

ISAE Product Requirements Specification

Immigration Support and Enforcement: Enrollee App, Agent Triage Dashboard, Caseload Management, and Supervisor Analytics

Based on the ISAE proposal by Alfred Holzheu and the ISAE policy white paper (October 2026)

Version 0.4 (Draft for review), October 2026

Prepared for government program, legal, privacy, and product teams. Factual figures are reused from the verified ISAE white paper and footnoted; parameters marked Proposed are design defaults pending approval.

Document Control

Item	Detail
Document	ISAE Product Requirements Specification (PRS)
Version / status	0.4, draft for government, legal, privacy, and product review. v0.2 adds field enrollment, the Temporary Digital ID, and the one-time enrollment background check (Section 6.9), per the proposal owner's October 2026 decision. v0.3 adds the Translate / Traducir helper (Section 6.10). v0.4 adds the Language Strategy (Section 6.11, LANG-01 to LANG-14).
Proposal owner	Alfred Holzheu (original ISAE proposal)
Source of record	<i>ISAE: Immigration Support and Enforcement white paper (October 2026). All factual figures in this spec are taken from that paper and carry its footnotes. Exception: Section 6.11 (Language Strategy) cites additional public sources, listed as [L1]–[L6] at the end of that section.</i>
Intended readers	DHS/ICE program leadership, product and engineering teams, DHS Privacy Office, Office for Civil Rights and Civil Liberties (CRCL), Office of the General Counsel, Inspector General staff, contracting officers, and pilot-site partners
Required approvals before pilot	Privacy Impact Assessment (PIA) and System of Records Notice (SORN); legal sufficiency review; CRCL review; security Authority to Operate (ATO); signed inter-agency agreements (Section 11)

How to read this document.

- **MUST / MUST NOT** are binding requirements. **SHOULD** is a strong default that may be departed from only with written justification. **MAY** is optional.
- Requirements carry IDs (for example, EA-03 for Enrollee App) so they can be traced into contracts, test plans, and audits.
- **Verified figures** come from the white paper and are footnoted. **Proposed parameters** (for example, some retention periods) are design defaults written by the product team. They are labeled *Proposed* and are not research findings. Each needs approval from the Privacy Office, the National Archives (NARA) records schedule process, or the program governance board before use.

Contents. 1. Product Summary · 2. Goals and Non-Goals · 3. Users and Roles · 4. Key Design Principles · 5. Program Lifecycle and Supervision Tiers · 6. Enrollee App Requirements · 7. Agent Triage Dashboard · 8. Caseload Management · 9. Supervisor Analytics · 10. Data Model · 11. Integrations · 12. Privacy and Civil Liberties Safeguards · 13. Security Requirements · 14. Legal Constraints · 15. Pilot Plan and Success Metrics · 16. Risks and Open Questions · Appendix A: Verified Figures · Appendix B: Glossary

1. Product Summary

ISAE is a supervision and integration platform for one population: noncitizens who are already in the United States, pose no public-safety threat, are not subject to mandatory detention, and can be supervised in the community. It re-sequences enforcement rather than abolishing it. Detention and

removal remain available for people who are dangerous, a flight risk, or under an executable final order.

The product has four parts:

1. **Enrollee app.** A multilingual mobile app (with SMS, voice, and in-person fallbacks) that delivers court and check-in reminders, scheduled check-ins, the *Green Path* milestone program, a document vault, work-permit and taxpayer-ID status, and a secure channel to a case specialist.
2. **Agent triage dashboard.** A decision-support tool for officers and case specialists at the point of encounter or intake. It shows a green, yellow, or red recommended pathway based on current law and existing records. A human always decides.
3. **Caseload management.** Work queues, tiering, stepped responses to missed obligations, and case notes for case specialists and officers.
4. **Supervisor analytics.** Program performance, caseload balance, override audits, accuracy and bias monitoring, and public reporting.

Why build it. As of July 11, 2026, ICE held 65,765 people in detention, and 70.6 percent of them had no criminal conviction; ATD was monitoring 183,181 individuals and family heads. The FY2023 cost of an adult detention bed was \$187.48 per day, compared with \$4.11 per participant per day under the ISAP IV ATD contract. The tools ISAE needs already exist in ATD: ISAP IV includes a smartphone app (SmartLINK), facial verification, telephonic reporting, GPS, court tracking, and case management. ISAE points those tools at a different goal: supervising and integrating people who are eligible to remain, with enforcement held in reserve.

What the evidence does and does not support. Intensive, service-rich case management has produced very high appearance rates. In the Family Case Management Program (FCMP), ICE reported 100 percent court attendance and 99 percent compliance with check-ins as of March 2017. Technology-only supervision at large scale has done worse: ATD's absconder rate was 12.8 percent in FY2023. **The product is therefore designed around a real case manager, legal orientation, and services, with the app as a force multiplier. It does not assume that an app alone will produce 99 percent compliance.**

2. Goals and Non-Goals

2.1 Goals

ID	Goal	How we will know (see Section 15)
G1	Raise court-appearance and check-in compliance among enrolled participants	Appearance rate at all hearings and at final hearings, compared with a matched or randomized comparison group
G2	Avoid unnecessary detention of low-risk people while keeping enforcement available for high-risk cases	Detention days avoided; share of red-tier cases routed to standard enforcement; no rise in public-safety incidents among enrollees

ID	Goal	How we will know (see Section 15)
G3	Reduce cost per supervised case and free officer hours for high-risk work	Cost per participant per day by tier; officer hours per case
G4	Bring eligible participants into the formal labor and tax system	Employment Authorization Document (EAD) approval and tax-filing milestone rates
G5	Reward compliance visibly through the Green Path	Milestone completion; step-downs to lower supervision tiers
G6	Protect privacy and civil liberties by design, and prove it publicly	Clean independent audits; biometric accuracy and bias test results; redress turnaround; firewall exception counts
G7	Produce trustworthy evidence on whether the model works	Pre-registered evaluation published at the end of the pilot

2.2 Non-Goals

ISAE will not:

- **Create immigration status or a path to permanent residence or citizenship.** Only Congress can do that. The Green Path mirrors the five-year residence period and the English and civics requirements for naturalization, but completing it confers no status.
- **Override mandatory detention.** If a statute requires detention, the dashboard shows red and the green pathway is unavailable.
- **Make automated enforcement decisions.** No arrest, detention, tier increase, or referral happens without a named human decision-maker.
- **Perform one-to-many (1:N) face recognition or general surveillance, except the single enrollment background check in FE-05, which is an investigative lead only.**
- **Track location continuously.** Location is captured only at scheduled check-ins or when the participant opens the app to check in. No background tracking, geofencing, or movement history for green-tier participants.
- **Serve as an enforcement lead source.** Enrollment data may not be used to target participants, their families, or their communities, except under the narrow, listed serious-criminal grounds in Section 12.2.
- **Replace legal counsel or immigration court.** ISAE refers participants to legal service providers; it does not give legal advice or decide cases.
- **Collect data the program does not need** (for example, phone contacts, photo libraries, social media, or data about family members beyond what the participant's own case requires).

3. Users and Roles

Role	Who they are	Primary needs	Key permissions	Explicitly cannot
Enrollee	A noncitizen	Know what is required and	View and export own	See other people's

Role	Who they are	Primary needs	Key permissions	Explicitly cannot
	enrolled in ISAE, sometimes the head of a family unit	when; prove compliance easily; track milestones; keep documents safe; reach a case specialist; understand rights	record; check in; complete lessons; upload documents; message case specialist; file a challenge or correction	data; turn on background tracking (the app has none)
Case specialist / agent	Contractor case specialist or ICE officer who supervises a caseload; officers also run field triage	Fast, accurate triage; a prioritized queue; clear next actions; low administrative burden	Run triage; enroll; view assigned cases; record check-in outcomes and notes; review face-match failures; propose tier changes	Access unassigned cases without logged justification; run 1:N searches; export bulk data; view raw location history beyond the current case need
Supervisor	ICE supervisory officer or contractor site manager	Caseload balance; quality control; approve yellow-tier and override decisions; program metrics	Approve yellow pathways, tier increases, and enforcement referrals; reassign cases; view team and site analytics	Override the firewall; access individual data for purposes unrelated to supervision
Legal counsel / auditor	DHS Office of the General Counsel, Privacy Office, CRCL, Inspector General, independent auditors, and the ombudsman	Verify lawful use; review overrides, firewall requests, accuracy, bias, and retention	Read-only access to audit logs, decision records, and model or rules documentation; approve firewall exception requests (counsel); sample case files under audit protocol	Change case records; take operational actions
Partner (secondary)	Legal service providers, English and civics course providers, community organizations	Confirm a referral or course completion	Submit attestations through a narrow partner portal	View case records, location, or biometrics

4. Key Design Principles

1. **Law first.** The rules engine encodes current statute and binding precedent, including mandatory-detention provisions. Legal changes are reviewed by counsel and released as versioned rule sets.
2. **Human decides; machine recommends.** Every consequential action names the person who took it and records the reason.
3. **Incentive over surveillance.** Participants should have a reason to open the app (progress, benefits, reminders), not only an obligation.
4. **Minimum data, shortest retention.** Collect only what a requirement needs, and delete on schedule.
5. **Verification after enrollment; the enrollment check is a lead only.** After enrollment, biometrics only confirm that the enrolled person is the one checking in (1:1). They are never used to find out who an unknown person is. The single exception is the one-

time background check at field enrollment (FE-05), whose result is an investigative lead only, never proof on its own.

