ATARC powered by GovExec

Fighting 21st Century Fraud with 20th Century Systems

Why Prevention Beats Recovery — and What's Finally Changing

IN PARTNERSHIP WITH

aws

"Fraud networks operate like startups — fast, coordinated, data-driven. Government still operates like a filing cabinet."

Executive Snapshot

The Problem: Federal agencies lose over $100 billion annually to fraud, waste, and abuse, yet most oversight systems were designed before the internet existed. Modern fraud networks move at digital speed, exploit program fragmentation, and adapt faster than government can respond.

The Opportunity: Agencies that invest in prevention over recovery are seeing dramatic returns. CMS stopped or recovered $41.9 billion in FY2025, a 59% increase year-over-year, demonstrating a 22-to-1 return on investment.[1]

Three Key Findings

1. **The "pay and chase" era is over.** Prevention must move upstream into operational gatekeeping. Once money leaves the system, recovery rates plummet.
2. **Government needs a "Fraud CVE" framework**. Cybersecurity shares threat intelligence in real time. Fraud prevention has no equivalent, agencies rediscover the same vulnerabilities independently.
3. **Technology alone won't solve this.** AI and analytics are accelerators, not substitutes for integrated governance, shared data, and executive accountability.

Call to Action: The federal government must transform fraud prevention from an isolated compliance exercise into a coordinated, intelligence-driven operational capability, matching the speed, adaptability, and collaboration of the adversaries it faces.

[1] https://www.cms.gov/files/document/cpi-roi-fy25-pdf.pdf

By the Numbers: The Scale of the Challenge

Before diving into findings and recommendations, consider the scale of what federal agencies are confronting:

$100B+

Annual fraud, waste, and abuse flowing through Medicare and Medicaid alone — out of a combined budget approaching $2 trillion

$41.9B

Stopped or recovered by CMS in FY2025 — a 59% increase over the prior year, demonstrating a 22:1 ROI

61%

Of high-risk providers in Minnesota that could not be revalidated — they vanished, did not respond, or could not prove legitimacy

4x

More hospice agencies than Starbucks in LA County[2], the predictable result of enrollment systems designed for a different era

CMS staff successfully enrolled a dog as a Durable Medical Equipment (DME) supplier using nothing more than basic bank account information[3]

These are not edge cases. They are the predictable outcomes of enrollment and oversight systems designed decades ago, now operating in an environment those designers never imagined.

[2] https://www.cbsnews.com/projects/2026/hospice-fraud/
[3] https://www.youtube.com/shorts/WdATCjDwXxI

Introduction: An Arms Race Government Is Losing

Federal agencies are confronting a fraud landscape that has evolved faster than the systems designed to defend against it. Across government, leaders responsible for financial oversight, grants management, investigations, analytics, cybersecurity, and operational integrity increasingly recognize that traditional approaches are no longer sufficient. Fraud schemes now move at digital speed, operate across programs and jurisdictions, and exploit fragmentation inside federal systems that were never designed for real-time coordination.

During a recent government-only roundtable conducted under Chatham House Rules, federal practitioners discussed the growing gap between the sophistication of modern fraud operations and the limitations of existing federal oversight models. Participants represented a broad cross-section of the federal ecosystem - oversight organizations, civilian agencies, financial management offices, law enforcement, technology leaders, and operational executives. The conversation revealed a strong consensus around one central idea: the federal government is still attempting to fight 21st century fraud with 20th century systems.

The discussion did not center on a single technology or a single agency challenge. Instead, participants repeatedly emphasized that fraud prevention is fundamentally an enterprise governance problem requiring alignment between people, process, data, policy, and technology. Artificial intelligence and advanced analytics may accelerate detection and investigation, but they cannot compensate for fragmented data, inconsistent controls, unclear accountability, or outdated operational workflows.

Critically, fraud rarely exists in isolation. Fraudsters target multiple programs simultaneously, exploit inconsistencies across agencies, and leverage gaps between federal, state, and local oversight structures. Meanwhile, agencies often investigate incidents independently, without shared visibility into patterns that span organizational boundaries. This fragmentation creates structural vulnerabilities that sophisticated actors increasingly understand how to exploit.

What emerged from the conversation was not pessimism, but ***urgency***. New analytical models, AI-assisted oversight tools, risk scoring systems, and integrated audit frameworks are already demonstrating measurable value. The challenge is scaling operational coordination across government while modernizing the institutional foundations that support trust, accountability, and stewardship.

The End of the “Pay and Chase” Era

> *Once money leaves the system, agencies are already operating at a disadvantage. Recovery operations are expensive, time-consuming, and often only partially successful.*

For decades, many federal programs have operated under a reactive framework in which payments are distributed first and oversight activities occur later. Investigations, audits, clawbacks, and prosecutions then attempt to recover improperly distributed funds after the fact. While this model reflected the operational realities of earlier eras, it now creates an unsustainable imbalance between fraud prevention and fraud recovery.

