ATARC

KEY TAKEAWAYS

ATARC Public Sector Law Enforcement Summit

Executive Summary

The ATARC Public Sector Law Enforcement Summit, held in September 2025, convened federal, state, and local law enforcement IT leaders to discuss strategies for strengthening digital infrastructure, cybersecurity, and the workforce supporting modern policing. Through keynotes and panel discussions, participants explored emerging policy and technology trends shaping the law enforcement community. This document recaps key insights from the event, focusing on fraud as a predictable risk in large federal programs, the data challenges that limit detection, and the potential for AI, analytics, and cross-agency collaboration to improve fraud prevention efforts.

1. Defining Fraud

Fraud is deliberate deception for unlawful gain, thriving in environments of scale, speed, and ambiguity.

Key elements include:

- **Intent: purposeful misrepresentation, not accidental error.**
- **Misrepresentation: false statements on qualifications, activities, or expenses.**
- **Financial impact: misuse of funds, improper benefits, loss of taxpayer dollars, or non-approved expenditures.**
- **Nonfinancial impact: national security and criminal risks, public harm, loss of trust in government**

Common examples: falsified records, inflated expenses, double-billing, and using funds for personal gain.

2. Fraud as a Predictable Risk

Fraud is not an edge case; it's a predictable outcome when programs move fast, operate at scale, and lack consistent controls.

Goal: remove ambiguity and add friction at critical points.

3. Detection Techniques

- **AI & Machine Learning: adaptive models that flag risk in real time.**
- **Anomaly Detection: identifies unusual activity before it escalates.**
- **Predictive Modeling: scores transactions by fraud likelihood.**
- **Biometrics & Behavioral Signals: stronger identity verification.**
- **Deepfake Defenses: detect manipulated media.**
- **Data Prerequisites: standardized, clean, and shareable data across agencies.**

4. Data Challenges & Practices

Analytics is critical to better fraud prevention and detection.

But to unlock the promise of enhanced analytics (ML/AI), we need better data. Current data limitations include:

- **Not collected, not standardized, different definitions (note recs from GAO)**
- **Siloed (within an agency and externally), residing in legacy systems that impede sharing/analytics**

Despite all the variation in data, fraud threats are fairly consistent across programs. Examples of progress include:

- **GAO's ontology and recommendations to OMB for standardization**
- **PRAC/COVID fraud enforcement task forces**
- **Treasury Do Not Pay system**

A broader, crosscutting approach that brings together programs, oversight entities, and private enterprises could drive progress. Approaches should be risk-based, considering:

- **Who is committing fraud (organized groups vs. opportunistic individuals)**
- **Impacts (financial and non-financial)**

5. Path Forward & Solutions

Getting there (delivering on the promise of ML/AI) requires:

- **Tools and resources (where public/private partnerships can help)**
- **Standard definitions and data structures across agencies and government levels**
- **Continuous training (fraud evolves, so must our responses)**
- **Agility: bad actors adopt new tools faster than government can; private sector often adapts more quickly**

6. Use Case: Federal Grants Fraud

Federal grants, with over $1 trillion awarded annually, present a high-value target for Return on Assets Employed (ROAE).

Challenges:

- **Lack of standardized data collection, definitions, and sharing**
- **Each grant program reviews independently with varying levels of sophistication**
- **Risks include duplicate benefits, hidden relationships, foreign influence, beneficial ownership, phoenix entities**

Proposed approach:

- **Start with publicly available data to explore feasibility**
- **Leverage GAO ontology for standard definitions and fraud typology**
- **Partner with private sector AI experts for refinement**
- **Conduct cross-program analysis to identify systemic risks**

7. Strategic Outlook

Fraud detection must be proactive, data-driven, and collaborative.

Real progress requires breaking down silos, building standards, and leveraging AI/ML.

Federal grants fraud is the ideal proving ground for testing scalable solutions with measurable ROI.