6. **Fail safe for the participant.** A technical failure (failed face match, dropped connection, app crash) must never by itself produce an adverse action.
7. **Transparent by default.** Published rules, published metrics, published audit results.
8. **Built for low-connectivity, multilingual, and disabled users.** These are core requirements, not enhancements.

5. Program Lifecycle and Supervision Tiers

Lifecycle. Encounter or referral → triage (Section 7) → enrollment and consent (Section 6.1) → supervision at an assigned tier → Green Path progress → step-down to lighter tiers → exit (case resolved, status granted, departure, or transfer out of ISAE) → retention and deletion (Section 10.4).

ISAE reuses ICE’s existing tier structure: enhanced case management capped at 40 participants per contractor case specialist, “technology sites” where ICE officers supervise lower-risk participants, and “maintenance sites” for compliant participants with no office or home visits.

Tier	Intended for	Contact pattern	Location data	Staffing
Intensive (enhanced case management)	New enrollees with stabilizing needs; yellow-pathway enrollees; anyone after repeated missed obligations	Frequent scheduled check-ins; case-manager meetings; legal orientation	At scheduled check-in only. GPS device only on an individualized, documented, supervisor-approved finding, reviewed on a set schedule	Case specialist, caseload no more than 40
Standard (technology site)	Green-pathway enrollees after onboarding	Scheduled app check-ins; periodic office contact	At scheduled check-in only	ICE officer or case specialist using the platform
Maintenance	Participants with a sustained compliance record and milestone progress	Infrequent check-ins; no office or home visits	At scheduled check-in only	Automated reminders plus periodic human review

Exact check-in frequencies per tier are **proposed parameters** to be set during Phase 0 and tested in the pilot. ICE does not publish officer-to-participant ratios, so the claim that one officer can manage “hundreds” of cases is unverified. **Caseload capacity per tier is a pilot measurement, not a design assumption.**

6. Enrollee App Requirements

6.1 Enrollment, onboarding, and consent

ID	Requirement
EA-01	The app MUST present a plain-language notice in the enrollee’s language, in text and audio, before any data collection. The notice covers what is collected, why, who can see it, how long it is kept, the firewall and its listed

ID	Requirement
	exceptions, and how to challenge or correct records.
EA-02	The app MUST record separate, granular consent for (a) face verification, (b) location capture at check-in, (c) optional programs (community milestone, partner referrals), and (d) optional notifications. Consent records are versioned and time-stamped.
EA-03	The app MUST tell the enrollee honestly which supervision conditions are required by their release terms. It MUST offer a non-biometric alternative check-in method (in-person or voice) for anyone who declines face verification or cannot use it. Declining biometrics MUST NOT by itself raise the tier or reduce eligibility for Green Path benefits.
EA-04	Enrollment MUST be completable at the point of encounter or at a field enrollment visit at the person's location (Section 6.9), so that a green-pathway person leaves with the app installed (or an SMS/voice alternative set up), a Temporary Digital ID delivered by SMS or WhatsApp, and a first check-in date. No office visit is required.
EA-05	The app MUST work on a participant-owned device. Where a participant has no suitable phone, the program SHOULD provide a basic device or a non-smartphone channel (SMS, voice, kiosk, in person).
EA-06	The app MUST NOT request permissions for contacts, photo library, microphone (except during a voice check-in the user starts), Bluetooth scanning, or background location.

6.2 Green Path milestones

The Green Path is a five-year, gamified track with milestones that unlock concrete benefits within the agency's discretion.

Track	Example milestones	Verification source
Accountability	Attend every hearing and check-in; keep a current address	EOIR hearing outcome; check-in log
Clean record	No disqualifying arrests or convictions; periodic background re-checks	FBI/DHS checks
Self-sufficiency	Lawful employment once authorized; annual tax filing	EAD status; participant-provided tax transcript
English	Progressive levels (for example, beginner to intermediate) through in-app and partner courses	Assessed modules; partner attestation
Civics	Units modeled on USCIS civics content	Assessed modules
Community (optional)	Volunteering; school enrollment for children	Partner attestation

ID	Requirement
GP-01	The app MUST show a clear progress view across all tracks, with the next required action, due dates, and the benefit each milestone unlocks.
GP-02	Benefits MUST be limited to lawful, discretionary actions: fewer check-ins, a lower supervision tier, longer renewal periods for deferred action and work authorization, and documented priority for any status Congress later creates.
GP-03	The app MUST state on the Green Path home screen and in onboarding that the Green Path does not grant permanent residence or citizenship.
GP-04	English and civics lessons MUST be downloadable for offline use and support audio-first learning for participants with limited literacy.
GP-05	Lesson assessments MUST record only the outcome needed for the milestone (pass, level reached, date). Item-level answers are deleted after the module is scored (see Section 10.4).
GP-06	Clean-record status MUST be shown in the app as a milestone state only ("current" or "under review"). Background-check details are visible to the case specialist, not displayed in the app. A change to "under review" MUST trigger human review, not an automatic consequence.

ID	Requirement
GP-07	The optional community track MUST NOT affect tier or benefits if the participant does not take part.
GP-08	Milestone rules (what counts, what it unlocks) MUST be published and versioned. Changes MUST NOT retroactively remove milestones already earned.
GP-09	Participants MUST be able to export a verified record of their compliance and milestones (signed PDF and machine-readable file). This supports any future status Congress creates.

6.3 Court and check-in reminders

ID	Requirement
RM-01	The app MUST deliver multilingual reminders for immigration court hearings, ICE or contractor appointments, and scheduled check-ins, by push notification, SMS, and voice call according to participant preference.
RM-02	Hearing dates MUST come from the authoritative EOIR hearing calendar where an agreement is in place (Section 11). Each reminder MUST show the source and the last sync time. Where no feed exists, the case specialist enters the date from the notice and the app labels it “entered manually.”
RM-03	Hearing changes (rescheduling, venue change, remote hearing) MUST generate an immediate notice and a confirmation request.
RM-04	Reminders MUST include the address, travel directions, what to bring, interpreter information, and a one-tap link to legal service referrals.
RM-05	The app SHOULD offer one-way calendar sync (add to device calendar) without read access to the participant's calendar.
RM-06	A missed obligation MUST trigger the stepped response in Section 8.3 (outreach first). It MUST NOT trigger automatic arrest or referral.

6.4 Check-ins and identity verification (enrollee side)

ID	Requirement
CI-01	Check-ins occur only within scheduled windows set by the case specialist, or when the participant opens the app to check in.
CI-02	At check-in, the app MAY capture a single location point (with notice and as a release condition). It MUST NOT capture location at any other time, run in the background, or set geofences for green-tier participants.
CI-03	Face verification MUST be 1:1 against the participant's own enrollment template. The device MUST delete the captured image after comparison, consistent with current SmartLINK practice. ¹
CI-04	If face verification fails, the app MUST immediately offer a retry and an alternative method (voice or in person). The failure goes to human review (Section 7.3). It MUST NOT be recorded as non-compliance.
CI-05	A check-in MUST succeed on a poor network: queue locally with a trusted timestamp and sync when connectivity returns. A late sync caused by connectivity MUST NOT count as a missed check-in.
CI-06	The participant MUST receive a receipt for every check-in (time, method, result).

6.5 Document vault

ID	Requirement
DV-01	Participants MUST be able to store and view official notices (for example, Notice to Appear, hearing notices,

¹ TRAC Immigration, “Quick Facts” (data current as of July 11, 2026): 65,765 in ICE detention; 46,436 (70.6%) with no criminal conviction; 183,181 monitored in ATD. <https://tracreports.org/immigration/quickfacts/>

ID	Requirement
	release conditions), EAD cards, receipts, and course certificates.
DV-02	The vault MUST be encrypted on the device and on the server. Documents uploaded by the participant are visible to the case specialist only when the participant shares them, or when the document is a required program record (for example, release conditions).
DV-03	Agency-issued documents MUST be pushed to the vault with an integrity signature so the participant can prove authenticity.
DV-04	The participant MUST be able to download, print, and share documents with their attorney through a time-limited link.
DV-05	On exit, the participant MUST receive an export of the vault before deletion.

6.6 Work permit and ITIN/SSN status

ID	Requirement
WP-01	The app MUST show EAD status (not filed, filed, pending, approved, denied, renewal due) for participants granted deferred action or parole who may apply under existing regulations. ²
WP-02	Status SHOULD come from USCIS case status through an intra-DHS agreement. Until then, the participant enters the receipt number and the app shows public case-status information.
WP-03	The app MUST remind participants of EAD renewal deadlines and link to official filing instructions and legal service providers.
WP-04	The app MUST track tax-ID setup as a milestone: a Social Security number where work authorization is granted, or an IRS Individual Taxpayer Identification Number (ITIN) otherwise. The app MUST NOT store the full SSN or ITIN; it stores only "on file: yes/no" and, at the participant's choice, the last four digits.
WP-05	Annual tax filing MUST be verified by participant-provided documents (for example, an IRS transcript), not by a data feed from the IRS. Federal tax information is protected by federal tax confidentiality law, and no IRS integration is planned.

6.7 Messaging, referrals, and help

ID	Requirement
MS-01	Secure, encrypted messaging between participant and assigned case specialist, with machine translation clearly labeled and the option to request a human interpreter.
MS-02	A directory of legal service providers, legal orientation, English and civics courses, health and social services, and community resources. Use of a referral MUST NOT be shared with enforcement.
MS-03	A "Know your rights and your data" section in every supported language, including how to reach the independent ombudsman.

