KAIA-OR · USE-CASE BRIEF

Diplomatic security

Events matched to your posts and facilities in one picture, each traveller's own picture of their trips, and a second look at targeted phishing.

DOCUMENT ID	UCB-13-DIPLOMATIC-SECURITY
VERSION	1.0
DATE	3 November 2026
AUDIENCE	Diplomatic security and mission-support teams in government organizations

At a glance

Who it is for	Teams responsible for posts, facilities and staff who move between countries, often at short notice.
Outcome	Events matched to posts and facilities in one picture, each with its source, corroboration status and confidence; each traveller's own picture; and a second look at suspicious messages in four languages.
Package	KAIA-OR Government

The challenge

Missions operate in many countries at once, each with its own publishers, languages and warning systems. Information about an incident near a post is often late, written for a whole country, or not specific to the post at all. Staff move between posts and travel at short notice, and the evidence they need sits in different places.

Staff abroad are also frequent targets of phishing and impersonation designed to look like colleagues, partners or official correspondence. One reply to the wrong message can expose a person, a post or a mission.

© Kaia Technologies, Inc.

What changes with KAIA-OR

Posts and facilities in one picture

Hazards, security incidents and disruptions that touch a post or facility appear on the site they affect, with severity, confidence, source and corroboration status, and why they matched. Unconfirmed reports are labelled.

Staff abroad: what changed, and a second look

Each traveller keeps their own KAIA-OR. They see which events touch their trip and what changed in the official travel advisory, and they get their own alerts for their own trips.

A second look at targeted phishing

Each member of staff can paste a suspicious message to see the warning signs KAIA-OR recognizes, in English, French, Turkish or Hebrew. Links stay unopened. You see what looks wrong, when the check can't tell, and a suggested next step, such as confirming through a channel you already trust.

AI informs. People decide.

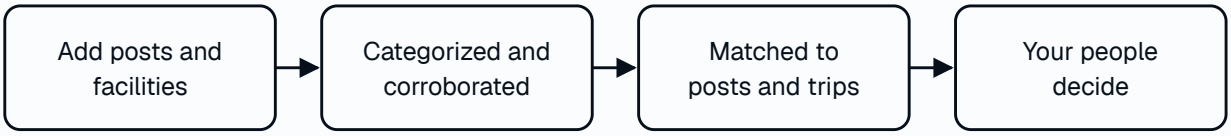
Government organizations start with cloud AI off. Answers from Hey KAIA, the KAIA-OR assistant, cite their evidence and are checked against it before anyone sees them. Model output grants no authority, and scanning agents act only within the limits you set and with your authorization.

What you see

Item	What it shows
An event at a post or facility	Category, severity, place, time window, confidence, source and corroboration status, and the reason it matched.
A traveller's own picture	What changed for their trip and which events touch it.
A message check	The warning signs recognized in the text and a suggested next step.
A link check	What in the address deserves a closer look, with the link left unopened.

© Kaia Technologies, Inc.

How it works



A shared picture of posts and facilities, and each traveller's own picture of their trips.

1. The security team adds posts and facilities to the organization's shared picture.
2. When an event published by official and authoritative sources concerns a post or facility, it appears on that site with its source, corroboration status, confidence and the reason it matched.
3. When a member of staff travels between posts, they see which events touch their own trip and what changed in the official travel advisory, in their own KAIA-OR.
4. When a message that appears to come from a colleague or partner contains requests for sign-in details or demands for money, the recipient pastes it in and sees the warning signs and a suggested next step.
5. The recipient checks with the sender through a channel they already trust, and the security team follows its own procedures.

© Kaia Technologies, Inc.

Privacy and control

- The organization sees its posts and facilities, 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 boundaries are enforced at the application layer.
- Government organizations start with cloud AI off, and each person gives their own consent: nothing goes to cloud AI unless that person agrees first.
- Single-use invitations, each bound to the invited person's account, and dated access reviews keep access accountable.

Honest boundaries

- KAIA-OR informs. It does not issue an all-clear for a post, a facility or a trip.
- 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.

Editions and related use cases

Diplomatic security is part of KAIA-OR Government. Annual and multi-year terms are arranged with our team. KAIA-OR runs on iOS, iPadOS, macOS, Android phones, Android TV, Windows and the web, in English, French (Canada), Turkish and Hebrew. One account works on every platform, with the same features and the same privacy rules.

Related use cases

- Force protection
- Executive and official awareness
- Travel risk

© Kaia Technologies, Inc.

Request early access

> Membership is by invitation. Request early access on the KAIA-OR website and choose Government. Enterprise and government teams can also choose Contact us on the KAIA-OR website.

© Kaia Technologies, Inc.

UCB-13-DIPLOMATIC-SECURITY · Version 1.0 · 3 November 2026

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