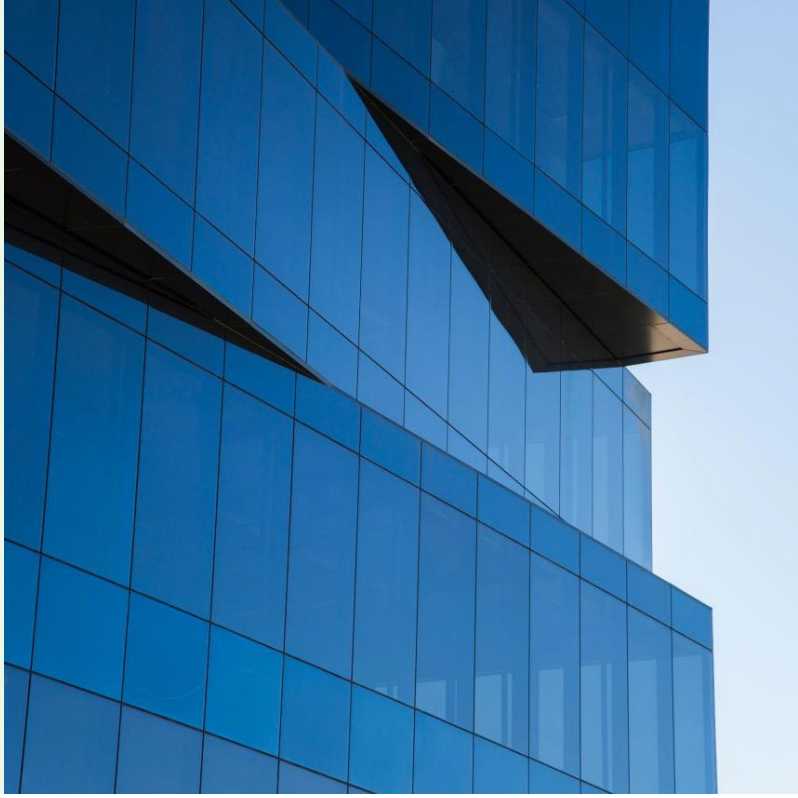
Clifford Chance

BRIEFING



October 2025

# DON'T WAIT FOR THE KNOCK: RIGHT-SIZING COMPLIANCE IN A SHIFTING ENFORCEMENT LANDSCAPE

As compliance professionals have observed, recent shifts in U.S. corporate enforcement priorities have altered the risk landscape for multinationals both foreign and domestic. We discussed in June 2025 one key component of this shift: the U.S. Department of Justice's new "Guidelines for Investigations and Enforcement of the Foreign Corrupt Practices Act (FCPA)," the marquee American foreign bribery law. On top of this development, a slew of other recent policies and guidelines have ramped up the pressure on multinationals to right-size their compliance programs to ensure that they adequately meet these new enforcement priorities and expectations.

## KEY ISSUES



### UNDERSTANDING NEW ENFORCEMENT PRIORITIES AND EXPECTATIONS

On May 12, 2025, the U.S. Department of Justice ("**DOJ**") issued four core pieces of guidance relevant to the recalibration of corporate compliance programs: (1) a memorandum titled "Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime" ("**White-Collar Memorandum**"); (2) an update to the "Corporate Enforcement and Voluntary Self-Disclosure Policy" ("**CEP**"); (3) an update to the "Corporate Whistleblower Awards Pilot Program" ("**Whistleblower Program**"); and (4) an updated "Memorandum on Selection of Monitors in Criminal Division Matters" ("**Monitor Memorandum**").

1. **White-Collar Memorandum**

The White-Collar Memorandum outlines the DOJ's renewed enforcement priorities for investigating and prosecuting corporate crime, including the following areas:

- Waste, fraud, and abuse of health care and procurement programs
- Complex frauds that victimize U.S. investors and weaken the integrity of markets (e.g., Ponzi schemes, investment fraud, digital asset / crypto fraud, securities fraud, market manipulation, elder fraud)
- Trade and customs fraud, particularly activities that harm the U.S. economy, competitiveness, and national security
- Bribery, money laundering, and exploitation of the U.S. financial system in a way that enables criminal conduct and undermines national security (e.g., shadow bankers and other intermediaries that process transactions that evade sanctions)
- Financial institutions and networks that provide material support to foreign terrorist organizations
- Fraud committed by U.S.-listed "*foreign adversary companies*" that harms U.S. investors (e.g., Chinese-affiliated variable interest entities)

Furthermore, the White-Collar Memorandum emphasizes the DOJ's focus on prosecuting individuals, as "*[n]ot all corporate misconduct warrants federal criminal prosecution [of an entity]. Prosecution of individuals, as well as civil and administrative remedies directed at corporations, are often appropriate to address low-level corporate misconduct and vindicate U.S. interests*." Rather, the DOJ will work closely with cooperating companies "*that are willing to learn from their mistakes*" and assess consequences on a case-by-case basis. Moreover, investigations are also expected to be more streamlined, limiting the duration and collateral impact of government-directed activity while requiring expeditious cooperation from corporations.