6.8 Multilingual, low-bandwidth, and accessibility requirements

ID	Requirement
AX-01	Languages. Launch languages MUST be chosen from the language data of pilot-site participants. All legal notices MUST be professionally translated and reviewed, not machine-translated. Indigenous and less common languages MUST be supported through audio and live interpretation.
AX-02	Low literacy. Core flows (check-in, reminders, milestone status) MUST work with icons and audio, without reading.

² U.S. Immigration and Customs Enforcement, *Budget Overview, Fiscal Year 2025 Congressional Justification* (DHS, 2024). Adult bed cost per day FY2023 actual \$187.48; ISAP IV FY2023 cost \$4.11 per participant per day; ECMS caseload of no more than 40 participants per case specialist; ATD absconder rates of 16.2% (FY2021), 8.1% (FY2022), 12.8% (FY2023); site tiers; 1–5 risk score; ISAP IV capabilities (SmartLINK, facial verification, telephonic reporting, GPS, court tracking, case management).
https://www.dhs.gov/sites/default/files/2024-04/2024_0308_us_immigration_and_customs_enforcement.pdf

ID	Requirement
AX-03	Low bandwidth. The app MUST be offline-first: reminders, schedules, documents, and downloaded lessons available without a connection; small install size; lessons downloadable over Wi-Fi; compressed images; no video required for core functions.
AX-04	Non-smartphone access. Every required action (reminder, check-in, rescheduling request) MUST be possible by SMS, interactive voice response, or in person.
AX-05	Accessibility. The enrollee app, dashboard, and portals MUST meet Section 508 standards and SHOULD meet WCAG 2.2 Level AA: screen-reader support, scalable text, sufficient contrast, captions, and alternatives to face verification for participants whose disability affects capture.
AX-06	Older and shared devices. The app MUST support older OS versions common among pilot participants and MUST protect data on shared family devices (separate PIN or device unlock; no sensitive content in notification previews).

6.9 Field enrollment and Temporary Digital ID

ISAE meets people where they are. Enrollment is done by a trained case worker or community partner at the person's location, using a phone. Face capture is the default because many field phones lack fingerprint readers. A face-based background check result is never proof on its own: any doubt defaults to a follow-up fingerprint check, with no adverse action in the meantime.

ID	Requirement
FE-01	Enrollment MUST be possible at the person's location (for example, home, church, clinic, workplace, or community center) by a trained ISAE case worker or a certified community partner using a program phone. An office visit MUST NOT be required.
FE-02	Community partners MUST complete ISAE training and vetting and sign a data-handling agreement. They work under a named case worker, see only the enrollment they are performing, and have no access to firewall-protected or enforcement data.
FE-03	The notice and consent in EA-01 and EA-02 MUST be presented in the person's chosen language and read aloud on the device before any capture. The person MUST be told about the one-time background check (FE-05), the follow-up rule (FE-06), and how to reach legal aid.
FE-04	Face capture MUST include an on-device quality check (framing, lighting, focus, glare) with retake. Fingerprints MUST be captured only if the device has a certified reader; otherwise the step is skipped automatically and handled under FE-06 if needed.
FE-05	A one-time 1:N face check of the enrollment photo MAY be run once, after the visit, against criminal-history databases authorized for background checks and listed in the PIA. Its result is an investigative lead only. It MUST NOT be treated as proof of identity or criminal history, MUST NOT by itself produce a red pathway or any adverse action, and MUST NOT be repeated. After enrollment, all face matching is 1:1 (FV-01).
FE-06	Any doubt MUST default to a follow-up fingerprint check: a possible match, a low-quality photo, or no match where confidence is below the published threshold. Every possible match MUST be reviewed by a trained human examiner, and the decision and reason MUST be recorded.
FE-07	The follow-up fingerprint check MUST be scheduled at the enrollee's convenience and done in the field. Until it is resolved, there MUST be no adverse action (no arrest, detention, tier increase, or loss of benefits) and the Temporary Digital ID MUST stay active.
FE-08	No arrests during enrollment visits. Field workers MUST NOT carry out, request, or signal enforcement action during a visit, and the field enrollment app MUST NOT contain any arrest or enforcement-referral function.
FE-09	A Temporary Digital ID MUST be sent at the end of the visit by SMS or WhatsApp (WhatsApp only with consent) as a secure, expiring, device-bound link. The message body MUST NOT contain sensitive data. The ID shows the person's photo, a QR code verifiable against ISAE, and "Temporary – official card arriving by mail", and stays valid until the printed card arrives.
FE-10	The ID screen MUST show a status tracker: Enrolled › Background check in progress › (Fingerprint follow-up needed, if FE-06 applies) › Cleared › Card printed › Card mailed. Follow-up wording MUST be reassuring and in

ID	Requirement
	the person's language, for example: "We need one more quick step; your temporary ID stays active." Results and how to dispute them (RD-01) MUST be communicated with a legal aid contact.

6.10 Translate / Traducir helper

A built-in helper so enrollees can understand and be understood in English in daily life and with officials. Phase 1 is typed text with spoken output; the design leaves room for speech input. It supports communication but never replaces a certified interpreter for legal matters.

ID	Requirement
TR-01	The helper MUST be reachable from every enrollee screen (floating button) and from the home screen, labeled in both the enrollee's language and English.
TR-02	A two-way conversation view MUST translate the enrollee's language to English and English to the enrollee's language, with a swap control. Every message MUST have a read-aloud control using a voice for the correct language, and a slower playback option.
TR-03	After each enrollee message is translated, the app MUST show a back-translation into the enrollee's language so they can confirm the meaning, and MUST visibly flag words or phrases translated with low confidence, offering "say it another way".
TR-04	Quick phrase cards MUST cover common situations (court, check-in, doctor, work, school, police stop), including "I have a lawyer" and "I want to speak to my case worker", in both languages with audio. Legally significant phrases MUST be reviewed by certified translators and counsel.
TR-05	Speech input SHOULD be added in a later phase. Until then the microphone control MUST be labeled "Coming soon" and the app MUST fall back to typing without error where speech recognition is unavailable.
TR-06	Translation MUST use a vetted service under a DHS-approved agreement: no vendor retention or model training on ISAE content, encryption in transit, and on-device processing where feasible. Conversations MUST NOT be stored by default; saving is an explicit opt-in kept only on the device, and helper content is excluded from enforcement use under the firewall (Section 12.2).
TR-07	The helper MUST state that it is not a substitute for a certified interpreter for court, legal papers, police, or medical consent, and MUST offer a one-tap "Request a human interpreter" option (free, by phone or video, or scheduled).
TR-08	Enrollees MUST be able to save any phrase to practice; saved phrases feed the English micro-lessons (Section 6.2) as listen-and-repeat items.
TR-09	Spanish ↔ English MUST be available at launch; other launch languages (AX-01) follow as vetted translation quality allows, with the target language's quality status shown to the user.

6.11 Language Strategy

Language access is not a feature to add after launch. If a person cannot understand a notice, a reminder, or a consent screen, the program cannot fairly hold them to it, and every compliance figure it reports is suspect. This section sets out which languages ISAE supports, in what order, how, and at what cost. It builds on AX-01 to AX-06 (Section 6.8) and the Translate / Traducir helper (Section 6.10, TR-01 to TR-09). Sources for this section are listed at its end as [L1]–[L6].

Scope of need

National picture. MPI estimates 13.7 million unauthorized immigrants lived in the United States in mid-2023, and that two-thirds of those aged 5 or older were limited English proficient (LEP), meaning they reported speaking English less than "very well" [L1]. Mexico accounted for 40% (about

5.53 million) and Guatemala for 10% (about 1.40 million), followed by Honduras and El Salvador at 8% each; the Philippines (about 294,000) and Brazil (about 286,000) were each about 2% [L1]. In MPI’s earlier state-level analysis (2012–16 data), the top home languages of unauthorized immigrants nationally were Spanish, English, Chinese, Tagalog, and Korean; Haitian Creole and Portuguese ranked in Florida’s top five and Vietnamese in Texas’s [L2].

Indigenous languages: the hidden layer. Census and survey data record “Spanish” for many people whose first language is Indigenous, so the Indigenous need is largely invisible in standard statistics. The Indigenous Farmworker Study estimated about 120,000 Indigenous Mexican farmworkers in rural California, about 165,000 including children; over half were Mixteco speakers, 26% Zapoteco, and 9% Triqui [L3]. The study says the true total is “considerably higher,” because it excluded urban residents and non-Mexican Indigenous immigrants such as Guatemalans [L3]. The figures date from 2007–09 field work and should be treated as a floor, not a current count.

Central Coast and Guatemala. MICOP, the Mixteco/Indigena Community Organizing Project, states that 20,000 Indigenous migrants live and work in Ventura County and another 25,000 in Santa Barbara County [L4]; an earlier MICOP presentation gave 29,000 for Santa Barbara County, so these are organizational estimates, not census counts. A First 5 Ventura County staff memo (April 16, 2026) describes Mixteco families there as often illiterate and says most “speak neither Spanish nor English, but only their native language” [L5]. In Guatemala’s 2018 census, 41.7% of the population identified as Maya; K’iche’ was the first language of about 1.05 million people (7.8%) and Mam of about 591,000 (4.4%) aged 4 and older [L6]. No reliable figure exists for how many Guatemalan immigrants in the United States speak a Mayan language first; ISAE SHOULD fund pilot-site intake data to find out.

