Login.gov

Program Roadmap

LOGIN.GOV

December 2024

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.

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” provides government agencies, members of the public, and the government-at-large with a variety of benefits.

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

Role in Government

The public's “one account for government”

Each agency's “public option” for Identity

A key piece of national infrastructure

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

Challenge of Identity in America

Fragmentation

Fragmentation by

- Level of Government - Federal / State / County / Local
- Agency - Multiple programs, overlapping services, etc.

Pain points for the public

- Creating multiple user accounts
- Unnecessarily siloed information
- Varying degrees of security

Challenge of Identity in Government Services

Increasing access while preventing fraud

Access

330M

Members of Public

Needing services but with varying degrees of access

Fraud

$7.7B

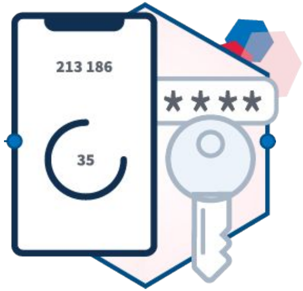
Improper Payments

*In FY 2021 attributed to identity issues**

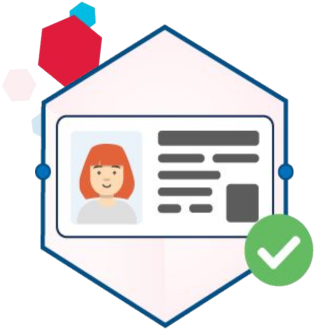
** Based on a 2022 JFMIP report*

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 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

Expands 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 and 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

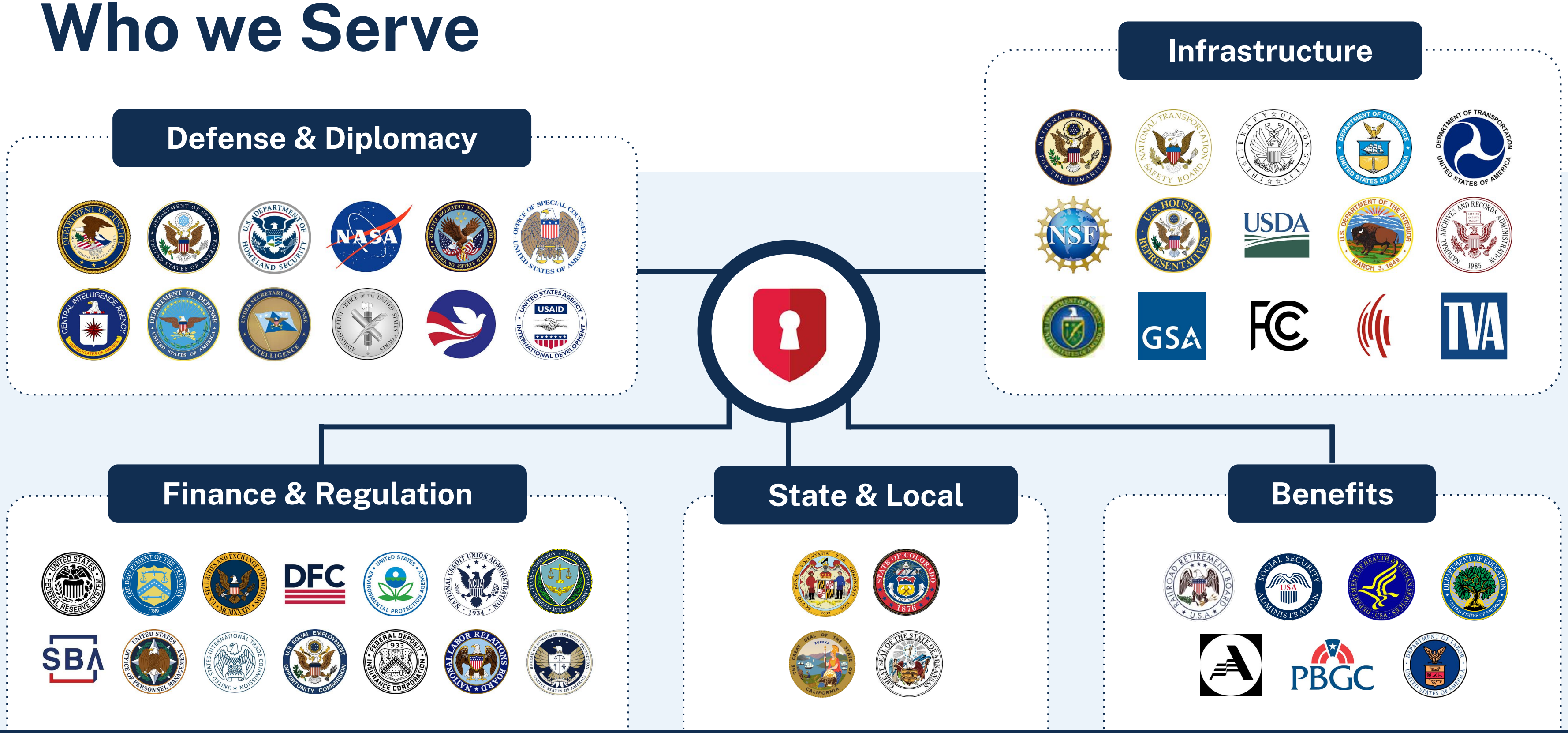
Better Support

- Multiple choices for MFA (multi-factor authentication), identity proofing, etc.
- A “serve everyone” mindset 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

