Program Integrity Alliance

April 16, 2026

The Honorable Pete Sessions
Chairman, Subcommittee on Government Operations
Committee on Oversight and Government Reform
U.S. House of Representatives

The Honorable Kweisi Mfume
Ranking Member, Subcommittee on Government Operations
Committee on Oversight and Government Reform
U.S. House of Representatives

Re: Letter for the Record — Hearing on *Fraud Prevention: Understanding Fraud in Federally Funded Programs Run by the States,* April 15, 2026

Dear Chairman Sessions and Ranking Member Mfume:

The Program Integrity Alliance (PIA) submits this letter for the record in response to the Subcommittee's April 15, 2026, hearing on fraud in federally funded, state-administered programs. PIA is a nonpartisan; nonprofit organization focused on advancing structural reform of the federal government's fraud prevention infrastructure. We are founded by two Government Accountability Office (GAO) veterans who together led the development of GAO's Framework for Managing Fraud Risks in Federal Programs.

The April 15 hearing surfaced findings that PIA has documented for years. We commend the Subcommittee for holding it, and we commend the witnesses—Seto Bagdoyan of GAO, Kentucky Auditor Allison Ball, Dr. OJ Oleka, and Robert Westbrooks—for testimony that was candid, technically grounded, and appropriately urgent. This letter supplements their testimony with PIA's analysis of the structural barriers that must be addressed legislatively, and with specific proposals for doing so.

The Hearing's Diagnostic Findings Are Correct—and Incomplete

The testimony presented a clear and accurate diagnosis. The federal government loses between $233 billion and $521 billion to fraud annually. Medicaid alone generated $31 billion in improper payments in FY 2024. Unemployment insurance fraud during the pandemic reached an estimated $100 to $135 billion. The "pay and chase" model—paying first and investigating later—is the dominant posture, and it fails structurally. Prosecuting the nation's way out of the problem, as Bagdoyan testified, "addresses only a small fraction

of fraudulent activity, requires significant time and resources, and returns pennies on the dollar."

Westbrooks' framing was equally apt. Offenders today can purchase stolen identities for the price of a Happy Meal, file simultaneous claims across multiple states using automated tools, and operate from anywhere in the world. The fraud threat is not a policy problem in the traditional sense. It is an adversarial systems problem—one in which organized networks actively study and exploit the architecture of federal payment systems, and in which the government's own fragmented, siloed structure is the primary attack surface.

What the hearing did not fully address is why this architecture persists. The diagnosis focused, correctly, on symptoms, including weak controls, inadequate verification, data silos, and the absence of cross-program visibility. But the deeper question—why these conditions have continued despite more than a decade of GAO recommendations, IG findings, and legislative mandates—requires examining the *structural incentives* that make fraud prevention the institutional path of least resistance, and the *legal and technical barriers* that prevent agencies from acting even when they want to.

PIA has identified four systemic barriers that are not addressable through coordination directives alone:

1. A culture that rewards inaction. When agencies identify significant fraud, the result often looks like punishment in the form of congressional hearings, IG investigations, and political exposure—not recognition for vigilance. The rational institutional response is to avoid looking too hard. As Bagdoyan noted in his testimony, agencies have too long relied on "reactive" strategies; the GAO Fraud Risk Framework has identified five key areas requiring action, yet as of April 2026, 40 percent of GAO's 215 outstanding fraud risk recommendations remain open. The perverse incentive structure is the reason why.

2. A verification system built on trust, not data. Across Medicaid, SNAP, unemployment insurance, and housing assistance, eligibility is still primarily established through self-attestation. Ball's testimony documented the consequences: dead individuals enrolled in Medicaid, multiple people using the same Social Security number, ineligible noncitizens receiving benefits. These are not exceptions—they are the predictable result of a system that lacks real-time, independent verification.

3. A broken data ecosystem. The federal government holds enormous stores of data that could prevent fraud—IRS income records, SSA death data, state employment records, incarceration data. It cannot use most of it. The Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988 were written for paper-era bureaucracy, not

real-time digital verification, and require almost comically difficult hurdles to sharing data. Even where sharing is legally permissible, technical interoperability is frequently absent. The result, as GAO has documented, is that data that could prevent fraud sits unused in one agency's database while another agency pays a fraudulent claim.