Launch tiers and rationale

Tier	Languages and rationale
Tier 1 (launch)	English; Spanish; Indigenous Mesoamerican languages: Mixteco, Zapoteco, Triqui, K’iche’, Mam. Spanish covers the largest share of participants [L1][L2]. The Indigenous languages are in Tier 1, not later, because their speakers are concentrated in likely pilot regions such as the Central Coast [L3][L4], are often not literate or fluent in Spanish [L5], and are the people most likely to be failed by a Spanish-only design. They are delivered through human-recorded audio and community interpreters, not machine translation.
Tier 2	Haitian Creole, Brazilian Portuguese, Mandarin, Cantonese, Vietnamese, Tagalog. Large established groups in national and state data [L1][L2]. Full written UI, audio, and vetted machine translation where quality testing passes (LANG-08).
Tier 3	Hindi, Punjabi, Gujarati, French, Arabic, Russian, Ukrainian. Groups that have grown recently or are concentrated in particular metros. Written notices and phone interpretation first; full UI as pilot-site demand data justifies it.
Under review	Korean appears in MPI’s national top five home languages of unauthorized immigrants [L2] but is not in the tiers above; it SHOULD be evaluated for Tier 2. Q’eqchi’ is a larger first language in Guatemala than K’iche’ or Mam [L6]; its US need is unknown. Tier placement for every language MUST be revisited after pilot-site intake data (LANG-02).

Design principles

Audio-first, literacy-optional. Many participants will not read comfortably in any language. Core flows are designed to be heard and seen first, and read second: an audio button on every screen, icons for every action, one action per screen, and no flow that requires typing to complete an obligation (AX-02, AX-04).

Indigenous languages are not one language each. Mixteco, Zapoteco, and Triqui are families of related varieties, and speakers from different towns may not fully understand each other.

“Mixteco” in a menu is therefore not enough: the app and the field worker **MUST** identify the person’s variety or home region and match recordings and interpreters to it. Machine translation for these languages is weak, inconsistent across varieties, or absent, and written forms are not used by many speakers. ISAE **MUST NOT** display machine-generated text in these languages.

Requirements

ID	Requirement
LANG-01	Tiers. The system MUST support languages in three tiers as defined in this section. Tier 1 (English, Spanish, Mixteco, Zapoteco, Triqui, K’iche’, Mam) MUST be available at pilot launch for all required actions.
LANG-02	Data-driven review. Each pilot site MUST record each participant’s preferred language, variety or home region, and whether they read it, with consent and only for service delivery. Tier placement MUST be reviewed every 6 months using this data and published in aggregate.
LANG-03	Language choice first. Language MUST be the first choice in the field enrollment flow and the enrollee app, shown with spoken prompts, and changeable at any time from every screen.
LANG-04	Audio-first. Every enrollee screen MUST have an audio version. Required obligations (court dates, check-ins, rights notices) MUST be deliverable by voice call or voice message in the participant’s language (see AX-04).
LANG-05	Indigenous audio. For Mixteco, Zapoteco, Triqui, K’iche’, and Mam, core screens, reminders, and the consent and rights notices MUST be human-recorded by paid community speakers of the matching variety, reviewed by a second speaker. Synthetic speech and machine-translated text MUST NOT be used for these languages.
LANG-06	Community interpreters. Field enrollment in an Indigenous language MUST be done with a trained community interpreter of the participant’s variety, in person or by phone. Enrollment MUST NOT proceed on the basis of Spanish if the person is not comfortable in Spanish; it is rescheduled instead.
LANG-07	Translation helper. The Translate / Traducir helper (TR-01 to TR-09) MUST show each language’s quality status (“Vetted”, “Testing”, or “Interpreter only”). For Tier 1 Indigenous languages the helper MUST offer recorded phrase cards and a one-tap human interpreter (TR-07) instead of free-text translation.
LANG-08	Machine translation gate. A language MAY use machine translation in the helper only after a documented test on ISAE content with community reviewers shows acceptable accuracy, with low-confidence flags (TR-03). Legal notices are never machine-translated (AX-01).
LANG-09	Translation QA. All written and recorded content MUST go through: professional translation, review by at least two community reviewers from the target population (paid), a back-translation check for legal and rights content, field testing with participants, and a correction channel. Every published string MUST carry its review status and date.
LANG-10	Plain language. Source English MUST be written at a plain-language level before translation; translators MUST be allowed to adapt wording for meaning rather than translate word for word.
LANG-11	English learning. English micro-lessons (Section 6.2) MUST be taught through the participant’s own language, including audio-only instructions for Indigenous-language speakers, and MUST NOT assume Spanish literacy.
LANG-12	Website and public materials. Public summaries MUST be published at least in all Tier 1 written languages and audio for Indigenous Tier 1 languages; deep policy material MAY remain in English with a notice.
LANG-13	Staffing. Each pilot site MUST budget for paid community interpreters and reviewers as a line item, not

ID	Requirement
	volunteers, and MUST track interpreter wait times and enrollments rescheduled for lack of an interpreter as public metrics.
LANG-14	No status inference. Language data MUST NOT be used for triage, risk scoring, or enforcement, and MUST NOT be shared outside the program (Section 12).

Cost and staffing realities

This is the most expensive and slowest part of the enrollee experience to build, and it does not scale like software. Human recordings must be redone whenever content changes. Qualified interpreters for specific Mixteco, Zapoteco, and Triqui varieties are scarce, and community organizations such as MICOP already depend on them for health, school, and legal work [L4][L5]; ISAE must pay for interpreter time and train new interpreters rather than draw down that capacity. No cost estimate is given here because no verified per-language figures were found; pilot budgets MUST be built from local quotes.

Honest risks

Exclusion by default. If Indigenous audio is not ready at launch, the pilot will in practice serve Spanish speakers only and undercount the people with the greatest need. The pilot SHOULD NOT start at a site until its Tier 1 audio is reviewed.

Wrong variety. A recording in the wrong Mixteco or Zapoteco variety may be partly or wholly unintelligible, and the person may not say so. Comprehension checks during field testing are required.

Trust and interpreter safety. Community interpreters may be seen as working for enforcement, which could hurt their standing at home. Their role, the firewall (Section 12.2), and their right to decline must be clear.

Quality drift. Machine translation quality varies by language and topic and changes when vendors update models. The LANG-08 gate must be re-run after vendor changes.

Data gaps. The best Indigenous population figures are more than 15 years old or are organizational estimates; national data does not separate Indigenous speakers. Planning must not overstate precision.

Sources for Section 6.11

[L1] Julia Gelatt, Ariel G. Ruiz Soto, and James D. Bachmeier, “Changing Origins, Rising Numbers: Unauthorized Immigrants in the United States,” Migration Policy Institute fact sheet, 2025 (mid-2023 estimates; pooled 2019–23 ACS).

https://www.migrationpolicy.org/sites/default/files/publications/mpi-unauthorized-immigrants-fact-sheet-2025_FINAL.pdf

[L2] Migration Policy Institute, “Settling In: A Profile of the Unauthorized Immigrant Population in the United States,” 2019, Table 3 (pooled 2012–16 ACS).

https://www.migrationpolicy.org/sites/default/files/publications/UnauthorizedData-FactSheet_FinalWeb.pdf

[L3] Indigenous Farmworker Study (with California Rural Legal Assistance), “California’s Indigenous Farmworkers,” final report, January 2010; and “Demographics.”

http://www.indigenousfarmworkers.org/IFS%20Full%20Report%20_Jan2010.pdf ;

<http://indigenousfarmworkers.org/demographics.shtml>

[L4] Mixteco/Indigena Community Organizing Project (MICOP), “Who Are We?”

<https://mixteco.org/> ; and “MICOP: Farmworkers, Census, and Indigenous Knowledge” (presentation, California Census Office).

<https://census.ca.gov/wp-content/uploads/sites/4/2020/06/MICOP-Peer-Learning-Slides.pdf>

[L5] First 5 Ventura County, “Recommendation to Grant Authority to the Executive Director to Contract with MICOP,” staff memo, April 16, 2026.

https://first5ventura.org/wp-content/uploads/2026/04/9.-Rec_MICOP_4-16-26_Final-2.pdf

[L6] Instituto Nacional de Estadística (Guatemala), XII Censo Nacional de Población 2018, principal results (pueblo de pertenencia; idioma en que aprendió a hablar).

https://www.ces.uvg.edu.gt/censo2018/documentos/Principales_resultados_Censo2018.pdf

7. Agent Triage Dashboard

7.1 Purpose and inputs

The triage dashboard brings together information officers already use and shows a recommended pathway. Inputs:

- identity verification result (see 7.3)
- criminal history (FBI/DHS checks)
- prior immigration history and pending cases (DHS records; EOIR case status)
- statutory detention flags, including the 2025 Laken Riley Act’s expansion of mandatory detention to certain inadmissible noncitizens who are charged with, arrested for, or admit to theft-related offenses, among others
- binding interpretations, such as the BIA’s 2025 decision in *Matter of Yajure Hurtado*, which reads the law to require detention without a bond hearing for people present without admission. That interpretation is being challenged in federal court, and the rules engine MUST be updated as the law changes.
- verified residence and stabilizing factors (for example, family ties, counsel of record)

7.2 Pathway logic

Pathway	Criteria	Recommended action	Who decides
Green	All of: no criminal convictions or disqualifying charges; not subject to	Administrative enrollment on site: issue required paperwork, enroll in	Officer

Pathway	Criteria	Recommended action	Who decides
	mandatory detention; identity and residence verified	ISAE, set the first check-in. No custodial arrest.	
Yellow	Minor history, incomplete information, or a data conflict	Supervisor review; enrollment at a higher supervision tier if approved	Officer, with supervisor approval
Red	Public-safety or national-security concern; mandatory-detention category; executable final order	Standard enforcement	Officer

