KAIA-OR · DATASHEET · GOVERNMENT

Know what affects your posts, missions and staff abroad. Your officials decide.

Hazards, security incidents and disruptions matched to your sites and missions, each with source, corroboration status and confidence. Each traveller gets their own alerts. AI informs; people decide.

DOCUMENT ID	DS-GOVERNMENT
VERSION	1.0
DATE	3 November 2026
AUDIENCE	Government security directors responsible for field personnel, posts and missions

Who it's for

Government security leaders responsible for staff in the field, posts abroad and missions in volatile places. KAIA-OR Government gives the security team one shared picture to brief from, gives each traveller their own KAIA-OR, and keeps decisions with the officials responsible.

The challenge

- **Personnel in volatile places.** Information arrives late, or it is about a whole country rather than the post, the facility or the trip that matters.
- **A picture stitched together by hand.** Reports come from many places with no clear corroboration status, so the team cannot tell how far to trust them.
- **Targeted phishing.** Staff abroad, often working in more than one language, are the softest point for messages that ask for sign-in details or demand money.

What you get

A shared picture your team can brief from

Sites and missions in one picture, each event with its source, corroboration status and confidence, and unconfirmed reports labelled.

Staff abroad: what changed, and a second look

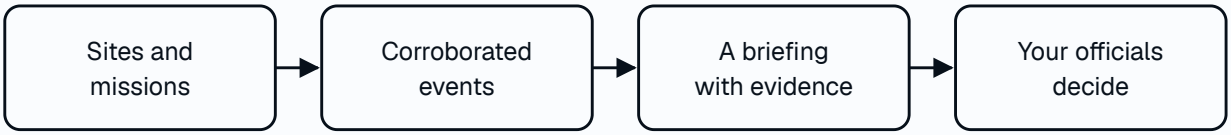
Each traveller sees which events touch their trip and what changed in the official travel advisory, and gets a second look at suspicious messages and links in English, French, Turkish or Hebrew. Each traveller's alerts follow their own trips.

AI informs. People decide.

Answers cite the evidence and are checked against it. Model output grants no authority, and scanning agents act only with your authorization. Government organizations start with cloud AI off.

© Kaia Technologies, Inc.

A day with KAIA-OR



One shared picture for the security team; each traveller keeps their own KAIA-OR.

1. The security team adds posts, facilities and mission sites to its shared picture.
2. When an event concerns a mission site, it appears with its source, corroboration status and confidence. Unconfirmed reports are labelled.
3. A member of staff about to travel sees what changed in the official travel advisory for their destination.
4. When a targeted message reaches a member of staff, they paste it in and see the warning signs and a suggested next step in their own language.
5. Hey KAIA, the KAIA-OR assistant, summarizes the evidence, and the officials responsible decide the next step.

Privacy and control

- Government organizations start with cloud AI off, and each person gives their own consent: nothing goes to cloud AI unless that person agrees first.
- The organization sees its sites, not its people's whereabouts. Each traveller's exact location stays on their own device.
- Roles manage membership, not people. Membership never grants access to another member's messages, devices, location or saved places. These membership boundaries, and the isolation between organizations, are enforced at the application layer.
- The Owner records dated access reviews of members and roles, and Owners and Administrators can download them.

Honest boundaries

- KAIA-OR informs. It does not issue an all-clear for a post, a facility or a trip.
- Missing or uncertain evidence never counts as a match or as safety, and a check that can't tell says so.

© Kaia Technologies, Inc.

- It does not provide travel assistance or evacuation services.
- Message and link checks show warning signs, not verdicts, and check only what staff choose to paste.
- Coverage depends on what official and authoritative sources publish. Reports that cannot be corroborated are labelled as unconfirmed.

Enterprise and government readiness

KAIA-OR fits the identity, security and governance tools an organization already runs.

Capability	What it means for you
Single sign-on and provisioning	Members sign in through your identity provider, and SCIM 2.0 creates and removes their accounts as your directory changes.
Passkeys and authenticator sign-in	Sign in with a passkey, or with your password and an authenticator app as a second step. Sign-in codes are never sent by text message.
Least-privilege roles	Define your own roles beside Owner, Administrator and Member, each with only the permissions it needs.
Audit log export	Export the organization audit log to your own security tools, beside the dated access reviews you already keep.
Data residency choice	Choose the region where your organization's data is held.
Cloud AI under your control	Turn cloud AI features off for your workspace. The control only restricts: it never turns cloud AI on for a member and never overrides a member's own choice.
Your tools, through the API	Send events and evidence to your own systems through the API and webhooks.

Platforms and languages

Platforms	iOS, iPadOS, macOS, Android phones, Android TV, Windows and the web.
Languages	English, French (Canada), Turkish and Hebrew, with full right-to-left layout.

One account works on every platform, with the same features and the same privacy rules.

Package

KAIA-OR Government. See Packages on the KAIA-OR website. Annual and multi-year terms are arranged with our team.

© Kaia Technologies, Inc.

Request early access

> Membership is by invitation. Request early access on the KAIA-OR website and choose Government, or choose Contact us on the KAIA-OR website.

© Kaia Technologies, Inc.

DS-GOVERNMENT · Version 1.0 · 3 November 2026

Capability availability depends on the edition and deployment. Capabilities are described as the committed KAIA-OR product scope.