WAGNER PROGRAM SERVICES

WHITE PAPER · AUGUST 2026

When Compliance Fails: The Real Cost of Weak Compliance Management in Government Contracting

Federal enforcement just posted its largest year on record. Across defense, financial and payment programs, small business set-asides, and grant-funded work, the pattern is the same: the contractors paying the price are not the ones who set out to defraud the government — they are the ones whose compliance programs could not keep up with what they had already promised.

EXECUTIVE SUMMARY

Compliance risk is now contract risk — and enterprise risk

In fiscal year 2025, the Department of Justice recovered more than **$6.8 billion** under the False Claims Act — the highest single-year total in the statute's history.[1] Whistleblowers filed a record **1,297** new suits, and the government self-initiated **401** investigations of its own.[1] Behind those numbers is a shift every contractor should internalize: enforcement no longer waits for fraud. It increasingly targets the gap between what a contractor *certified* and what its compliance program can actually *demonstrate*.

$6.8B	1,297	401	3×
FCA settlements and judgments in FY2025 — an all-time record	New whistleblower (qui tam) suits filed in FY2025 — also a record	Investigations DOJ opened on its own initiative in FY2025	Damages multiplier under the FCA, plus $14,308–$28,619 per claim

Sources: U.S. Department of Justice FY2025 False Claims Act statistics; 2025 inflation adjustment to FCA civil penalties.[1,2]

This white paper examines how poor compliance management converts into concrete loss across the major sectors of government contracting — defense and aerospace, federal financial and payment programs, small business and set-aside programs, and emergency or grant-funded work. In each sector the mechanics differ, but the failure mode is constant: certifications and representations are made at proposal time, the operational program never catches up, and an auditor, examiner, or insider eventually documents the difference.

The consequences extend far beyond the settlement figure. Treble damages and per-claim penalties are only the entry point; suspension and debarment can eliminate every federal revenue stream at once, degraded past performance ratings follow a company into every future evaluation, and executives face personal liability. Meanwhile, the single largest source of enforcement — the whistleblower — is usually a current or former employee who watched a known gap go unaddressed.

The conclusion is practical, not alarmist: a compliance program that exists on paper but not in operations is not a neutral deficiency. In today's enforcement climate it is an accumulating liability, priced in treble damages. The final sections of this paper describe why programs fail and what a defensible, examination-ready compliance function actually looks like.

SECTION 01

The enforcement climate: certification is the new battleground

The False Claims Act remains the government's primary enforcement instrument against contractors, and its center of gravity has moved. Classic procurement fraud — billing for work never performed — still occurs, but the growth area is **certification-based liability**: the theory that when a contractor represents compliance with a material requirement (small business status, pricing data accuracy, quality standards, data safeguards) and bills the government anyway, every invoice can become a false claim. FY2025 saw this theory applied across program areas, including more than $52 million recovered across nine settlements involving contractors that attested to controls their operations did not maintain.[1]

Three features of the current environment deserve particular attention.

Enforcement is increasingly self-initiated

The 401 investigations DOJ opened on its own in FY2025 reflect growing use of data analytics across billing, certification, and award databases. Agencies cross-reference what contractors certify against what other data shows. A contractor no longer needs an accuser to draw scrutiny — an anomaly is enough.

The whistleblower pipeline is at full capacity

Qui tam relators filed 1,297 new actions in FY2025 and were responsible for more than $5.3 billion of the year's recoveries.[1] Relators are overwhelmingly insiders: employees, compliance staff, and subcontractor personnel with firsthand knowledge. A known-but-unremediated gap is precisely the fact pattern that produces a relator — and rewards them with a share of the recovery.

The arithmetic is punitive by design

FCA damages are trebled, and each false claim carries a civil penalty of $14,308 to $28,619 after the 2025 inflation adjustment.[2] Because every invoice, progress payment, or claim line can count separately, penalties alone can dwarf the underlying contract value on high-volume work. Settlement negotiations start from that arithmetic.

> *"Enforcement no longer asks whether you intended to defraud. It asks whether you can produce evidence that you did what you certified — and a program that cannot produce evidence loses that argument by default."*

SECTION 02

Where the risk lives: sector by sector

A Defense & aerospace: pricing integrity under the microscope

Defense contractors face the oldest and best-resourced enforcement infrastructure in government: DCAA audits, DCMA surveillance, and truthful cost or pricing data requirements. FY2025 produced major recoveries rooted not in phantom billing but in **pricing and disclosure failures** — the kind of issues an internal compliance function should catch first.

