Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in the United States

COUNTRY United States

INDUSTRY Government & Public Services

LAST UPDATED 16 October 2026

KEY REGULATORS Office of Management and Budget · National Institute of Standards and Technology · General Services Administration

Key takeaways

- No licence is needed to sell identity verification to US public bodies, but federal agencies may only rely on providers that meet the National Institute of Standards and Technology (NIST) digital identity guidelines, now in their fourth revision (SP 800-63-4, final July 2025).
- Since 31 August 2026, the White House budget office requires federal agencies to offer Login.gov, the government's own sign-on service, on public websites and to use it for identity checks unless it cannot meet a service's needs; other providers are allowed only alongside it for specific gaps. A September 2026 executive order also makes Login.gov the sign-in for the new America.gov portal.
- Remote, fully online identity proofing is permitted at the standard and middle assurance levels, and the middle level does not require a selfie: a mailed code or a video call with a trained agent can replace face matching. The highest level still requires an in-person session.
- Knowledge-based questions ("which street did you live on?") can no longer be used to verify identity, and remote providers must detect deepfakes, injected video and virtual cameras.
- Banking anti-money laundering rules do not apply; the binding rules come from federal IT security law, budget office policy, the Privacy Act and procurement contracts, and false claims of compliance can lead to False Claims Act liability.

The US public sector is open to digital identity providers, but it is a policy-driven market rather than a licensed one. Federal agencies are bound by the Federal Information Security Modernization Act and by Office of Management and Budget (OMB) memoranda, which make the NIST guidelines mandatory for agency services. Vendors reach those agencies as credential service providers, as components inside Login.gov, or as contractors to state programmes.

The principal authorities are OMB, NIST and the General Services Administration (GSA), which runs Login.gov, with the Department of Homeland Security (DHS) and its Transportation Security Administration (TSA) governing mobile driver's licences for federal purposes.

The biggest obstacle for a new entrant is OMB Memorandum M-26-18: it makes Login.gov the default for federal public services, and Executive Order 14432 reinforces that by routing high-volume services through America.gov with Login.gov sign-in. Commercial providers must show a gap that Login.gov cannot fill, or supply technology to Login.gov itself.

CONTENTS

1 Who regulates this sector
2 Licensing and authorisation
3 Identity framework (AML rules do not apply)
4 Identity verification and onboarding
5 Digital channels: what's different
6 Data protection and biometrics
7 Sector-specific obligations
8 Risk indicators and red flags
9 Enforcement and penalties
10 Recent changes and what to watch
11 What this means for identity verification
- Sources

1 Who regulates this sector

There is no single digital identity regulator in the United States. Federal agencies set and enforce identity requirements for their own services, and states issue the underlying credentials. The table lists the bodies that shape identity verification for public services.

Authority	Remit	Level	Official site
Office of Management and Budget (OMB)	Binding identity, credential and access management policy for federal agencies (M-19-17, M-22-09, M-26-18)	Federal	whitehouse.gov/omb
National Institute of Standards and Technology (NIST)	Digital Identity Guidelines (SP 800-63-4) and the PIV standard (FIPS 201-3); standard-setter, not an enforcer	Federal	csrc.nist.gov
General Services Administration (GSA)	Operates Login.gov, the shared sign-on and identity verification service	Federal	login.gov
Transportation Security Administration (TSA), within DHS	Administers REAL ID, including waivers allowing federal acceptance of state mobile driver's licences	Federal	tsa.gov
U.S. Citizenship and Immigration Services (USCIS), within DHS	Form I-9 and E-Verify employment eligibility verification	Federal	uscis.gov

Social Security Administration (SSA)	Authoritative source for Social Security number validation	Federal	ssa.gov
Department of Justice (DOJ)	Civil and criminal enforcement, including False Claims Act cases against contractors	Federal	justice.gov
State motor vehicle agencies	Issue driver's licences, identity cards and mobile driver's licences	State	Each state's own site

State benefit agencies and state privacy authorities set their own identity rules for state programmes; those vary by state and are not surveyed here.