Who we Serve



Defense & Diplomacy

Infrastructure

Finance & Regulation

State & Local

Benefits

100+ million user accounts | **400+** million sign-ins annually | **600+** live sites and services | **52** agencies and states

Now Offering IAL2 Enhanced Identity Verification

Convenience

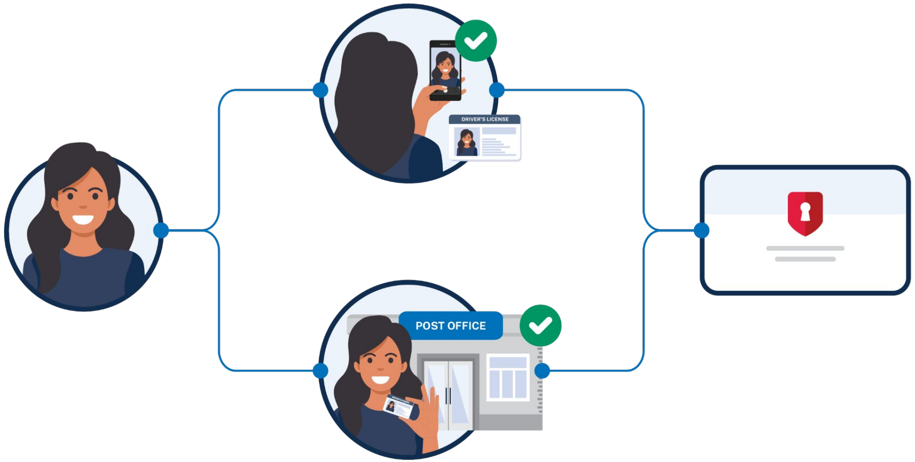
Enables users to easily prove their identity from their phone or in person

Security

Adds additional fraud checks to protect agency systems and user identities

Privacy

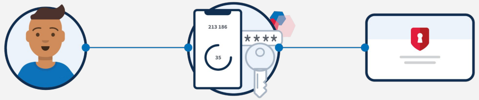
Maintains Login.gov's commitments to protecting user data



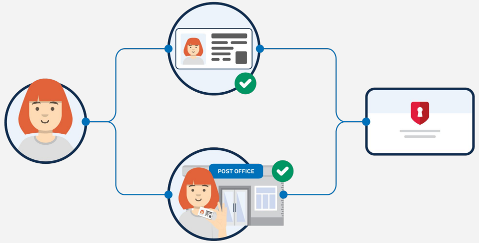
Our Updated Service Offerings

We have successfully completed the independent Kantara assessment process for National Institute of Standards & Technology (NIST) SP 800-63-3 compliance at the IAL2 and AAL2 levels. As a result, Login.gov is now able to offer even more integration options to partners and access options for users.

Authentication-only

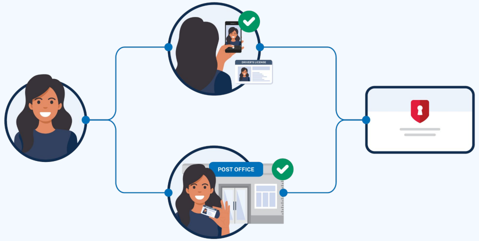


Basic identity verification



NEW

IAL2-compliant identity verification



?

Learn more about this important milestone and **reach out** to your account management team if you’re interested in IAL2 identity verification for your agency

Other FY24 Accomplishments

Introduced new affordable pricing model to help agencies scale their adoption

UNITED STATES POSTAL SERVICE®

Added In-Person Proofing (IPP) which is available at thousands of participating USPS locations

Launched new language support to simplify the translation process and add new languages like Chinese (Simplified)

