FCPA Enforcement is Back: Is Your Compliance Program Ready?

By Allison Spagnolo, Crystal Jezierski, and Melissa Price

The Department of Justice (DOJ) message at the recent American Conference Institute Foreign Corrupt Practices Act (FCPA) conference was clear: FCPA enforcement is alive and well.

Deputy Attorney General Todd Blanche, Acting Assistant Attorney General Matthew Galeotti, and FCPA Unit Chief David Fuhr confirmed that after the pause in early 2025, enforcement has returned to a "more traditional cadence." Even more striking: the DOJ's whistleblower program has received more than 1,100 submissions since launch, with over 50 percent referred to prosecutors for investigation.

What's Changed in the June 2025 FCPA Guidelines

The June 2025 FCPA guidelines refocused enforcement on cases that:

- Impact U.S. competitive interests (including bribery by U.S. companies)
- Involve cartels and transnational criminal organizations
- Threaten national security
- Connect to trade fraud, sanctions evasion, and healthcare fraud priorities

DAG Blanche made it clear: these guidelines "are not shields for criminal conduct." With individual accountability at the forefront and a new department-wide corporate enforcement policy on the horizon, every company with international operations needs a robust compliance program.

The New Corporate Enforcement Policy: What to Expect

In the coming weeks, the DOJ will announce a single, department-wide corporate enforcement policy applying to all criminal cases. This unified policy will provide greater certainty and transparency across prosecutors.

Core tenets will include:

- Incentivizing self-disclosure and cooperation
- Ensuring individual accountability: "companies do not go to jail—people do"
- Applying evidence-based approaches to enforcement

Combined with the expanding whistleblower program and increasing case volume, the time for complacency has passed.

The Urgency Is Real

David Fuhr confirmed case volume has picked up in the second half of 2025, with voluntary self-disclosures increasing significantly. The DOJ expects to announce a mix of corporate and individual enforcement actions in 2026. Meanwhile, since expanding in May 2025 to cover trade fraud, customs violations, and sanctions offenses, 80 percent of new whistleblower tips have been referred to prosecutors.

What this really means for companies is you can pay for compliance on your own terms now or you can pay more when the DOJ gets involved. In our experience, it is much better to be in control of the timing, scope, and reach of compliance assessments. While this is still an investment in time, effort, and funds, it allows your company to avoid fines and reputational harm.

Three Questions to Stress-Test Your Compliance Program

1. When did you last conduct a comprehensive third-party risk assessment?
Third-party relationships remain the highest-risk area for FCPA violations. With heightened focus on supply chains potentially infiltrated by cartels or TCOs—especially in Latin America—do you really know who you're doing business with?

Your assessment should go beyond traditional due diligence. Consider whether your third-party vetting processes can identify:

- Connections to transnational criminal organizations or cartels
- Links to sanctioned entities or individuals
- Exposure to DOJ priority sectors (defense, critical infrastructure, emerging technologies)
- Red flags related to customs and trade fraud

Effective disclosure requires effective detection—you can’t report what you don't know about. If your last assessment was before June 2025 or before the whistleblower program expansion, it’s time for a refresh.

2. Do you understand your exposure to new priority areas and individual accountability risks?

Anti-corruption compliance can no longer operate in a silo. Does your program address the intersection of FCPA risks with national security, cartel activity, trade fraud, or sanctions exposure?

With DOJ’s emphasis on individual accountability, your compliance program should:

- Map individual responsibilities for key compliance functions
- Document decision-making and approval chains for high-risk transactions
- Ensure leadership understands personal exposure
- Create clear escalation pathways

The forthcoming policy will emphasize cooperation and self-disclosure, but cooperation means quickly identifying culpable individuals when issues arise.

3. Is your compliance program agile enough for this enforcement environment?

The DOJ emphasized programs must adapt to rapidly evolving risks and priorities.

An agile program means:

- **Regular risk assessments** reflecting current DOJ priorities
- **Dynamic training** beyond annual checkboxes to address emerging risks
- **Robust internal reporting** encouraging employees to report internally before going to DOJ
- **Rapid response capabilities** to investigate and self-disclose within the 120-day window

Evaluate whether your program can pivot quickly enough to address new risks before they become enforcement actions.

Focused Risk Assessments & Due Diligence

Don’t wait for enforcement to find you. Many organizations find value in bringing in an external perspective to validate assumptions, uncover blind spots, and benchmark program maturity against current standards. An experienced third-party compliance advisor, such as Guidepost Solutions, can help organizations navigate these shifts with independent assessments, practical insights, and support in strengthening program agility. We have helped companies benefit from regularly pressure-testing their programs against emerging risks and evolving DOJ expectations that includes refreshing third-party due diligence, reassessing exposure to cartel/TCO, sanctions, and national security risks, and ensuring accountability structures are well-defined and documented for cooperation credit.