2 Licensing and authorisation

No federal licence or registration is required to offer identity proofing or authentication to government bodies. Market access is controlled through three other routes.

Agency policy

OMB Memorandum M-26-18 (31 August 2026) requires agencies to offer Login.gov as a sign-on option on in-scope public websites and to use Login.gov identity verification unless it does not meet a service's user base, risk profile or operations. Other solutions may be offered alongside it only to cover use cases Login.gov cannot meet or to avoid burdening existing users, and agencies must phase out the rest.

Assurance and assessment

A credential service provider must operate under a documented practice statement covering every proofing step, evidence type, technology, fraud programme and retention policy, and make it available to the agencies relying on it (SP 800-63A-4, section 3.1). Login.gov itself states that its services are assessed by an independent third party against the NIST levels, and M-26-18 asks Login.gov to maintain such an assessment.

Procurement

Under M-19-17, agencies must buy identity and credentialing products that comply with OMB policy and NIST standards, and contracts giving contractors access to federal systems or facilities must require compliance with HSPD-12 and FIPS 201.

For state-issued mobile driver's licences, the gate sits with the state: federal agencies may accept a state's mobile licence for REAL ID official purposes only if TSA has granted that state a waiver under 6 CFR 37.7, valid for three years.

3 Identity framework (AML rules do not apply)

Government agencies, and the identity providers serving them, are not financial institutions under the Bank Secrecy Act regulations, so there is no customer identification programme, suspicious activity reporting or beneficial ownership duty for this sector. Identity assurance for public services is governed by a layered federal framework instead.

Layer	Instrument	What it requires	Status
Policy	OMB M-19-17 (May 2019)	Agencies must implement NIST SP 800-63-3 "and any successive versions", select assurance levels through digital identity risk management, and limit personal data collection	`In force, section V.5 superseded by M-26-18`

Policy	OMB M-22-09 (January 2022)	Phishing-resistant multi-factor authentication for agency staff, contractors and partners; a phishing-resistant option for public users	In force
Policy	OMB M-26-18 (31 August 2026)	Login.gov as universal sign-on; risk management under SP 800-63-4; reuse of verified credentials	In force, phased deadlines
Standard	NIST SP 800-63-4 (July 2025)	Identity, authenticator and federation assurance levels; supersedes SP 800-63-3	In force
Standard	FIPS 201-3 (January 2022)	PIV credentials for federal employees and contractors under HSPD-12	In force

Two points about the current revision are often misreported. First, self-asserted identity now sits outside the assurance levels entirely: SP 800-63A-4 defines a "no identity proofing" tier, and the lowest level, IAL1, requires real proofing, with every core attribute validated against an authoritative or credible source. Second, SP 800-63-4 is written for federal systems; it binds private and state services only where a law, contract or agency agreement adopts it.

4 Identity verification and onboarding

SP 800-63A-4 sets three identity assurance levels (IALs). At every level the provider must collect a government identifier (such as a Social Security, driver's licence or passport number) and should collect name, date of birth and a postal or digital address.

Level	Evidence	Verification	Where it can happen
IAL1	One piece of fair evidence that can be digitally validated or has a photo, or one strong or superior piece	Code to a validated address, micro-deposit, federated login at AAL2/ FAL2, or face comparison; biometrics optional	Any proofing type, including remote unattended
IAL2	Fair plus strong, two strong, or one superior (cryptographically signed) piece	Non-biometric, biometric or digital evidence pathway	Any proofing type, including remote unattended
IAL3	As IAL2, plus collection of at least one biometric	Trained proofing agent in an attended on-site session	On-site attended only (a CSP-controlled kiosk with a remote agent qualifies)

Controls that apply across levels include:

- Knowledge-based verification is prohibited as a means of identity verification; it may still feed a provider's fraud programme.
- Every proofing process must include a death records check, and providers must analyse remote channels for high-risk indicators such as blocklisted proxies.
- Automated document validation must reach a document false acceptance rate and false rejection rate of 0.1 or less, use live capture with document presence checks, and compare the machine-readable zone or barcode with the printed data.
- Biometric verification must achieve a false match rate of 1 in 10,000 or better and a false non-match rate of 1 in 100 or better, with no demographic group (sex, age and skin tone, where they affect performance) performing more than 25% worse than the overall population. Remote capture needs presentation attack detection tested under ISO/IEC 30107-3:2023 with an impostor attack accept rate below 0.07.
- After successful proofing, a notification must be sent to a validated postal address or phone number (email is allowed at IAL1 only), explaining how to dispute the enrolment.