2. **CEP**

In combination with the White-Collar Memorandum, the DOJ unveiled updates to the CEP to incentivize voluntary self-disclosure of misconduct. Rather than giving a "*presumption*" of a declination, as the previous CEP did, the updated CEP states that the DOJ "*will decline to prosecute a company for criminal conduct when the following factors are met*:"

The Company—

- voluntarily self-disclosed the misconduct;
- fully cooperated with the investigation;
- timely and appropriately remediated the misconduct; and
- did not have any aggravating circumstances related to the misconduct or a history of similar misconduct.

Even if aggravating circumstances exist, the updated CEP affords prosecutors the discretion to recommend a CEP declination based on those circumstances and the company's actions.

Furthermore, the updated CEP creates a "*Near Miss*" voluntary self-disclosure framework, whereby the DOJ "*shall*" permit certain benefits to a company that fully cooperated and timely and appropriately remediated yet remains ineligible for a declination (due to either aggravating circumstances or not adequately meeting the voluntary self-disclosure criteria). Those benefits include the following:

- Provide a Non-Prosecution Agreement (NPA);
- Allow an NPA term length of fewer than three years;
- Not require an independent compliance monitor; and
- Provide a reduction of 75% off the low end of the U.S. Sentencing Guidelines fine range

3. **Whistleblower Program**

To complement the above, the DOJ also updated the Whistleblower Program to encourage more voluntary self-disclosure and robust compliance programs by companies. It did so, in part, by doubling the number of eligible subject-matter areas (from four to eight) to include—

- fraud against the United States in connection with federal programs unrelated to health care;
- trade, tariff, and customs fraud;
- violations of federal immigration law; and
- offenses related to sanctions, terrorism, cartels, or transnational criminal organizations.

This expansion fills gaps left by other whistleblower programs and is in addition to the more established types of issues covered under the Whistleblower Program, which include—

- violations by financial institutions such as money laundering and fraud;
- violations related to foreign corruption and bribery;
- violations committed by or through companies related to bribes or kickbacks involving domestic public officials; and
- violations committed by or through companies related to (a) federal health care offenses; and (b) fraud against patients, investors, and other non-governmental entities in the health care industry.

To augment the Whistleblower Program's self-disclosure goals, the updated CEP now states that if a whistleblower reports to both the DOJ and the company, the company "*will still qualify for a declination under the CEP*" (and not just a presumption of a declination)—even if the whistleblower submits to the DOJ before the company self-discloses—**provided that** the company:

- self-reports to the DOJ within 120 days after receiving the whistleblower's internal report; and
- meets the other requirements for voluntary self-disclosure and a declination.

4. **Monitor Memorandum**

The updated Monitor Memorandum clarifies the factors that DOJ prosecutors must consider when determining the appropriateness of monitors, which oversee compliance with criminal resolutions and the enhancement (or development) of a company's compliance program. Such factors include the following:

- the likelihood of repeated criminal conduct with significant consequences for U.S. interests (e.g., sanctions evasion, tariff evasion, health care fraud);
- the effectiveness of oversight by other government authorities;
- the strength of the company’s compliance program and culture at the time of resolution; and

- the maturity of the company's controls and its capacity to independently assess and improve its compliance program.

Already, we have seen multiple years-long monitorships conclude early, and the updated Monitor Memorandum makes no secret the DOJ's belief that monitorships can impose unnecessary burdens and high costs on companies. In fact, the acting head of the DOJ Criminal Division, Matthew Galeotti, recently noted that the DOJ would take a more active role in overseeing compliance, a responsibility previously outsourced to third-party monitors. Thus, companies can revamp and tailor their compliance programs in ways that obviate the need for a monitor, including by demonstrating the long-term suitability of recent enhancements.

## HOW MULTINATIONALS SHOULD RESPOND: PRACTICAL STEPS TO ALIGN WITH DOJ EXPECTATIONS

In response to these significant policy shifts, and the DOJ's recent implementation of them, companies should take concrete, proactive steps to recalibrate their compliance programs and fully align them with the DOJ's evolving expectations. We recommend implementing the following practical measures:

### 1. Conduct a Comprehensive Risk (Re)Assessment

Reassess your company's risk profile, focusing on DOJ priority areas including sanctions, trade and customs, procurement, and health care, and continue the focus on financial crimes, money laundering, and corruption. As always, risk assessments should be ongoing and tailored to your company's business model, geographic reach, and industry sector(s). For example, life sciences and health care companies operating in Greater China, defense contractors operating in Eastern Europe (i.e., near Russia), and non-American, U.S.-listed companies like Chinese variable interest entities should be acutely aware of their operating risks.