ID	Requirement
TD-01	The rules engine MUST be deterministic, documented, and published (operationally sensitive national-security indicators are documented for auditors only). Each recommendation MUST list the specific rules and data that produced it.
TD-02	The green pathway MUST be unavailable whenever release is not legally allowed. Mandatory-detention rules are hard stops that cannot be overridden on the dashboard.
TD-03	The officer MUST make and record the decision. Departing from a recommendation in either direction (for example, arresting a green-pathway person or enrolling a yellow-pathway person without approval) requires a coded reason plus free text.
TD-04	Departures MUST be audited in both directions and reported in supervisor analytics by officer, site, and demographic group (in aggregate).
TD-05	The dashboard MUST show data freshness and source for each input, and MUST flag missing or conflicting data as yellow rather than guessing.
TD-06	No opaque risk scoring. ICE already uses a 1–5 ATD risk score; any score ISAE uses MUST be published, tested for disparate impact, and open to challenge by the participant. ¹
TD-07	Protected characteristics (race, ethnicity, religion, sex, disability) and proxies for them MUST NOT be inputs to the pathway logic. They MAY be collected separately, voluntarily, and only for aggregate bias testing under Privacy Office controls.
TD-08	Rule-set changes MUST go through counsel review, version control, regression testing against a reference case set, and a release note visible to auditors.
TD-09	The dashboard MUST work on agency mobile devices in the field. When key data cannot be retrieved, it MUST default to yellow, never to green or red.

7.3 Face verification: 1:1 after enrollment, with human review

ID	Requirement
FV-01	After enrollment, face matching MUST be 1:1 verification only: a live capture compared with the enrolled template of one claimed identity. The only exception is the one-time enrollment background check (FE-05 to FE-07). Apart from it, the system MUST NOT contain or expose any function that searches a face against a gallery (1:N), including watchlists, other participants, or external databases, and there MUST be no street scanning. Contracts MUST prohibit vendors from enabling 1:N on ISAE data beyond FE-05.
FV-02	The template store MUST be technically isolated so that it cannot be queried in bulk or exported, and MUST NOT be shared with other DHS or outside systems.
FV-03	A failed match MUST go to a trained human reviewer, and the participant MUST be offered an alternative check-in (voice or in person) before any adverse action. A failed match alone MUST NOT generate an arrest alert.
FV-04	The algorithm MUST meet the NIST-based accuracy thresholds in Section 12.6 before deployment and every year after.

¹ DHS Office of Inspector General, U.S. Immigration and Customs Enforcement's Award of the Family Case Management Program Contract (OIG-18-22, Nov. 30, 2017), "Program Costs and Performance Metrics."
<https://www.oig.dhs.gov/sites/default/files/assets/2017-12/OIG-18-22-Nov17.pdf>

ID	Requirement
FV-05	Reviewers MUST see the likely reason for failure (for example, poor lighting or low capture quality) and MUST record their decision. Reviewer decisions are sampled for quality audit.
FV-06	Liveness detection MAY be used to prevent spoofing. It MUST be tested for demographic differences on the same terms as matching.
FV-07	A face-based result MUST NOT produce a red pathway on its own. Triage, case, and audit screens MUST display any face-based hit as “Possible match – fingerprint follow-up required” until fingerprints and human review resolve it.

8. Caseload Management

8.1 Work queues

ID	Requirement
CM-01	Each case specialist MUST have a prioritized queue: upcoming hearings, missed or late check-ins, failed verifications awaiting review, milestone reviews, EAD renewals due, and participant messages.
CM-02	Queues MUST be sorted by published, explainable rules (for example, nearness of hearing date), not opaque scoring.
CM-03	The system MUST enforce the enhanced case management cap of 40 participants per case specialist and warn supervisors as a caseload nears the cap.
CM-04	Case notes MUST use structured, coded fields where possible. Free text is limited and subject to the same audit and retention rules.

8.2 Tier changes

ID	Requirement
CM-05	Step-down to a lighter tier SHOULD be proposed automatically when published milestone and compliance criteria are met, and confirmed by the case specialist.
CM-06	Step-up to a heavier tier, or adding a GPS device, requires an individualized written finding and supervisor approval, with a scheduled review date.
CM-07	The participant MUST be notified of every tier change, with the reason and how to challenge it.

8.3 Stepped response to missed obligations

1. **Outreach:** automated reminder, then a call from the case specialist, to find out what happened (illness, transport, work, notice not received, or technical failure).
2. **Remedy:** reschedule, fix contact details, refer to services, or switch to an in-person check-in.
3. **Increased supervision:** tier step-up on a documented finding.
4. **Enforcement referral:** only after the earlier steps, with supervisor approval and a recorded reason, or immediately where a red-tier condition arises (for example, a new disqualifying arrest).

ID	Requirement
CM-08	The system MUST NOT generate an arrest or referral automatically. Each step is a human action with a recorded reason.
CM-09	A missed court hearing MUST trigger immediate outreach and a referral to legal services (for example, to explore a motion to reopen).

ID	Requirement
CM-10	Technical failures (app outage, connectivity, failed match) MUST be recorded separately from participant non-compliance in records and metrics.

9. Supervisor Analytics

ID	Requirement
SA-01	Dashboards for the core metrics in Section 15 by site, tier, and team: appearance rates (all hearings and final hearings), absconder rate, check-in compliance, milestone completion, EAD and tax-filing rates, cost per participant per day by tier, and officer hours per case.
SA-02	Absconder rates MUST be calculated against both active and unenrolled participants, following GAO's recommendation, so that people who leave the program are not dropped from the denominator. ¹
SA-03	Caseload balance and capacity measurement by tier, to answer the unverified question of how many participants one officer can supervise safely.
SA-04	Override and departure audit: rates by officer, site, pathway, and (in aggregate) demographic group, with drill-down to recorded reasons.
SA-05	Biometric performance: match-failure rates, human-review outcomes, and demographic differentials, refreshed at least quarterly.
SA-06	Civil-liberties panel: complaints, redress requests and outcomes, correction turnaround, firewall exception requests (granted and denied), and deletion compliance.
SA-07	Analytics MUST use de-identified or aggregated data by default. Drill-down to an individual case is logged and limited to the user's supervisory scope.
SA-08	Small-cell suppression MUST apply to any published figure that could identify individuals.
SA-09	A public quarterly report MUST be generated from the same metric definitions.

10. Data Model

10.1 Core entities

Entity	Purpose	Key fields (illustrative)	Sensitivity
Participant	The enrolled person	ISAE ID (random, not derived from other identifiers); A-number (link to existing DHS record); legal name; date of birth; preferred language; contact channels; address of record; tier; enrollment and exit dates; consent references	High
Family unit (optional)	Link a head of household to enrolled dependents	Unit ID; member ISAE IDs; role	High
Case link	Connect to immigration proceedings	EOIR case reference; court; next hearing; hearing outcomes; counsel of record (with consent)	High
Release conditions	Legal basis and obligations	Authority (for example, INA § 236(a) release, parole, deferred action); conditions; issue and review dates; issuing officer	High
Triage decision	Record of recommendation and	Rule-set version; inputs used and sources; recommendation; final decision; decision-maker;	High

¹ INA § 316, 8 U.S.C. § 1427 (residence requirements for naturalization). <https://www.law.cornell.edu/uscode/text/8/1427>

Entity	Purpose	Key fields (illustrative)	Sensitivity
	human decision	departure reason; timestamp	
Check-in event	Proof of compliance	Scheduled window; time; method (app, SMS, voice, in person); verification result; location point (if captured); network state; outcome	High
Biometric template	1:1 verification	Template (not image); algorithm version; enrollment date; consent reference	Very high; isolated store
Verification review	Human review of failed matches	Event reference; failure reason; reviewer; decision; time	High
Milestone	Green Path progress	Track; milestone; status; evidence type; verified by; date	Moderate
Lesson progress	English and civics learning	Module; level reached; pass/fail; date (item-level answers deleted after scoring)	Low to moderate
Document	Vault item	Type; issuer; integrity signature; owner; sharing state	High
Work authorization	EAD and tax-ID milestones	EAD receipt number; status; validity dates; tax ID on file (yes/no)	High
Message	Participant-specialist communication	Thread; sender; time; content (encrypted); translation flag	High
Referral	Services and legal aid	Referral type; partner; date; completion attestation (with consent)	Moderate; never shared with enforcement
Supervision action	Tier changes and stepped responses	Action type; reason code; finding text; approver; review date	High
Challenge / redress request	Corrections and appeals	Subject; filed date; status; outcome; reviewer; deadline	High
Firewall request	Exception requests under Section 12.2	Requesting office; listed ground; warrant or order reference; data requested; counsel decision; data released; date	Very high
Audit log entry	Accountability	Actor; role; action; object; purpose code; time; device	High; append-only

10.2 Data that MUST NOT be collected

- Continuous or background location, movement histories, or geofence events for green-tier participants
- Phone contacts, call logs, photo libraries, browsing history, or social-media data
- Face images kept after template comparison (except a capture held for human review of a failed match, under the retention schedule)
- Information about non-enrolled family or household members, beyond emergency contact details the participant chooses to give
- Religious, political, or associational information
- Full SSN or ITIN values
- Item-level lesson answers after scoring

10.3 Minimization rules

ID	Requirement
DM-01	Every field MUST map to at least one requirement in this spec. Fields with no mapped purpose MUST be

ID	Requirement
	removed before ATO.
DM-02	Location points MUST be reduced to a pass/fail result (“checked in within the approved area”) after the dispute window, and the precise coordinates deleted.
DM-03	Access to each entity MUST be restricted by role, assignment, and purpose code (Section 13).
DM-04	Analytics and evaluation datasets MUST be de-identified or pseudonymized, with re-identification keys held separately.
DM-05	ISAE data MUST NOT be copied into other ICE or DHS systems except the minimum fields needed for the participant’s own case (for example, hearing attendance), under a documented agreement. The DHS ATD PIA acknowledges that ATD data may today be stored in other ICE/DHS databases and used for other mission purposes; ISAE MUST close that gap. ¹

10.4 Retention schedule

The white paper’s only recommended retention period is deletion of biometric templates within 90 days of program exit. Under current ATD practice, per the DHS PIA, contractor records are generally destroyed seven years after a participant leaves, and records in one ATD case-management system are kept permanently until that system is linked with ICE’s removal module. **ISAE MUST NOT keep anything permanently.** All other periods below are *Proposed* defaults for Privacy Office and NARA approval, not figures from the source.

