JOINT WHITEPAPER

Turning Fraud Intelligence into Systemic Prevention with Baseline.ai

A joint partner white paper on AI-enabled identification, understanding and elimination of vulnerabilities across government programs.

October 2026

Overview

Fraud investigations often end when the case closes, but the vulnerability remains. Government benefit programs generate massive volumes of eligibility, payment, transaction, identity, case and investigative data. Traditional fraud solutions identify suspicious activity, but agencies struggle to connect investigations to the process, policy, data, and technology weaknesses that enabled the fraud. As a result, the same fraud patterns can reappear across programs such as SNAP, TANF, Medicaid, unemployment insurance, and other public benefits. Agencies need a repeatable way to convert fraud outcomes into enterprise intelligence, identify systemic exposure, govern mitigation, and verify that vulnerabilities have been actually been addressed.

Key Themes

Prevent Recurrence — Turn lessons from closed fraud cases into systemic controls designed to prevent the same exploitation from happening elsewhere.

Expand Fraud Intelligence — Correlate case, eligibility, payment, transaction, identity, employee, vendor, and external data to expose previously hidden relationships and patterns.

Create Measurable Accountability — Translate findings into governed Mitigation Requirements with owner, evidence, verification criteria, and closure decisions. The case is closed when the loophole is closed and verified.

Guided Workflow — Analysts are guided through an easy to use 5 step process to ensure no area is overlooked. The AI maximizes the Analyst's investigative experience

Intended Audience

This paper is designed for Federal and State CIOs, CTOs, Inspector General Offices, Government Accountability Offices, and Program Integrity Leads to investigate and eliminate fraud exposure to Government programs.

From Closed Cases to Corrective Action

Baseline.ai helps oversight and program-integrity organizations move beyond individual case disposition by examining how control weaknesses recur across investigations, documenting the underlying exposure, and establishing a governed path from finding to verified corrective action.

An Oversight-Centered Approach

Inspectors General and government auditors routinely identify questioned costs, control deficiencies, improper payments, recurring findings, and weaknesses in program administration. The challenge is converting those findings into an enterprise view of **why the weakness occurred, where else it may exist, and whether corrective action actually resolved the exposure.**

Baseline.ai supports that work by analyzing closed investigative and audit-related information, correlating relevant program and operational data, and surfacing recurring patterns that may indicate a systemic vulnerability rather than an isolated event.

What Baseline.ai Helps Oversight Teams Do

Identify recurring vulnerabilities. Compare closed cases and findings to expose common control, process, policy, data, or technology weaknesses.

Trace cause and exposure. Reconstruct how a transaction, approval, eligibility decision, or other program action moved through existing controls.

Establish accountable corrective action. Convert validated findings into governed Mitigation Requirements with owners, evidence, verification criteria, and closure decisions.

Preserve an audit trail. Maintain evidence and status showing what was identified, what action was taken, and how closure was validated.

Illustrative Use Case: Government Grant Fraud

Challenge. Closed SBIR grant fraud investigations revealed false or duplicative expenses, misrepresented payroll costs, and violations of funding requirements. Although individual matters were resolved, similar schemes across participating agencies raised a broader oversight question: were common program vulnerabilities allowing the same types of fraud to recur?

Analysis. Baseline.ai reconstructs the invoice approval workflow across closed cases and examines controls surrounding supporting documentation, validation rules, recipient and vendor data, and approval decisions. The objective is not simply to identify another suspicious transaction, but to determine the control weakness that allowed improper or fraudulent activity to pass through the program.

Corrective action and closure. Baseline.ai generates recommended corrective actions to strengthen validation, documentation, data correlation, and approval controls. Recommendations can be prioritized, assigned, supported with evidence, tracked through remediation, and maintained until the responsible organization validates that the identified vulnerability has been addressed.

1 FIND	2 ANALYZE	3 RECOMMEND	4 TRACK	5 VERIFY & CLOSE

Designed to Support - Not Replace - Professional Judgment

Baseline.ai is intended to augment investigators, auditors, evaluators, and program-integrity professionals. AI-assisted analysis can organize evidence, identify relationships, and surface patterns for review; determinations, recommendations, acceptance of corrective action, and closure remain governed by responsible officials and established oversight processes.

The result is a repeatable, evidence-oriented approach for turning lessons from completed work into stronger internal controls, measurable accountability, and reduced risk of recurrence across government programs.