FY2025 OUTCOMES — A defense contractor paid **$428 million** to resolve allegations of false pricing data and double-billing; a communications equipment supplier paid **$62 million** over undisclosed pricing; a military aircraft matter settled for **$29.7 million** over defective pricing.[1]

Estimating systems, cost accounting disclosures, and subcontractor flow-downs are compliance-managed artifacts. When they drift out of sync with actual practice, every certified proposal becomes potential FCA exposure.

B Financial & payment programs: where the obligations compound

Contractors that administer, process, or support federal financial and payment programs carry the densest compliance load in government contracting. Federal agencies estimated **$186 billion** in improper payments in fiscal year 2025 — up $24 billion year over year, across 64 programs.[3] The operations where those payments succeed or fail are largely contractor-run: eligibility verification, documentation standards, servicing, case processing, and recovery.

The exposure here is structural rather than occasional. Under the Payment Integrity Information Act, agencies must estimate improper payments, classify root causes, and demonstrate reduction — and their Inspectors General grade them annually. A contractor whose documentation or verification quality slips does not simply miss a service level; it degrades a compliance number the agency reports to Congress. Half of major agencies failed at least one PIIA criterion in FY2025.[3] Health-related matters, meanwhile, remain the single largest share of FCA recoveries year after year, and that exposure reaches the contractors supporting those programs, not just the providers billing them.

SECTION 02 · CONTINUED

C Small business & set-aside programs: status is a certification too

Set-aside programs — SDVOSB, 8(a), HUBZone, WOSB — are under intensified scrutiny as SBA eliminates self-certification and enforcement agencies pursue pass-through arrangements. Eligibility, affiliation, and limitations on subcontracting are living compliance obligations, not one-time registrations.

JUNE 2026 — Two contractors and their executives agreed to pay **$21.3 million** for using purported SDVOSBs as pass-through fronts that kept only 1–3% of contract value while the larger firms ran the work. Two whistleblowers shared **$3.67 million** of the recovery.[4]

Primes are not insulated: teaming with an ineligible small business, or failing to monitor subcontracting-plan performance, creates exposure on both sides of the agreement.

D Emergency & grant-funded work: speed leaves a paper trail

Pandemic-era programs generated **more than 200 FCA settlements totaling over $230 million** in FY2025 alone — years after the funds were disbursed.[1] The lesson generalizes to every surge-funded program: when money moves faster than controls, the documentation gap does not disappear. It waits. Contractors performing grant-funded or emergency work should assume that today's relaxed intake will be examined against tomorrow's full standard.

THE COMMON THREAD

Across all four sectors, the failure is rarely the absence of a rule anyone knew about. It is the distance between an obligation accepted at award and an operation that can prove, on demand, that the obligation was met. That distance is invisible internally — and obvious to the first examiner who asks for evidence.

SECTION 03

Beyond the settlement: the full consequence cascade

The settlement figure is the most visible cost of a compliance failure. It is rarely the largest. A single sustained finding can trigger every item below — and several of them compound each other.

- **Treble damages and per-claim penalties.** FCA liability is three times actual damages plus $14,308–$28,619 per claim. On invoice-heavy contracts, penalties alone can exceed total contract revenue.[2]
- **Suspension and debarment.** A government-wide exclusion from all federal awards — not just the affected contract. Debarment decisions turn heavily on whether the contractor is "presently responsible," which is, in practice, an evaluation of its compliance program. Companies have lost their entire federal pipeline over conduct on one vehicle.
- **Past performance damage.** Adverse CPARS ratings and terminations for default follow a contractor into every future source selection, suppressing win rates for years — a cost no settlement agreement caps.
- **Loss of program eligibility.** Set-aside status, facility clearances, and agency-specific qualifications can be revoked independently of any court outcome, eliminating the revenue base a small or mid-sized firm was built on.
- **Individual liability.** Executives and owners are increasingly named personally — as in the June 2026 SDVOSB matter, where the CEO and president were parties to the $21.3 million resolution.[4]
- **Remediation under supervision.** Post-settlement compliance obligations — independent monitors, corporate integrity agreements, enhanced reporting — force the contractor to build, at premium cost and on the government's schedule, the very program it declined to build voluntarily.
- **Teaming and market consequences.** Primes screen partners for compliance posture; a public enforcement action makes a firm a flow-down risk that competitors are quick to point out.