4. Outdated technology. GAO has identified 11 legacy IT systems in the greatest need of modernization, many running COBOL or Assembly code, several with known cybersecurity vulnerabilities. Real-time fraud analytics require modern infrastructure. These systems cannot provide it. As Westbrooks testified, AI and automation now allow fraudsters to operate at industrial scale—yet the systems designed to stop them were, in some cases, built in the 1970s.

Until these structural conditions change, coordination will coexist with the fraud it is meant to prevent.

The Legislative Reforms the Subcommittee Should Prioritize

PIA has developed a comprehensive legislative reform agenda—the *Integrity Blueprint*—spanning seven thematic areas and 17 specific reforms. The following represent the highest-priority actions most directly responsive to the issues raised in the April 15 hearing.

Establish the Federal Payee Integrity System (FPIS)

The single most consequential structural reform available to Congress is the establishment of a Federal Payee Integrity System—a Treasury-operated, governmentwide orchestration platform that performs identity verification once and enforces payment integrity consistently across all federal and federally funded programs.

The FPIS consists of three integrated components: a *Federal Payee Registry* that assigns a unique, non-PII Payee ID to every individual or entity receiving federal funds and performs cross-program identity resolution and de-duplication; an *Eligibility Assertions Framework* that preserves program agency and state authority over eligibility determinations while standardizing how those determinations are conveyed to Treasury as a payment authorization credential; and a *Treasury Payment Control Plane* that screens all payments in real time before disbursement, enforcing the existence of a valid Payee ID and active eligibility assertion, and running centralized fraud and duplication checks.

The FPIS directly addresses the cross-program, cross-state fraud patterns documented at the hearing. Ball's finding of $836 million in concurrent Medicaid capitation payments for the same beneficiaries in multiple states is precisely the kind of fraud the Federal Payee Registry would detect automatically. Westbrooks' description of fraudsters filing

simultaneous claims across programs is the exact attack surface the Payment Control Plane is designed to close.

Critically, the FPIS is designed to *complement*, not replace, program agency and state authority. Eligibility decisions remain with the programs that make them. Treasury enforces payment integrity—it does not adjudicate eligibility. This separation is essential to preserving federalism and avoiding the centralization concerns that would otherwise impede adoption.

PIA has developed a detailed implementation roadmap for FPIS, available to the Subcommittee upon request. The system can be deployed incrementally, with Phase 1 delivering standalone value through cross-program deduplication before any enforcement capability is activated.

Modernize Privacy Law to Enable Responsible Data Sharing

Every reform in this space ultimately runs into the same wall: the Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988, which were not written for real-time fraud prevention. GAO's testimony noted that one state agency is restricted by law from sharing information with other programs in the same state. This is not an anomaly. It is the structural condition in which federal fraud prevention operates.

Congress should enact legislation that explicitly authorizes privacy-preserving record linkage and cryptographic matching for fraud prevention purposes, streamlines Computer Matching Agreement procedures for program integrity infrastructure, and creates clear statutory authority for limited, de-identified use of IRS income data for payment verification. None of these reforms require weakening privacy protections—they require modernizing them so they reflect technological reality and the public interest in protecting the programs that millions of Americans depend on.

Fraud networks do not respect data silos. The government's defenses should not be legally required to.

Strengthen and Enforce PIIA's Fraud Risk Management Requirements

The Payment Integrity Information Act of 2019 (PIIA) requires agencies to conduct fraud risk assessments—but its mandate expired after fiscal years 2019 and 2020, OMB lacks clear enforcement authority, and agencies are not required to measure whether prevention controls are actually working. Congress should amend PIIA to make annual fraud risk assessment a permanent requirement, authorize OMB to impose corrective action plans on non-compliant agencies, and require agencies to report on control effectiveness—not just fraud detection. As Bagdoyan testified, 40 percent of GAO's outstanding fraud

recommendations remain open. A stronger PIIA with enforcement teeth is the mechanism for changing that.