- The Social Security Administration's electronic consent-based SSN check returns a yes or no match, with a death indicator, but is open only to financial institutions and their service providers, with the number holder's written consent.
- Providers should offer trusted referees for applicants who cannot complete the standard flow, and must support applicant references for people under 18.

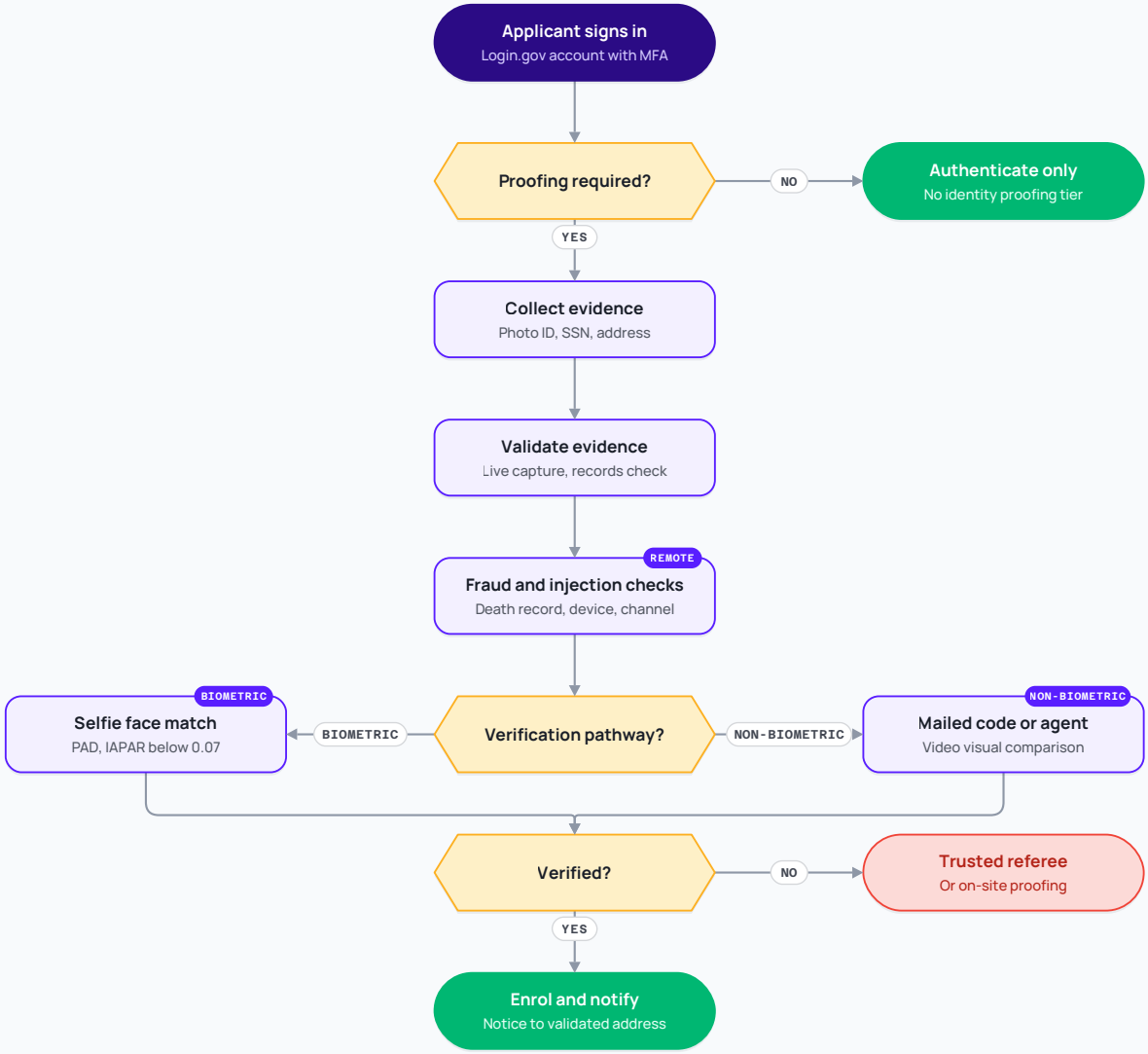


Figure 1. Remote unattended identity proofing for a federal public service at IAL2 under NIST SP 800-63-4.

5 Digital channels: what's different

Bottom line: remote proofing is fully permitted up to IAL2, but it carries extra technical duties (injection and deepfake detection, channel analysis, live capture) that on-site proofing does not, and IAL3 cannot be achieved remotely.

Requirement	In person / on-site	Online / remote	Difference
Highest achievable level	IAL3	IAL2	Differs
Biometric at IAL2	Optional	Optional (non-biometric and digital evidence pathways)	Same
Evidence validation	Physical and tactile inspection by trained agent	Automated doc validation with live capture, or agent visual inspection on video	Differs
Deepfake and injection controls	Operator inspects the biometric source	Genuine-sensor checks, media forgery analysis; random cues in video sessions	Differs
Channel risk analysis	Not applicable	Mandatory review of remote channels (proxies, IP addresses)	Differs
Death records check and proofing notification	Required	Required	Same
Mobile driver's licence for REAL ID purposes	Accepted with an ISO/IEC 18013-5 reader if the state holds a TSA waiver	Unattended remote presentation is not a REAL ID use case	Differs
Form I-9 document examination	Physical examination	Live video alternative for E-Verify employers in good standing only	Differs

Remote IAL2 without a selfie

SP 800-63A-4 offers three IAL2 pathways and lets providers combine them. The non-biometric pathway accepts a confirmation code sent to a validated postal address or phone number, or a visual comparison by a proofing agent, including in a live video session. Providers offering several pathways must record which one each subscriber used and pass that to relying agencies. Confirmation codes expire after 10 minutes by SMS or voice, 24 hours by email and 21 days by post within the contiguous United States.

Recorded video sessions