Program Roadmap

	FY25 (Oct - Mar) Soon to deliver	**FY25 (Apr - Sep)** Next on the docket	**FY26** Expected direction
End User Impact	• New fraud controls to further protect against identity theft • More seamless handoff to agency applications • A11y for low-vision/blind users • Educational videos	• Passports as evidence during identity verification • Enhanced attended identity verification • Improved account recovery and management	• Mobile Driver's Licenses • New use cases supported (e.g. international users) • Enhanced multi-tiered IdV • Continued UX investments across the full user journey
Partner Support	• Improved reporting • Identity working groups	• Self-service portal • Anti-fraud data sharing APIs	• Expanded self-service portal • Shared research initiatives
Policy & Compliance	• Compliant to latest NIST 800-53 requirements (rev 5) • NIST 800-63 assurance level framework for agencies	• Path to NIST 800-63-4 • Deeper policy collaboration	• Additional FedRAMP High security controls
Other	• Additional identity vendors & private sector partnerships	• Deeper anti-fraud analytics and investigative tools	• More data sources to inform anti-fraud efforts

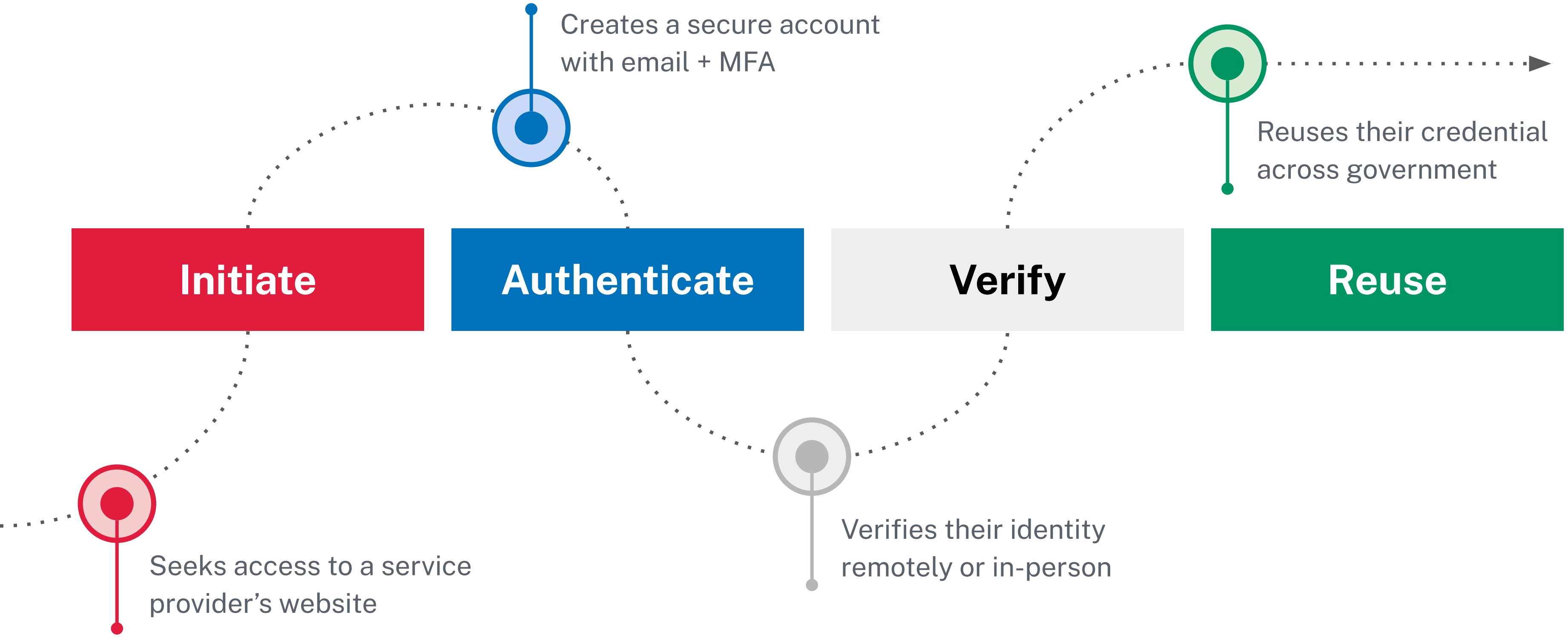
Last Updated Dec 2024 – These are estimates and may be revised in the future; Login.gov will be transparent with partners about when / why this happens.

Program Roadmap

End User Impact

- End User Impact
- Partner Support
- Policy & Compliance

The Login.gov User Journey



Initiate

Seeks access to a service provider's website

Authenticate

Creates a secure account with email + MFA

Verify

Verifies their identity remotely or in-person

Reuse

Reuses their credential across government

Importance of User Access

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

Access

330M

Members of Public
Needing services but with varying degrees of access

Login.gov is addressing these top barriers

●○○○○
○○○○○

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

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].

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.

We are continuing to invest in our IPP offering in FY25 and beyond.

Source: [1]USPS

IPP is one way we provide user access while preventing fraud:

More successful completions

21% Users that would have otherwise failed remote proofing were able to successfully verify their identity in-person

85% Users followed through by visiting a USPS location after generating a barcode

15 hrs Users visit a USPS location within a day of starting the process – 15 hours on average.