Data	Retention	Basis
Biometric template	Deleted within 90 days of program exit	White paper recommendation
Check-in face image on device	Deleted immediately after comparison	Current SmartLINK practice (PIA)
Face image held for failed-match review	Deleted when the review closes; <i>Proposed</i> : no later than 30 days	Proposed
Precise check-in location point	<i>Proposed</i> : 30 days (dispute window), then reduced to pass/fail	Proposed
Check-in outcome (pass/fail, method, time)	Life of participation plus the approved case-file schedule	Proposed; NARA schedule
Lesson item-level answers	Deleted when the module is scored	Proposed
Milestones and compliance history	Life of participation plus the approved case-file schedule; participant receives an export at exit	Proposed; supports any future congressional status
Messages	<i>Proposed</i> : life of participation plus 1 year	Proposed
Participant-uploaded vault documents	Exported to participant; deleted within 90 days of exit	Proposed, aligned to template period
Referral records	<i>Proposed</i> : deleted 1 year after referral closes; never shared with enforcement	Proposed
Triage decisions, supervision actions, firewall register	Approved case-file schedule (accountability record)	Proposed; NARA schedule
Audit logs	<i>Proposed</i> : 7 years, append-only	Proposed; matches current contractor-record period
Contractor-held copies	Returned or destroyed on the same schedule as government records, with a certificate of destruction	Contract requirement

¹ INA § 312, 8 U.S.C. § 1423 (English and civics requirements). <https://www.law.cornell.edu/uscode/text/8/1423>

ID	Requirement
RT-01	Deletion MUST be automated, logged, and verified, including backups (within the backup rotation period) and contractor systems.
RT-02	A legal hold MAY suspend deletion only for a specific record named by counsel. Holds are logged and reported in aggregate.
RT-03	Retention compliance MUST be part of the annual independent audit.

11. Integrations

ISAE connects at a high level to systems that already exist. No integration may go live without the listed agreement, a PIA update, and security review. Where an agreement is not yet in place, the fallback is manual entry by the case specialist or upload by the participant, so the pilot does not depend on any single feed.

System / partner	Purpose	Data and direction	Agreement needed	Phase
EOIR (DOJ) hearing calendars and case status	Accurate hearing reminders; attendance and outcomes for the accountability milestone	Inbound: hearing date, time, location, format, changes, outcome; minimal identifiers	Cross-department DOJ–DHS memorandum of understanding and interconnection security agreement	Pilot if signed; manual entry otherwise
USCIS case status (EAD; deferred action or parole)	Work-permit status and renewal reminders	Inbound: receipt status, validity dates	Intra-DHS data-sharing agreement; PIA update	Pilot
ICE ERO case systems	A-number, release conditions, statutory flags, and history for triage	Inbound for triage. Outbound: only minimum own-case fields (enrollment status, attendance, tier)	Internal DHS agreement defining permitted fields and the firewall (Section 12.2)	Pilot
ATD contractor platform (ISAP IV, including SmartLINK)	Reuse existing check-in, 1:1 verification, and case-management tools	Bidirectional within ISAE	Contract modification adding ISAE privacy, retention, 1:N prohibition, and audit clauses	Pilot
FBI criminal history (and DHS biometric records)	Triage and periodic clean-record re-checks	Inbound: results relevant to disqualifying criteria	Existing law-enforcement access agreements; CJIS Security Policy compliance	Pilot
Legal service providers	Referrals and legal orientation	Outbound: referral (with consent). Inbound: completion attestation	Partner agreements with confidentiality terms; referral data excluded from enforcement	Pilot
English and civics course partners	Course enrollment and completion	Inbound: attestation of level completed	Partner agreements	Pilot
IRS	None. The tax-filing milestone uses participant-provided transcripts	None	None planned	n/a
Language services	Translation and interpretation	Content only; no case data where avoidable	Vendor contract with confidentiality terms	Pilot
Notification channels	Reminders	Outbound: minimal message	Vendor contract with	Pilot

System / partner	Purpose	Data and direction	Agreement needed	Phase
(SMS, voice, push)		content; no case details in previews	data-processing terms	

ID	Requirement
IN-01	All integrations MUST use documented interfaces with mutual authentication, encryption, and field-level allow-lists.
IN-02	Every outbound data flow MUST be listed in the SORN and PIA. An undocumented flow is a security incident.
IN-03	The enrollee app MUST show the source and freshness of integrated data (for example, "Hearing date from EOIR, updated today").

12. Privacy and Civil Liberties Safeguards

ISAE asks participants to share identity, biometric, and location data with the government that may later decide their case. The DHS ATD PIA itself identifies retention and secondary-use risks, and NIST testing found demographic differences in false-match and false-non-match rates across many face-recognition algorithms. Without strong safeguards the program risks function creep; chilling effects, with participants and mixed-status families avoiding enrollment, schools, or health care; and constitutional exposure, since the Supreme Court has recognized strong privacy interests in historical location data. These safeguards MUST be written into the program's governing directive, the SORN, and every vendor contract.

12.1 Purpose limitation

ID	Requirement
PL-01	ISAE data MAY be used only for (a) supervising the participant, (b) providing services and Green Path benefits, (c) adjudicating the participant's own immigration case, (d) program evaluation using de-identified data, and (e) oversight and audit.
PL-02	Every data access MUST carry a purpose code from this list. Access without a valid purpose code MUST be blocked.

12.2 Enforcement firewall

ISAE enrollment data (including check-in locations, messages, referrals, lesson records, documents, and biometric templates) MUST NOT be used for immigration enforcement targeting of participants, their families, household members, or communities. **The only exceptions are the listed serious criminal grounds below, and each also requires a judicial warrant or court order.**

Listed serious criminal grounds (proposed list for counsel review):

1. Terrorism or national-security grounds
2. A pending charge or conviction for a violent felony involving death or serious bodily injury (for example, homicide, kidnapping, armed robbery)
3. Sexual offenses, including any sexual offense against a child

4. Human trafficking, or smuggling of people for profit
5. An outstanding criminal arrest warrant issued by a court for any of the above

ID	Requirement
FW-01	An exception request MUST cite a listed ground, attach a judicial warrant or court order, identify the specific person and specific data needed, and be approved by designated counsel. The Privacy Office and CRCL MUST be notified.
FW-02	Only the minimum data necessary MAY be released. Check-in location history MUST NOT be released unless the warrant specifically covers it.
FW-03	Every request, grant, denial, and release MUST be logged in the firewall register and counted in the public quarterly report.
FW-04	The firewall MUST be technical as well as procedural: enforcement users outside the participant's case team have no access path to ISAE data, and bulk export to enforcement systems is disabled.
FW-05	The firewall does not prevent the stepped response in the participant's own case (Section 8.3), red-pathway routing at triage, or use of the address of record the government already holds in the immigration file. Whether ISAE-captured information may be used to locate a participant who has absconded under an executable final order is an open question for counsel (Section 16).
FW-06	Suspected firewall violations MUST be reportable directly to the Inspector General, and confirmed violations MUST be reported publicly in aggregate.

12.3 Consent and notice

Consent and notice are covered by EA-01 to EA-03. In addition:

- Consent is renewed, in the participant's language, whenever terms change materially.
- Withdrawing an optional consent (for example, the community track or partner referrals) has no effect on tier or benefits.
- Where a condition is mandatory under the release terms (for example, scheduled check-ins), the app says so plainly and does not describe it as voluntary.

12.4 Location: scheduled check-ins only, no continuous tracking

ID	Requirement
LC-01	Location MUST be captured only at the moment of a scheduled check-in, or when the participant opens the app to check in.
LC-02	No continuous tracking, background location, geofencing, or movement histories for green-tier participants.
LC-03	GPS ankle monitors only on an individualized, documented finding approved by a supervisor, with a set review date and automatic expiry unless renewed.
LC-04	Location data MUST sit in a separate, access-restricted store, follow Section 10.4 retention, and be excluded from analytics except as aggregated pass/fail rates.

12.5 Deletion and participant rights

ID	Requirement
DR-01	Participants MUST be able to view and export their own records, with narrow, documented exceptions for law-enforcement-sensitive information.
DR-02	Biometric templates are deleted within 90 days of exit. Participants MAY request earlier deletion when they switch to a non-biometric check-in method.
DR-03	Participants MUST receive confirmation of deletion at exit.