Video recording of remote attended sessions is optional and must follow a privacy risk assessment. If a session is recorded, the applicant must be notified and consent beforehand, and the provider must publish its retention schedule and deletion process for video records.

Mobile driver's licences

Under the REAL ID waiver rule (89 FR 85340, effective 25 November 2024), an agency accepting a mobile licence must confirm the state's waiver, read the credential with a reader that validates it under ISO/IEC 18013-5:2021, and check that the underlying physical card is REAL ID compliant. The rule covers attended presentation only and applies solely to REAL ID official purposes, such as boarding aircraft and entering federal facilities, not to benefit applications. TSA has described it as a temporary first phase before comprehensive mobile licence rules.

Remote employment verification

Employers that participate in E-Verify in good standing may examine Form I-9 documents remotely by reviewing copies and then holding a live video call, retaining clear copies of the documents. Employers outside E-Verify must examine documents physically.

6 Data protection and biometrics

There is no single federal data protection statute or authority in the United States. For federal identity services, the Privacy Act of 1974 and the E-Government Act of 2002 do the work: agencies must consult their Senior Agency Official for Privacy, publish a System of Records Notice and a Privacy Impact Assessment where applicable, and conduct their own assessment even when using an external provider.

SP 800-63A-4 adds provider-level rules. Biometrics require explicit informed consent, recorded against the subscriber's account, and a public statement of what biometric data is collected, how it is stored and how to remove it. Providers must publish a default retention period and deletion process and should honour deletion requests unless law or policy prevents it. Social Security numbers may be collected for identity resolution, but knowing the number is not evidence of identity. Personal data processing must be limited to what proofing, fraud mitigation and relying party needs require.

State biometric privacy laws, including those in Illinois, Texas and Washington, can apply to providers that capture biometrics from residents of those states.