The structural roots of this vulnerability are often decades old. Medicare’s enrollment model, established in 1965, was built on an “any willing provider” philosophy with minimal barriers to entry, a design Congress has never meaningfully tightened. The consequences of that permissiveness are now well documented and startling:

- CMS staff successfully enrolled a dog as a DME supplier using nothing more than basic bank account information
- Los Angeles County has four times as many hospice agencies as Starbucks locations
- Miami-Dade County has as many DME companies as McDonald’s franchises[4]
- When Minnesota revalidated ~5,800 high-risk providers, 61% could not be found or verified

Modern fraud operations exploit speed, fragmentation, and automation. Fraud networks operate across multiple programs simultaneously, adapting quickly to policy changes and exploiting weak controls before agencies can respond. Federal systems designed primarily for compliance reporting and post-award oversight simply cannot keep pace.

[4] https://www.facebook.com/DrOzCMS/videos/seniors-pay-into-medicare-their-whole-lives-and-we-will-cherish-the-program-cms-/3824171387715846/

The Shift to Prevention

Agencies are beginning to shift toward preventive controls and real-time intervention models. Rather than focusing solely on identifying fraud after disbursement, organizations are investing in analytics capable of identifying anomalies before payments are approved:

- AI-assisted review processes that flag elevated-risk transactions in real time
- Predictive analytics that identify patterns preceding fraudulent activity
- Identity verification systems that validate providers and beneficiaries at enrollment

Integrated audit frameworks that monitor compliance continuously, not episodically

Importantly, prevention does not mean slowing legitimate service delivery. The goal is to introduce smarter controls that distinguish between normal operational activity and elevated risk behavior - balancing accessibility, speed, accountability, and stewardship.

Prevention changes the economics of fraud. When agencies establish visible controls, clear accountability mechanisms, and active monitoring processes, they alter the incentive structure facing potential bad actors. In some cases, simply signaling increased oversight can reduce opportunistic abuse before enforcement action becomes necessary.

A “Fraud CVE” for Government: The Missing Intelligence Framework

> *Fraudsters collaborate in real time. Government shares lessons in fiscal quarters.*

In cybersecurity, organizations benefit from mature mechanisms for sharing information rapidly. Common Vulnerabilities and Exposures (CVEs), threat intelligence feeds, and coordinated advisories enable organizations to identify and mitigate risks before incidents scale broadly.

No equivalent capability currently exists for fraud.

Agencies often encounter similar fraud schemes independently, yet there is no consistent mechanism for rapidly distributing structured information about emerging tactics, vulnerabilities, or operational weaknesses. As a result, organizations may unknowingly remain exposed to risks already identified elsewhere in government.

Roundtable participants proposed the concept of a “Fraud Vulnerability Equivalent” framework — a structured method for identifying, cataloging, and sharing fraud-related vulnerabilities across agencies. Such a framework could allow organizations to communicate patterns, indicators, control failures, and exploitation methods in a standardized way.

What a Fraud Intelligence Framework Could Enable

- **Earlier detection:** Agencies could identify emerging schemes before they scale across programs
- **Benchmarking:** Organizations could measure control effectiveness against government-wide standards
- **Prioritized mitigation:** Resources could focus on the highest-impact vulnerabilities first
- **Cross-agency awareness:** Situational understanding that spans organizational boundaries
- **Proactive prevention:** Strengthening controls before losses occur, not just investigating after

Such a framework would require careful governance. Fraud indicators are often sensitive, operationally complex, and potentially connected to ongoing investigations. Any information-sharing model would need strong protections around privacy, operational security, and legal authorities.

Nevertheless, the concept addresses one of the core asymmetries discussed throughout the roundtable: fraud networks collaborate and adapt rapidly, while government organizations often operate independently. Just as cybersecurity matured through shared standards, collective defense models, and operational collaboration, fraud management may require a similar transformation.

Data as the Foundation: Breaking Down Silos

Perhaps the most consistent theme across the roundtable was the recognition that data centralization and federated information sharing are foundational requirements for effective fraud prevention.

Today, critical fraud-relevant data often remains locked in agency-specific systems, incompatible formats, or legacy platforms that cannot communicate across organizational boundaries. Fraudsters exploit these gaps with impunity, targeting multiple programs simultaneously because they know no single agency has complete visibility.

The Path Forward: Federated Models

Participants discussed federated collaboration models that preserve privacy and governance protections while enabling cross-agency visibility. Key principles include:

- **Interoperability over centralization:** Agencies need not consolidate all data into a single system; they need systems that can communicate effectively
- **Real-time over retrospective:** Analytics must operate on current data, not quarterly reports
- **Shared standards:** Common data formats, risk taxonomies, and fraud indicator definitions
- **Privacy by design:** Information sharing that protects PII and sensitive investigation details

AI, machine learning, and advanced analytics serve as powerful accelerators in this environment, but only when built on integrated, high-quality data foundations. Without them, even the most sophisticated algorithms operate in isolation, detecting patterns within a single program while missing the cross-program coordination that defines modern fraud networks.

