KAIA-OR · USE-CASE BRIEF

Force protection

Events matched to your installations, each with its source and corroboration status, so the decisions stay with commanders.

DOCUMENT ID	UCB-14-FORCE-PROTECTION
VERSION	1.0
DATE	3 November 2026
AUDIENCE	Force protection and installation security teams in government organizations

At a glance

Who it is for	Teams responsible for personnel and installations exposed to hazards, unrest and disruption, at home and abroad.
Outcome	Events matched to installations in one shared picture, each with its source, corroboration status and confidence. AI informs; commanders decide.
Package	KAIA-OR Government

The challenge

Installations and the people at them depend on information about hazards, unrest and disruption nearby, from publishers in many countries and languages. Reports arrive at different times. Some are corroborated and some are not, and the picture is often assembled by hand while a situation develops.

Any tool that informs these decisions must keep authority where it belongs: with the people accountable for personnel and installations. Automated output that acts on its own, or that cannot show its evidence, is not acceptable in this setting.

> Decisions about personnel and installations stay with commanders. KAIA-OR informs them; it never decides for them.

© Kaia Technologies, Inc.

What changes with KAIA-OR

Installations in one shared picture

Hazards, security incidents including unrest, and infrastructure disruptions that touch an installation appear on the installation they affect, with severity and why they matched.

Corroboration commanders can brief from

Each event carries its source, confidence and corroboration status. Unconfirmed reports are labelled, so a briefing can separate what is corroborated from what is still being reported.

Authority stays with people

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

Personnel: their own picture, and a second look

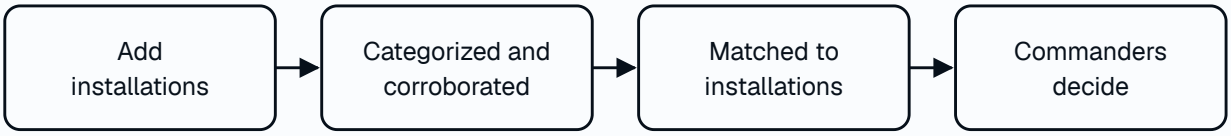
Each member of personnel keeps their own KAIA-OR for their own trips and gets their own alerts for them. They can paste a suspicious message or check a link while it stays unopened, in English, French, Turkish or Hebrew. You see what looks wrong, when the check can't tell, and a suggested next step, such as confirming through a channel you already trust.

What you see

Item	What it shows
An event at an installation	Category, severity, place, time window, confidence, source and corroboration status, and the reason it matched.
An unconfirmed report	A clear label, with its source, so it is never mistaken for a corroborated event.
A Hey KAIA answer	What an event means for an installation, with the evidence it rests on.
A scanning agent's work	Only what it was given authorization to do, within the limits you set.

© Kaia Technologies, Inc.

How it works



A shared picture of installations, with authority kept by the people accountable for them.

1. The team adds its installations to the organization’s shared picture.
2. When official and authoritative sources publish a hazard, an incident of unrest or a disruption near an installation, KAIA-OR categorizes it and shows how well independent sources corroborate it.
3. When the event concerns an installation, it appears there with its severity, confidence, source and the reason it matched. Unconfirmed reports are labelled.
4. When a staff officer asks Hey KAIA what the event means for the installation, the answer cites its evidence and relays the publisher’s own guidance.
5. Commanders decide the response under their own procedures. Model output grants no authority at any step.

© Kaia Technologies, Inc.

Privacy and control

- The organization sees its installations, not its people's whereabouts.
- Each person'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. Nothing goes to cloud AI unless each person agrees first, and only that person can give that consent.
- Single-use invitations, each bound to the invited person's account, and dated access reviews keep access accountable.

Honest boundaries

- KAIA-OR provides information, not orders. Model output grants no authority.
- It does not issue an all-clear for an installation or a movement.
- Scanning agents act only within the limits you set and with your authorization.
- Coverage depends on what official and authoritative sources publish. Reports that cannot be corroborated are labelled as unconfirmed.
- On hazards, KAIA-OR relays the publisher's own guidance and never writes its own safety instructions.

Editions and related use cases

Force protection 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

- Diplomatic security
- Emergency management
- Sites and natural hazards

© 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-14-FORCE-PROTECTION · Version 1.0 · 3 November 2026

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