7 Sector-specific obligations

Login.gov as the default for public services

Since 2015, 6 U.S.C. 1523(b)(1)(D) has required each agency to implement the GSA-developed single sign-on platform for public websites that require user authentication, unless the agency head personally certifies with particularity that it would be excessively burdensome and unnecessary and sends that certification to Congress. M-26-18 enforces that duty: an agency that cannot meet a deadline must notify OMB with that personal certification. It does not apply to sites used only by organisations or by people acting for someone else, and it exempts the Department of War, national security systems and the intelligence community. Where agencies need extra anti-fraud controls, they should add them inside their own systems rather than reject Login.gov credentials.

Executive Order 14432 (29 September 2026) directs GSA to run America.gov as the single online entry point for covered services, defined as public-facing services with more than 100,000 users in a 12-month period, excluding IRS tax filing, the Department of War and the intelligence community. Login.gov is to be America.gov's authentication service, and agencies must complete Login.gov integration consistent with the statute and M-26-18. The order keeps in-person, telephone, mail and agency-specific digital routes open, so offline proofing channels remain part of the picture.

Authentication for the workforce and the public

At AAL2, verifiers must offer at least one phishing-resistant option, and federal agencies must require phishing-resistant authentication for staff, contractors and partners. AAL3 requires a cryptographic authenticator with a non-exportable private key, so synced passkeys cannot be used at that level. Agencies must select at least AAL2 whenever personal information is made available online. M-22-09 also bars password rules that force

special characters or regular rotation, and SP 800-63B-4 requires at least 15 characters for single-factor passwords.

Post-quantum migration

Executive Order 14412 (22 June 2026) directs OMB to require agencies to move high value assets and high impact systems to post-quantum key establishment by 31 December 2030 and post-quantum digital signatures by 31 December 2031, and directs the FAR Council to propose contractor requirements. Digital signatures underpin PIV certificates, mobile licences and federated assertions, so identity vendors should plan for this.

8 Risk indicators and red flags

IDENTITY FRAUD INDICATORS NAMED IN NIST SP 800-63A-4

- **Recent SIM swap or number port**: the phone used for proofing has just moved to a new user or device.
- **Short account tenure**: phone or email account recently created or heavily modified.
- **High-risk mailing address**: a virtual PO box or similar address type.
- **Deceased identity**: claimed identity matches a death record.
- **Data washing**: repeated attempts that tune stolen attributes until they pass validation.
- **Injected or forged media**: virtual cameras, emulators, jailbroken devices or deepfake artefacts.
- **Velocity anomalies**: unusual IP addresses, geolocations or volumes of enrolments from one device.

9 Enforcement and penalties

NIST guidelines and OMB memoranda carry no civil penalties of their own. They bind agencies through federal IT security law and OMB oversight, and they reach vendors through contracts and trust agreements. Consequences therefore take three forms.

- **Contract and False Claims Act exposure.** DOJ uses the False Claims Act against contractors that misrepresent compliance with cybersecurity standards. In July 2025

Illumina agreed to pay $9.8 million to resolve allegations that it sold systems to federal agencies while falsely representing adherence to NIST and ISO standards; The whistleblower received $1.9 million, and the settlement involved no determination of liability.

- **Loss of acceptance.** TSA may suspend or terminate a state's mobile licence waiver, removing it from the list federal agencies rely on, including for a reportable cyber incident that must be notified within 72 hours.
- **Agency accountability.** Under M-26-18, an agency that cannot deploy Login.gov by the deadlines must file a notice with OMB carrying a personal certification from the agency head, shared with congressional committees.