### 2. Enhance and Test Compliance Programs

Review and, where necessary, strengthen your compliance policies and procedures to address identified risks. Stress test and perform spot audits on your compliance program based on these risks and properly document any enhancements. Doing so will help demonstrate that your company is "*willing to learn*" from its mistakes should a regulatory enforcement issue arise.

### 3. Monitor and Benchmark Compliance Efforts

Regularly benchmark your compliance program against DOJ guidance and industry best practices. Where appropriate, engage third-party experts to independently assess the effectiveness of your controls and remediation efforts. Be prepared to demonstrate to regulatory authorities that your company's program is both current and effective. For example, your company could point to several recent hires that ensured sufficient staffing for the company's compliance function or to refreshed training modules tailored to high-risk areas of the business.

### 4. Promote a Strong Culture of Compliance

Foster a culture of integrity and ethical conduct at all levels of the organization, reinforcing that compliance is every individual employee's responsibility. Senior management should set the tone from the top by, for example, incorporating compliance metrics in personnel evaluations, participating in trainings alongside line employees, sending out compliance communications, and ensuring that all employees are aware of reporting channels. Given the DOJ's emphasis on individual accountability, companies should warn their employees of this risk and adopt a zero-tolerance policy towards misconduct regardless of position.

### 5. Prepare for Voluntary Self-Disclosure

Establish clear internal protocols for timely escalating and investigating potential misconduct. Ensure that your organization is prepared to evaluate a potential self-disclosure to the DOJ within the required timeframes, particularly in light of the new 120-day window following a whistleblower's internal report (a welcome change from the somewhat ambiguous prior policy). In real time, document all remedial actions and cooperation efforts to maximize eligibility for declinations or other benefits under the CEP.

6. **Strengthen Whistleblower Reporting Mechanisms**

Reinforce internal whistleblower policies (including the company's anti-retaliation policy) to encourage early internal reporting of concerns. To ensure that employees are aware of and trust the mechanisms in place, promptly and thoroughly investigate credible reports. The expanded scope of the Whistleblower Program, combined with the DOJ's stated desire for swift resolutions, should signal to companies that they must act quickly and nimbly in handling misconduct.

7. **Update and Test Incident Response Plans**

Ensure that your organization has a clear, actionable incident response plan for addressing potential violations. Identify and address related legacy issues, such as delays in responding to whistleblower complaints, claims of employee unfamiliarity with policies, and recurring internal problems arising from control gaps.

8. **Document Remediation and Disciplinary Actions**

Maintain thorough documentation of all remedial measures taken in response to identified misconduct, including disciplinary actions against responsible individuals. This documentation will be critical in demonstrating your company's commitment to accountability and remediation. Also maintain a track record of how the compliance program has prevented and detected past misconduct, how the company addressed risks and related reports over time, and what additional or enhanced trainings were developed in response.

9. **Implement Robust Third-Party Management**

Ensure that appropriate due diligence procedures exist for third parties, including agents, distributors, and joint venture partners. Ensure that contractual terms contain appropriate compliance obligations—including certifying compliance with all applicable sanctions and anti-bribery laws—as well as an illegality clause addressing breaches of applicable laws.

10. **Leverage Technology, Data Analytics, and AI Tools**

Utilize technology solutions and data analytics to enhance monitoring, detect anomalies, and identify potential compliance risks in real time. AI tools can help streamline compliance processes and provide valuable insights for continuous improvement. For example, some programs use intelligent intake portals that leverage natural language processing to automatically extract key information (e.g., names, dates, locations) and generate summaries and initial risk assessments. Others can assist with triaging complaints by classifying allegations by severity and issue type based on pre-defined criteria.

## CONCLUSION

The DOJ's recent policy updates once again make clear that multinational companies must take ownership of their compliance obligations, promptly and proactively address risks, and fully cooperate with enforcement authorities. By taking these steps now, companies can not only mitigate enforcement risk but also position themselves to benefit from the incentives and protections offered under the DOJ's new enforcement framework.

# Contacts

**Vasu Muthyala**
Partner
Singapore / Washington D.C.

Email vasu.muthyala@cliffordchance.com
Mobile +65 6661 2051

**Daniel Silver**
Partner
Washington D.C.

Email daniel.silver@cliffordchance.com
Mobile +1 212 878 4919

**Glen Donath**
Partner
Washington D.C.

Email glen.donath@cliffordchance.com
Mobile +1 202 912 5138

**Joshua Berman**
Partner
Washington D.C.

Email joshua.berman@cliffordchance.com
Mobile +1 202 912 5174

# Disclaimer

**Megan Gordon**
Partner
Washington D.C.

Email megan.gordon @cliffordchance.com
Mobile +1 202 912 5021

**Jan van der Kuijp**
Senior Associate
Singapore / Washington D.C.

Email jan.vanderkuijp@cliffordchance.com
Mobile +65 6661 2073