SECTION 04

Why compliance programs fail

Almost no contractor sets out to be non-compliant. The failures that end in enforcement follow recognizable patterns — and every one of them is a management failure before it is a legal one.

The program is a document, not an operation

Policies were written for a proposal or an audit and never wired into daily work. Controls exist in a binder; no one executes them, tests them, or owns them. The first serious examination exposes the gap in an afternoon.

Certification drift

Representations made at award — security scores, small business status, pricing data currency, quality processes — are treated as historical events instead of living obligations. The business changes; the certifications are never revisited. Every invoice submitted in the interim accumulates exposure.

Corrective actions that never close

Findings are logged, assigned, and forgotten. An open corrective action is discoverable evidence that the contractor knew about a deficiency and failed to fix it — the exact scienter narrative an FCA complaint is built on.

No metrics, no early warning

Without KRIs and KPIs, leadership learns about compliance deterioration from the government instead of from its own dashboard. By then the options are all expensive.

No one who has sat across from a regulator

Programs designed by people who have never faced an examination are designed for internal comfort, not external scrutiny. They document activity instead of evidence, and they answer questions no examiner asks while leaving the real ones exposed.

> *"An open finding is not a to-do item. In an enforcement file, it is proof of knowledge."*

SECTION 05

What effective compliance management looks like

A defensible program is not the biggest one — it is the one that can produce evidence on demand. Five capabilities separate contractors who survive examinations from those who fund enforcement statistics.

1 · Risk assessment that drives design

Start from the obligations actually in your contracts — clauses, certifications, flow-downs — and rank them by enforcement consequence, not administrative convenience. The program is built against that map, so effort lands where liability lives.

2 · Controls that are executed and tested

Every material obligation has an owner, a control, and a QC/QA loop that independently verifies the control works. Testing evidence is retained in examination-ready form — because the difference between compliance and provable compliance is the whole game.

3 · Certification lifecycle management

Every representation to the government is inventoried, assigned, and re-validated on a schedule — security postures, size status, pricing data, quality standards. Nothing signed at award is left to drift.

4 · Case and corrective action management that closes the loop

Findings move through intake, root cause, remediation, and verified closure with dates and evidence. Closed means proven closed — the record that turns a finding from a liability narrative into a responsibility narrative.

5 · Metrics and examination readiness

KRIs and KPIs give leadership early warning; a standing examination-response capability means an audit notice triggers a process, not a panic. Contractors who practice being examined perform differently — and regulators notice.

None of this requires a Fortune 500 compliance department. It requires deliberate design, honest testing, and leadership that treats compliance as a performance function — the discipline is the differentiator, not the headcount.

ABOUT WAGNER PROGRAM SERVICES

We don't just execute controls.
We defend them — directly to regulators.

Wagner Program Services LLC is a Service-Disabled Veteran-Owned Small Business providing regulatory compliance support to federal prime contractors: compliance program design and build-out, QC/QA development, regulatory examination and audit response, risk assessment, KRI/KPI development, and corrective action management. Our experience is regulator-facing — programs designed from zero, led at the director level, and defended in live examinations.

SDVOSB

Certified Service-Disabled Veteran-Owned Small Business — 100% of revenue counts toward SDVOSB subcontracting goals.

REGULATOR-FACING

12+ years of regulatory leadership, including direct examination response and remediation oversight.

IDENTIFIERS

UEI CZCNFX3F92X5 · CAGE 18TG4 · NAICS 541611, 541618, 541690, 541990

Let's see where you stand.

jon@wagnerprogramservices.com
(804) 399-6604 · Phoenix, AZ

SOURCES & NOTES

1. U.S. Department of Justice, False Claims Act settlements and judgments statistics for fiscal year 2025 (announced January 2026), as summarized in contemporaneous analyses by Holland & Knight, Seyfarth Shaw, and Paul Hastings.
2. Civil Monetary Penalties Inflation Adjustment, effective July 3, 2025: FCA per-claim penalty range of $14,308–$28,619; damages trebled per 31 U.S.C. § 3729.
3. U.S. Government Accountability Office, "Payment Integrity: Agencies' Estimated Improper Payments Increased to $186 Billion in Fiscal Year 2025" (GAO-26-108694), including Payment Integrity Information Act compliance results reported by agency Inspectors General.
4. U.S. Small Business Administration & U.S. Department of Justice, June 9, 2026: $21.3 million resolution of SDVOSB pass-through scheme (Broadway Electric Inc., Cornerstone Contracting Inc., and executives).