ID	Requirement

12.6 Biometric accuracy thresholds (NIST-based)

ID	Requirement
BA-01	Only algorithms evaluated in NIST's face recognition testing for 1:1 verification are eligible for check-ins. The one-time enrollment check (FE-05) MUST use an algorithm evaluated in NIST's 1:N identification testing. Vendors MUST disclose the exact algorithm versions and their NIST results.
BA-02	Before procurement, the governance board MUST set and publish three thresholds, measured at the operating threshold actually deployed: a maximum false non-match rate, a maximum false match rate, and a maximum ratio between the error rates of the worst- and best-performing demographic groups. <i>The white paper supplies no numeric values, so this spec leaves them as required pilot-gate parameters.</i>
BA-03	The algorithm MUST meet all three thresholds both in NIST results and in independent testing on images captured under field conditions (participant devices, real lighting), before deployment and every year.
BA-04	If in-service monitoring shows a threshold breach, the system MUST move affected check-ins to alternative methods until the breach is fixed.

12.7 Bias testing

ID	Requirement
BT-01	Independent bias testing before launch and every year, covering face verification, liveness detection, the triage rules, queue prioritization, and any published risk score.
BT-02	Tests MUST compare outcomes (match failures, pathway recommendations, officer departures, tier step-ups, enforcement referrals) across demographic groups, nationalities, languages, ages, and disability status, using voluntarily provided attributes or approved statistical methods, held only for testing.
BT-03	Disparities above the published tolerance trigger a mandatory review and corrective plan and are included in the public report.

12.8 Challenge and redress

ID	Requirement
RD-01	Participants MUST be able to challenge, in their language and through the app, SMS, voice, or in person: a triage outcome, a tier change, a recorded missed check-in, a failed verification, a milestone decision, or a data error.
RD-02	Each challenge MUST be reviewed by someone other than the original decision-maker, within a published response deadline (to be set by the pilot governance board).
RD-03	An independent ombudsman MUST be able to receive complaints, review files, and publish findings.
RD-04	Corrections MUST propagate to every system that received the incorrect data.
RD-05	Filing a challenge MUST NOT lead to any adverse action.

12.9 Audits, oversight, and transparency

- Quarterly public reporting by the DHS Office for Civil Rights and Civil Liberties and the Privacy Office.
- Annual Inspector General audits.
- Full implementation of GAO's ATD recommendations on performance measurement and contractor oversight; as of mid-2026, most of GAO's ten recommendations were still open.

- An annual independent audit of firewall compliance, retention and deletion, biometric accuracy and bias, override patterns, and access logs.
- Publication of the triage rules, Green Path rules, metric definitions, PIA, and SORN.

13. Security Requirements

ID	Requirement
SC-01	Encryption. All data encrypted in transit (TLS 1.2 or higher; TLS 1.3 preferred) and at rest using FIPS 140-validated cryptographic modules. Biometric templates and location points kept in separately keyed stores. Keys controlled by the government in a hardware-backed key management service.
SC-02	Hosting and authorization. Hosted in a FedRAMP-authorized environment at the impact level set by the security categorization (expected to be High, given biometric and location data). Agency Authority to Operate under FISMA before pilot launch.
SC-03	Access control. Role- and attribute-based access (role, case assignment, site, purpose code), least privilege by default. Phishing-resistant multi-factor authentication (PIV or equivalent) for all staff, contractor, and auditor accounts. Quarterly access recertification.
SC-04	Participant authentication. Device-bound credential with PIN or device unlock; account recovery that does not rely on a single channel; protections for shared devices.
SC-05	Logging. Append-only, tamper-evident audit logs of every read, write, export, and query, recording actor, role, purpose code, and time. Logs are monitored for anomalous access (for example, browsing unassigned cases or bulk queries) and reviewed by the Privacy Office.
SC-06	Zero trust. Architecture aligned with federal zero-trust guidance: no implicit trust based on network location, and continuous verification of users and devices.
SC-07	Mobile app security. Certificate pinning; secure local storage; no sensitive data in logs or notification previews. Rooted or jailbroken device detection warns the participant but does not lock them out, so device state never becomes grounds for adverse action.
SC-08	Testing. Independent penetration testing before launch, every year, and after major releases; continuous vulnerability scanning; a public vulnerability disclosure policy.
SC-09	Vendor obligations. Contracts MUST include breach-notification duties, flow-down of all privacy and security requirements to subcontractors, government ownership of all data, a ban on vendor secondary use (including training models on ISAE biometrics), and certified destruction at contract end.
SC-10	Incident response. A documented plan covering notice to affected participants in their language, the Privacy Office, and oversight bodies.

14. Legal Constraints

ISAE must stay inside existing law to be durable.

What the product relies on (existing executive authority):

- **Prosecutorial discretion and enforcement priorities.** In *United States v. Texas* (2023), the Supreme Court held that states lacked standing to challenge DHS's enforcement-priority guidelines, leaving the executive substantial room to set priorities.
- **Release with conditions.** For people not subject to mandatory detention, DHS may release on bond or conditional parole pending proceedings under INA § 236(a). ATD operates under this authority.

- **Parole**, only case by case for urgent humanitarian reasons or significant public benefit (INA § 212(d)(5)(A)).
- **Deferred action**, granted individually, with eligibility to apply for work authorization.

What the product must not do or imply:

- Create a new immigration status, or a path to permanent residence or citizenship. Those require an act of Congress; naturalization generally requires five years of lawful permanent residence.
- Waive statutory bars such as the three- and ten-year unlawful-presence bars, or override mandatory-detention provisions.
- Use categorical eligibility rules that invite litigation. DAPA was blocked, and in January 2025 the Fifth Circuit held DACA’s work-authorization and lawful-presence provisions unlawful while leaving its forbearance from removal in place. In November 2024 a federal court vacated the “Keeping Families Together” parole-in-place process.

Product implications:

ID	Requirement
LG-01	Eligibility and benefits MUST be decided case by case. The dashboard recommends a supervision pathway; it does not grant status or benefits by category.
LG-02	All participant-facing text MUST be reviewed by counsel so that nothing states or implies a path to status or citizenship.
LG-03	Where benefits are standardized (for example, Green Path step-downs), the program SHOULD use notice-and-comment rulemaking.
LG-04	The rules engine MUST track statutory and case-law changes (for example, the Laken Riley Act and litigation over <i>Matter of Yajure Hurtado</i>) through a counsel-owned change process.
LG-05	Privacy Act compliance (SORN, PIA, and any required computer-matching agreements) MUST be complete before data collection begins.

What Congress would need to do. A genuine earned-legalization path requires legislation, for example updating the INA § 249 registry date (today limited to people who entered before January 1, 1972) or enacting a conditional-status program such as H.R. 4393, the bipartisan Dignity Act of 2025. ISAE’s verified compliance export (GP-09) is designed to work alongside such legislation. The program should also seek explicit appropriations language and authorizing legislation to make it durable.

15. Pilot Plan and Success Metrics

15.1 Phases

Phase	Timing	Scope	Exit criteria
Phase 0: Readiness	Before month 0	PIA and SORN; legal sufficiency review; ATO; EOIR and USCIS agreements (or manual fallbacks); ATD contract modification; biometric threshold setting	All approvals in hand; thresholds met; benchmarks published

Phase	Timing	Scope	Exit criteria
		and independent testing; translation; pre-registration of the evaluation design and benchmarks	
Phase 1: Pilot	Months 0–12	Three to five ICE field offices with existing ATD contractor sites and established legal-service partners. Randomized or matched-comparison design where feasible. DHS's existing Case Management Pilot Program, run through CRCL with nonprofit providers, offers a governance model.	Pre-registered benchmarks met; no unresolved critical audit findings
Phase 2: Scale with evidence	Months 12–36	Expand only if pre-registered benchmarks are met. Publish results.	Benchmarks sustained at scale; quarterly public reporting in place

15.2 Metrics and baselines

Benchmarks are pre-registered before launch against a comparison group. The figures below come from the white paper and give context. They are not targets, because the populations differ.

Metric	Definition	Context from verified sources
Court-appearance rate	Share of scheduled hearings attended; all hearings and final hearings reported separately	Non-detained immigrants FY2008–2018: 83% attended all hearings; 96% of those with lawyers. ¹ ISAP II full-service, FY2011–2013: 99%, falling to 95% at final removal hearings. ² FCMP (vulnerable families): 100%, ICE-reported.
Absconder rate	Measured against active and unenrolled participants, per GAO	ATD overall: 16.2% (FY2021), 8.1% (FY2022), 12.8% (FY2023). FCMP: 23 of 954 (2%).
Check-in compliance	Share of scheduled check-ins completed; technical failures counted separately	FCMP: 99% compliance with ICE check-ins and appointments
Cost per participant per day, by tier	Fully loaded program cost divided by participant-days	ISAP IV, FY2023: \$4.11. FCMP, FY2016: about \$38.47 per family. Adult detention bed, FY2023: \$187.48.
Officer hours per case	Staff time per participant per month, by tier	No published ratio; enhanced case management capped at 40 per specialist. New measurement.
Milestone completion	Share reaching each Green Path milestone on schedule	New measurement
EAD issuance and tax filing	Share of eligible participants with an approved EAD; share filing taxes	New measurement. ITEP estimates that work authorization would raise annual tax contributions of the undocumented population by \$40.2 billion, from \$96.7 billion paid in 2022. ³