10 Recent changes and what to watch

- **29 September 2026, Executive Order 14432** `In force`: establishes America.gov with Login.gov as its sign-in; an OMB implementation memorandum is due within 90 days, by the end of December 2026.
- **31 August 2026, OMB M-26-18** `In force`: agencies must inventory authenticated public websites within 60 days, run SP 800-63-4 risk management within 240 days, deploy Login.gov on high impact services within one year and on all in-scope sites within two years.
- **22 June 2026, Executive Order 14412** `In force`: post-quantum deadlines for federal systems; a FAR proposed rule for contractors is due within 180 days.
- **31 July 2025, NIST SP 800-63-4** `In force`: replaces SP 800-63-3, with new fraud, injection-attack and syncable authenticator rules; Login.gov is being reassessed against it.
- **6 June 2025, Executive Order 14306** `In force`: removed the January 2025 directions encouraging agencies to accept digital identity documents for public benefits.
- **7 May 2025, REAL ID card-based enforcement** `Waiver available`: mobile licences accepted only from states holding a TSA waiver; TSA has not yet published the comprehensive second-phase rule it described (as of October 2026).

11 What this means for identity verification

A provider serving US public bodies should design to SP 800-63-4, not the 2017 revision still quoted in many requirements documents. In practice that means offering more than one IAL2 pathway, including a non-biometric route; dropping knowledge-based questions from

verification; running a death records check on every applicant; and building injection and forged-media detection into both selfie and video flows. Document and biometric engines need independent test results published, with demographic performance shown. Providers should be ready to accept mobile driver's licences and other signed digital evidence, which can count as superior evidence when its issuance meets NIST criteria and its signature is cryptographically validated, and to document every deviation in a Digital Identity Acceptance Statement. Retention and deletion policies, biometric consent records and proofing notifications to a validated address are product features, not paperwork. Commercial providers should plan around Login.gov rather than against it, focusing on populations and risk profiles that M-26-18 recognises it may not serve.

IDENTOMAT

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Remote identity proofing with ID document capture and verification, including NFC chip reading of e-passports.
- Biometric liveness and face match to support a biometric verification pathway, alongside video KYC with trained agents for a non-biometric route.
- Phone and email verification for validated addresses used in proofing notifications and confirmation codes.
- No-code workflow builder to configure separate assurance-level flows, with cloud, on-premises or hybrid deployment for public-sector hosting needs.

Request a meeting

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **NIST SP 800-63-4, Digital Identity Guidelines**, July 2025, supersedes SP 800-63-3, csrc.nist.gov
- **NIST SP 800-63A-4, Identity Proofing and Enrollment**, July 2025, sections 1.2, 2, 3 and 4, pages.nist.gov (PDF edition via doi.org/10.6028/NIST.SP.800-63A-4)
- **NIST SP 800-63B-4, Authentication and Authenticator Management**, July 2025, sections 2 and 3, pages.nist.gov
- **NIST FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors**, January 2022, csrc.nist.gov
- **OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management**, 21 May 2019, whitehouse.gov
- **OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles**, 26 January 2022, section III.A, whitehouse.gov
- **OMB Memorandum M-26-18, Scaling Use of Login.gov to Deliver a Universal Sign-on for Public Services**, 31 August 2026, whitehouse.gov
- **Executive Order 14144, Strengthening and Promoting Innovation in the Nation's Cybersecurity**, 90 FR 6755, 17 January 2025, federalregister.gov
- **Executive Order 14306, Sustaining Select Efforts To Strengthen the Nation's Cybersecurity**, 90 FR 24723, 11 June 2025, govinfo.gov
- **6 U.S.C. 1523, Federal cybersecurity requirements**, United States Code 2024 edition, subsection (b), govinfo.gov
- **Executive Order 14432, Streamlining Access to Government Services Through America.gov**, 91 FR 63121, 2 October 2026, federalregister.gov
- **Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks**, 91 FR 38483, 25 June 2026, federalregister.gov
- **TSA final rule, Waiver for Mobile Driver's Licenses (6 CFR Part 37)**, 89 FR 85340, 25 October 2024, govinfo.gov
- **USCIS, Remote Examination of Documents (Optional Alternative Procedure)**, I-9 Central, uscis.gov
- **Login.gov, Our services (partner service levels)**, login.gov
- **SSA, electronic Consent Based SSN Verification (eCBSV) Service**, ssa.gov
- **DOJ, Illumina Inc. to Pay $9.8M to Resolve False Claims Act Allegations**, 31 July 2025, justice.gov