Expand the False Claims Act to State-Administered Federal Programs

The False Claims Act—the government's primary tool for fraud recovery through qui tam enforcement—does not apply to fraud in state-administered federal programs such as Medicaid, SNAP, TANF, and unemployment insurance. This is a significant gap. Congress should extend FCA liability to states administering federal benefit programs using federal funds, permit qui tam actions for fraud in those programs, protect state employees who report fraud from retaliation, and authorize federal takeover of qui tam claims where states have a conflict of interest.

Protect and Fund the Inspectors General

Westbrooks' testimony raised a point that deserves explicit emphasis: the USDA OIG's budget submission calls for an approximate 14 percent decrease from FY 2026. PIA shares this concern across the IG community. Independent oversight is where accountability enters the equation. For decades, GAO and the IGs have served as the federal government's most important sources of systemic fraud intelligence. Weakening them in the middle of an administration-wide fraud prevention initiative is incoherent. Congress should provide dedicated appropriations for all federal IGs to conduct fraud investigation and audit work, authorize IGs to issue mandatory-response recommendations to agencies on fraud prevention, and strengthen IG access to agency records and systems.

A Concern the Subcommittee Should Address: Honest Reporting Requires Safe Harbor

The administration's concurrent approach of threatening to withhold federal matching funds from states that are found to have fraud vulnerabilities creates a significant implementation risk that this Subcommittee is well-positioned to address.

If submitting an honest fraud vulnerability assessment triggers financial penalties, the rational response—for agencies and states alike—is to produce an assessment that is complete enough to satisfy oversight requirements, but not so candid that it becomes an enforcement target. This is not hypothetical. CMS recently acknowledged a tenfold error in its fraud accusations against New York's Medicaid program, having used that inflated figure as the basis for a formal investigation and funding threat before the math was checked. The effect of "accuse now, verify later" enforcement on voluntary candor cannot be overstated.

The cultural barrier that Bagdoyan, Ball, and Oleka all identified—the institutional taboo around admitting fraud—is only made worse by an enforcement dynamic that transforms

honest self-disclosure into a financial liability. Congress should legislate a clear safe harbor: a formal distinction between the state or agency that is *hiding* fraud and the one that has finally *found* it. These are not the same problem, and they should not receive the same response. Building that distinction into the legal framework would do more to unlock honest vulnerability assessments than any number of taskforce directives.

Directives Must Be Accompanied by Appropriations

Every agency that testified before this Subcommittee is being asked to do more with infrastructure built for a different era. Real-time analytics require modern systems. Cross-program verification requires data integration. All of this requires sustained investment, and none of it happens through executive directives alone.

The administration's March 2026 fraud task force executive order conditions implementation on "the availability of appropriations." That phrase, as PIA has noted, is a hedge—and it is likely the single most important variable in determining whether the current moment produces lasting change or a well-documented compliance cycle.

Congress should treat fraud prevention infrastructure as a capital investment with returns measured in hundreds of billions of dollars annually. The cost of modernizing the critical legacy systems GAO has identified, establishing the systems needed to verify information prior to making a payment, and funding the IGs to oversee the work is a fraction of the savings those investments would generate.

Conclusion

The April 15 hearing demonstrated that the diagnostic work has been done. GAO, the IG community, and state auditors like Allison Ball have documented the problem well. The question before this Subcommittee is whether Congress will provide the statutory authority, the appropriations, and the institutional architecture that would allow the government's fraud prevention posture to actually change.

PIA's *Integrity Blueprint* and our detailed Federal Payee Integrity System proposal are available in full, and we would welcome the opportunity to brief Subcommittee staff. The reforms we have described are not aspirational—they are technically specific, grounded in existing legal precedent, and designed to be deployed incrementally. Several countries with comparable challenges have built versions of this infrastructure. The United States has the data, the technical capacity, and now, with this Subcommittee's engagement, the political attention. What has been missing is the system that can say no before the money goes out.

Respectfully submitted,

Linda Miller,
President, Program Integrity Alliance
linda.miller@programintegrity.org

The Program Integrity Alliance is a nonpartisan 501(c)3 organization whose mission is to strengthen public integrity through data, evidence, and innovation. Learn more at www.programintegrity.org