — Jul. — Aug. — Sept. — Oct.

In April
IPP is available to all IDV partners

In May
Limited set of partners test our facial matching capability

In July
Roll-out with a broader set of partners to test scale

Targeting October
Kantara certification received*

* Timing depends on 3rd party assessment schedule, which isn't within Login.gov's control

NIST Compliance Path Forward

Login.gov is developing new capabilities in accordance with NIST SP 800-63 Revision 3, and is excited to be a part of the NIST SP 800-63 Revision 4 publication process.

FY24 Delivery	**COMPLETED** In-person identity verification at a local Post Office, available as an upfront option for all users	**DELIVERING SOON** Digital identity verification using proven facial matching technology to verify that you match your own identification
FY24 Discovery	**IN DISCOVERY** Digital identity verification that does not require automated facial matching, such as a live video chat with a trained identity verification professional	**IN DISCUSSIONS** Digital identity verification that builds upon promising new technologies such as mobile drivers licenses (mDLs) and verifiable credentials

Login.gov will also be working towards NIST 800-53 rev5 compliance for additional security and privacy controls in order to meet Federal Information Security Management Act (FISMA) requirements.

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 also ensuring equity and access is more important than ever.

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 compares "selfies" exclusively with the user's photo ID
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 invest in academic-quality research, such as GSA's Equity Study on Remote Identity Proofing, to measure all aspects of Login.gov's performance, including algorithmic bias across demographic factors

Anti-fraud Investments

Login.gov's Fraud Operations Team implements a variety of fraud controls and investigative techniques in order 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.

Phone number

State ID / driver's license number

Social Security number

Mailing address

Device / IP address

Other controls

⭐ 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

Next Steps

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 fix issues and develop new capabilities.

Our team **follows agile practices** and deploys code to production every two weeks.

We believe in **continuous improvement** and employ a variety of methods to learn and grow. We stay ahead of emerging technologies and federal policies.

We Value Your Feedback

We will update and re-share this artifact quarterly, 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.