Leadership, Accountability, and the Export-Import Bank Model

Successful fraud prevention requires visible leadership commitment and embedded organizational accountability. When fraud prevention is treated solely as a compliance exercise or investigative responsibility, operational ownership remains fragmented. When executive leadership consistently reinforces it as a shared institutional responsibility, accountability becomes embedded across business functions.

Case Study: Export-Import Bank

Multiple roundtable attendees referenced the Export-Import Bank of the United States as a best-in-class example. The organization has integrated fraud risk management into executive governance structures and operational decision-making processes, demonstrating several characteristics participants viewed as exemplary:

- **Enterprise integration:** Fraud risk management is not isolated within technology teams or investigative offices — it is incorporated into broader governance involving executive leadership, operational stakeholders, and financial management
- **Clear definitions:** The organization grounds fraud management in clear operational definitions and legal frameworks, distinguishing fraud from general operational deficiency
- **Tailored strategies:** Fraud prevention approaches are customized to agency-specific operational realities and risk exposure
- **Connected disciplines:** Fraud controls are integrated with cybersecurity, financial management, operational governance, and customer trust — these domains increasingly intersect

Leadership engagement is especially critical during modernization efforts. Technology initiatives frequently fail when executive sponsorship weakens or operational ownership becomes unclear. Agencies making measurable progress are often those where leadership consistently aligns policy, operations, governance, and technology investments around shared objectives.

Accountability mechanisms must also extend beyond federal headquarters into the broader ecosystem of grantees, contractors, states, and external partners managing federal funds. Establishing expectations around controls, transparency, and stewardship creates stronger incentives for compliance and more sustainable operational discipline.

What to Do Monday Morning: A Roadmap for Action

The roundtable made clear that federal agencies are entering a transitional moment in fraud prevention. The question is no longer whether transformation is needed, but how quickly agencies can move. Here is a prescriptive roadmap based on the consensus findings:

Immediate Actions (0-90 Days)

1. **Conduct a fraud vulnerability self-assessment.** Map your agency's enrollment, payment, and award processes to identify points where controls are weakest or most outdated. Prioritize the highest-volume transaction pathways.

2. **Establish executive ownership.** Designate a senior leader accountable for fraud prevention outcomes (not just compliance reporting). Integrate fraud metrics into executive performance reviews.

3. **Inventory your data landscape.** Identify what fraud-relevant data exists across your agency, where it lives, and who can access it. Document the gaps that prevent cross-program visibility.

Near-Term Priorities (90-365 Days)

4. **Deploy pre-payment analytics.** Implement AI-assisted risk scoring on at least one high-volume payment stream. Even basic anomaly detection dramatically outperforms post-payment review alone.

5. **Initiate cross-agency intelligence sharing.** Establish bilateral or multilateral agreements with agencies facing similar fraud typologies. Begin with structured information exchanges, even informal ones.

6. **Conduct provider/recipient revalidation.** Following the Minnesota model, validate high-risk participants in your programs. The results may be revealing — and they will justify expanded prevention investment.

Strategic Transformation (1-3 Years)

7. **Build federated data infrastructure.** Invest in interoperable systems that enable real-time, cross-agency fraud intelligence without requiring full data centralization.

8. **Advocate for a government-wide Fraud CVE framework.** Champion the creation of standardized fraud vulnerability cataloging and sharing mechanisms — modeled on cybersecurity's proven approach.

9. **Embed prevention into culture.** Move beyond individual programs. Build fraud prevention into agency culture, performance management, and strategic planning as a permanent operational discipline.

Fraud Prevention Maturity: Where Does Your Agency Stand?

Based on roundtable findings, agencies can assess their current posture across five dimensions:

Dimension	Reactive (Legacy)	Proactive (Target)	Adaptive (Best-in-Class)
Detection	Post-payment audits	Pre-payment analytics	Real-time, cross-program AI
Data	Siloed, program-specific	Federated access across agency	Cross-agency intelligence sharing
Governance	Compliance-driven, fragmented	Executive-owned, integrated	Enterprise risk management
Response	Pay-and-chase recovery	Prevention-first controls	Predictive prevention + rapid response
Collaboration	Isolated agency efforts	Bilateral sharing agreements	Government-wide Fraud CVE ecosystem

Conclusion: The Next Generation of Federal Fraud Prevention

Federal agencies may still be fighting 21st century fraud with 20th century systems. But the conversation reflected growing consensus that transformation is not only possible, it is already underway.

CMS's $41.9 billion in stopped or recovered funds demonstrates that modernized prevention delivers extraordinary returns. The Export-Import Bank proves that executive-led governance creates durable institutional change. And the vision of a government-wide Fraud CVE framework points toward a future where agencies defend collaboratively rather than in isolation.

The central challenge is not simply adopting new technology. It is building operational ecosystems capable of matching the speed, coordination, and adaptability of modern fraud networks while preserving public trust, accountability, and mission delivery.

> *The next generation of fraud prevention will depend on changing not only the tools government uses, but the way government itself operates.*

If you do one thing: Stop treating fraud prevention as a compliance exercise. Start treating it as a strategic capability that protects the public trust, preserves taxpayer resources, and demands the same executive attention as cybersecurity.