¹ U.S. Immigration and Customs Enforcement, *Budget Overview, Fiscal Year 2025 Congressional Justification* (DHS, 2024). Adult bed cost per day FY2023 actual \$187.48; ISAP IV FY2023 cost \$4.11 per participant per day; ECMS caseload of no more than 40 participants per case specialist; ATD absconder rates of 16.2% (FY2021), 8.1% (FY2022), 12.8% (FY2023); site tiers; 1–5 risk score; ISAP IV capabilities (SmartLINK, facial verification, telephonic reporting, GPS, court tracking, case management). https://www.dhs.gov/sites/default/files/2024-04/2024_0308_us_immigration_and_customs_enforcement.pdf

² DHS, *Privacy Impact Assessment for the Alternatives to Detention (ATD) Program*, DHS/ICE/PIA-062 (Aug. 2023). Describes SmartLINK's one-to-one facial verification, deletion of photos from the device, and location transmitted only at log-in or check-in; acknowledges storage in other ICE/DHS databases, contractor retention generally seven years after exit, and permanent retention in one case-management system pending linkage to ICE's removal module. <https://www.dhs.gov/sites/default/files/2023-08/privacy-pia-ice062-atd-august2023.pdf>

³ 8 C.F.R. § 274a.12(c)(11) (parolees) and (c)(14) (deferred action). <https://www.ecfr.gov/current/title-8/chapter-I/subchapter-B/part-274a/subpart-B/section-274a.12>

Metric	Definition	Context from verified sources
Civil-liberties indicators	Complaints; redress outcomes and turnaround; firewall requests; override disparities; biometric differentials; audit findings	New measurement; published quarterly
Public safety	New disqualifying arrests among participants versus the comparison group	New measurement

Honest cost framing. At the FY2023 ISAP IV rate of \$4.11 per day, five years of supervision costs about \$7,500 per participant (white paper calculation). That is not dramatically cheaper than one removal, which has cost \$10,854 on average (ICE, FY2016) and \$17,121 (DHS, 2025). The case for ISAE rests on detention avoided (about \$187 per day), a tax base kept and expanded, officer time saved for high-risk cases, and step-downs to lower-cost tiers as participants show compliance. Pilot reporting must not overstate savings.

15.3 Pilot stop conditions

The pilot **MUST** pause for review if any of the following occur: a confirmed firewall violation; a biometric threshold breach that is not promptly fixed; a security breach involving biometric or location data; a statistically significant deterioration in public safety compared with the comparison group; or a court ruling that removes the legal basis for a pilot component.

16. Risks and Open Questions

16.1 Risks

Risk	Likelihood	Impact	Mitigation
Function creep: enrollment data repurposed for enforcement operations	Medium	High	Technical and procedural firewall (12.2); purpose codes; public firewall register; IG audit
Low enrollment because of fear (chilling effect), especially in mixed-status families	High	High	Plain-language notices; outreach through trusted partners; firewall published and audited; no family data beyond need
Compliance below the 99% headline because of a lighter, app-heavy model	High	Medium	Fund real case management and legal orientation; publish honest baselines; tier by need
Face verification errors, uneven across demographic groups	Medium	High	NIST-based thresholds; field testing; human review; alternative check-ins; no adverse action on a failed match alone
Litigation against discretionary relief or categorical features	Medium	High	Case-by-case decisions; rulemaking where standardized; counsel-owned rules engine
Policy reversal or change in enforcement priorities	Medium	High	Minimization and short retention limit what could be misused later; seek authorizing legislation
Contractor control and security of sensitive data	Medium	High	Government data ownership; flow-down clauses; audits; certified destruction
Integration delays (EOIR, USCIS agreements)	High	Medium	Manual-entry and participant-upload fallbacks; pilot does not depend on feeds

Risk	Likelihood	Impact	Mitigation
Officer distrust or non-use of the dashboard	Medium	Medium	Co-design with field officers; fast, explainable recommendations; training; override audits used for learning, not punishment
Digital divide (no smartphone, low literacy, poor coverage)	High	Medium	SMS, voice, kiosk, and in-person channels; offline-first app; provided devices
Breach of biometric or location data	Low to medium	Very high	Encryption; separate stores; zero trust; penetration testing; incident response
False or doubtful 1:N face match at enrollment leads to wrongful suspicion	Medium	High	Lead-only rule (FE-05); any doubt defaults to follow-up fingerprints with no adverse action (FE-06, FE-07); human review of all possible matches; published 1:N thresholds

16.2 Open questions

1. **Firewall scope.** Is the proposed list of serious criminal grounds right, and should it be fixed in a directive, a regulation, or statute? May ISAE-captured information (as opposed to the address already in the immigration file) be used to locate a participant who has absconded under an executable final order?
2. **Legal basis per participant.** Which participants receive release under INA § 236(a) only, and which also receive deferred action or parole with work authorization? Who decides, and on what criteria?
3. **Biometric thresholds.** What numeric false non-match, false match, and demographic-differential thresholds will the governance board adopt, and who certifies the field test results?
4. **1:N face accuracy thresholds.** What false match and false non-match rates, and what demographic-differential limits, will apply to the one-time enrollment check (FE-05) at its operating threshold? Below what confidence does a result count as “doubt” that triggers follow-up fingerprints (FE-06)?
5. **1:N database coverage.** Which criminal-history databases may the enrollment check search, how complete and current are their photos, and how will gaps (for example, foreign records or records without photos) be disclosed and handled?
6. **Retention periods.** Will the Privacy Office and NARA approve the proposed periods? How will legacy ATD records of transferring participants be brought onto the ISAE schedule?
7. **EOIR and USCIS data.** Will DOJ agree to share hearing calendars and outcomes, on what timeline, and with what minimum dataset?
8. **Caseload capacity.** How many participants per officer can each tier support safely? This is unverified and must be measured.
9. **Check-in frequencies and step-down criteria.** What schedules and milestone thresholds produce good compliance at the lowest burden?
10. **Devices.** Who funds devices and data plans for participants without smartphones?

11. **Counsel access.** How much legal orientation and representation can be funded at pilot sites, given its strong link to appearance rates?
12. **Evaluation design.** Is randomization feasible and ethical at pilot sites, or must the evaluation use a matched comparison?
13. **Unsettled law.** How will the rules engine handle unsettled questions, such as litigation over *Matter of Yajure Hurtado*, without producing inconsistent outcomes across sites?
14. **Future status.** If Congress enacts a conditional-status program, what compliance record format would it accept, and should ISAE align its export to it now?
15. **State and local partners.** Should ISAE accept attestations from state or local partners (for example, school enrollment), and on what terms?

Appendix A: Verified Figures Used in This Spec

All figures come from the ISAE white paper, which verified them against the sources listed. “White paper calculation” marks simple arithmetic in the white paper, not an estimate by the cited organization.

Figure	Value	Source
People in ICE detention (July 11, 2026)	65,765	TRAC
Share of detainees with no criminal conviction	70.6%	TRAC
People monitored in ATD (July 11, 2026)	183,181	TRAC
Adult detention bed cost per day, FY2023	\$187.48	ICE FY2025 Congressional Justification
ISAP IV cost per participant per day, FY2023	\$4.11	ICE FY2025 Congressional Justification
Enhanced case management cap	40 participants per case specialist	ICE FY2025 Congressional Justification
ATD absconder rates	16.2% (FY2021); 8.1% (FY2022); 12.8% (FY2023)	ICE FY2025 Congressional Justification
FCMP court attendance / check-in compliance (as of March 2017)	100% / 99%; 23 of 954 absconded (2%)	DHS OIG-18-22
FCMP cost, FY2016	About \$38.47 per family per day	CRS R45804
ISAP II full-service court appearance, FY2011–2013	99%; 95% at final hearings	GAO, via CRS R45804
Non-detained immigrants attending all hearings, FY2008–2018	83%; 96% with lawyers	American Immigration Council
Average cost per removal, FY2016	\$10,854	ICE, via CNN Money
Average cost to arrest, detain, and remove (2025)	\$17,121	DHS
Taxes paid by undocumented immigrants (2022)	\$96.7 billion	ITEP
Added annual taxes with work authorization	\$40.2 billion	ITEP
Five years of supervision at \$4.11 per day	About \$7,500	White paper calculation
Biometric template deletion after exit	Within 90 days	White paper recommendation
Contractor record destruction (current ATD practice)	Generally seven years after exit	DHS/ICE/PIA-062

Appendix B: Glossary

Term	Meaning
1:1 verification	Comparing a live face capture with one enrolled template to confirm a claimed identity
1:N identification	Searching a face against a gallery of many people to determine who it is. Prohibited in ISAE.
ATD	Alternatives to Detention, ICE’s existing community supervision program
ATO	Authority to Operate, the formal security authorization for a federal system
CRCL	DHS Office for Civil Rights and Civil Liberties
EAD	Employment Authorization Document (work permit)
EOIR	Executive Office for Immigration Review (DOJ), which runs the immigration courts
FCMP	Family Case Management Program (2016–2017)

Term	Meaning
Green Path	ISAE's five-year milestone program that rewards compliance
ISAP IV	The current ATD contract, which includes the SmartLINK app
ITIN	IRS Individual Taxpayer Identification Number
PIA / SORN	Privacy Impact Assessment / System of Records Notice under the Privacy Act
Provisional Integration ID	A DHS-issued credential proposed in the white paper that records a participant's ISAE status, obligations, and milestones. It rests on existing authorities and is not an immigration status.
1:N identification	Searching one face against a gallery of many. Allowed in ISAE only once, at enrollment, as an investigative lead (FE-05).
Temporary Digital ID	A phone-based program ID sent by SMS or WhatsApp at enrollment, valid until the printed card arrives (FE-09).