Security is still a priority

1% Users who visited a USPS location and were turned away because of insufficient or invalid evidence, which is in line with expectations

Remote Attended Workflow

- Some members of the public want the opportunity to engage with a human during the identity verification process, but aren’t able to visit an IPP 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

Login.gov is expanding the types of evidence[1] it can use to verify a person's identity.

★ NEW

Passports

In FY25, we're expanding our document collection process in order to accept and validate U.S. passports.

94% of U.S. adults have either a driver's license or a passport[2].

In Discovery

Mobile Driver's Licenses (mDLs)

In FY25, we're actively collaborating with NIST and states via the NCCoE initiative to chart a path towards accepting mobile driver's licenses (mDLs)

[1] The lack of reliable, available data sources makes this difficult. We continue to prioritize pathways for more use cases (i.e. international, unbanked, unhoused, minors, etc.)
[2] Source: CDCE

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 2023, American adults lost a total of $43 billion to identity fraud[1] with victims 80+ experiencing 3-4 times higher median losses than the 20-49 age group[2]

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

Time Lost to Recovery

6+ months and 200 hours to recover from identity theft[3]

Psychological Impact

Per ITRC, 87% of victims report feeling anxious or worried, 77% felt violated, and 16% reported feeling suicidal after becoming victims of this crime[4]

Sources: [1]AARP, [2]DeLiema et al, [3]FTC, [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.

Anti-Fraud Investments in FY25 and Beyond

TOOLS & DATA

New tools and data sources for fraud detection and prevention

COLLABORATION

Fraud signal sharing with agencies via data APIs and working groups

EDUCATION

More information and guidance for partners and users to be vigilant about where and how fraud may occur

Educating the Public About Identity Issues

Login.gov is investing in educational resources and tools to help users understand fraud risks and encourage adoption. These include:

Videos explaining basic identity concepts (identity verification, MFA, fraud, etc.) and how to use Login.gov

Guidance for protecting their identity and what to do to mitigate fraud risks, including how to spot social engineering tactics

Program Roadmap

Partner Support

End User Impact

Partner Support

Policy & Compliance

New 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

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

2 Identity Verification

Identity verification prices are oriented around a user's "credential lifecycle" and are 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 is lower than previous plans, and more aligned with agency usage.

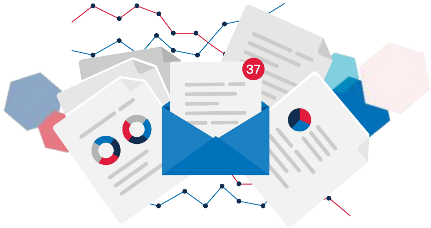
$2,500/month*

Savings up to 50%

*Transactional costs now count towards minimum, providing additional savings

Streamlined Partner Tools

In FY25, we will be launching a partner portal that consolidates 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

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.

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 small agencies using Login.gov
- **1-2** SLTT partners representing State / Local / Territorial / Tribal entities using Login.gov

In FY25

- We are standing up a cross-agency Cybersecurity & Anti-fraud working group
- We are collaborating with NIST, FIDO, and others in industry forums
- We are exploring other partner engagement channels, e.g. "Login.gov user groups"

Partnering with Industry to Accelerate Innovation

Login.gov harnesses best-in-class private sector technologies to stay ahead of evolving threats. As a shared service / single sign-on (SSO) serving 50+ agencies and 100M+ users, Login.gov enables cutting-edge solutions to reach 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. We recently completed a large-scale acquisition process to procure the next-generation of identity proofing capabilities, with 50% of awards going to small businesses.

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.

Partner / Industry Outreach

Upcoming Events

A few of the events we're excited to attend in 2025:

- **ACT-IAC Emerging Technology and Innovation** (5/4)
- **Code for America Summit** (5/29)
- **Federal Identity Forum and Expo** (6/1)
- **Identiverse** (6/3)
- **Identity Week** (9/1)
- **BenCon** (9/1)
- **FIDO Authenticate Conference** (TBA)

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 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 Focus	**COMPLETED** IPP identity verification at a local Post Office, available as an upfront option for all users	**COMPLETED** Digital identity verification using proven facial matching technology to verify that you match your own identification
FY25 Focus	**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 DISCOVERY** Digital identity verification that builds upon promising new technologies such as mDLs and verifiable credentials

Login.gov has achieved NIST 800-53 rev5 compliance for additional security and privacy controls, and meets 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 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 engage agency partners via anti-fraud collaboration, incorporate private sector best practices, and invest in academic-quality research to use emerging technologies responsibly

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 quickly adopt emerging technologies and federal policies.

We Value Your Feedback

We will 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.

LOGIN.GOV