

DOJ Reinforces Emphasis on Voluntary Self-Disclosure with Latest Updates to the Evaluation of Corporate Compliance Programs Guidance

Article By:

Eoin P. Beirne

Nick A. LaPalme

Karen S. Lovitch

On September 23, 2024, the Criminal Division of the United States Department of Justice (“DOJ” or the “Department”) revised its [Evaluation of Corporate Compliance Programs guidance](#) (the “ECCP”).^[1]

DOJ’s “Principles of Federal Prosecution of Business Organizations” describe factors that the Department will consider when investigating a company, determining whether to bring charges, and/or negotiating a plea agreement. Those factors include an assessment of the adequacy and effectiveness of a corporation’s compliance program. The ECCP acts as a tool to assist prosecutors when conducting this analysis. It thus serves as an important aid for companies seeking to strengthen their compliance systems and minimize exposure. A company whose compliance program would be considered robust under the ECCP – even one that does not detect a potential violation – is likely to be viewed more favorably by DOJ in its charging decisions and in a potential resolution.

While every company should review the ECCP in its entirety, this article focuses on significant revisions detailed in the most recent installment of the guidance, which are aimed at 1) bolstering internal reporting mechanisms, 2) adapting to emerging technologies, and 3) ensuring that compliance professionals have sufficient access to the resources and data they need to adequately perform their duties.

Internal Reporting Mechanisms

In the wake of DOJ issuing its Whistleblower Awards Pilot Program^[2] last month, the revised ECCP focuses on the effectiveness of internal reporting mechanisms.

Prosecutors will consider whether a company encourages internal reporting of misconduct or, conversely, whether it employs practices that may chill internal reports. In doing so, prosecutors will inquire as to *how* a company assesses the willingness of its employees to report potential

misconduct. Prosecutors also expect companies to have anti-retaliation policies, practices, and training to ensure that potential whistleblowers are protected. While a compliance program typically has anti-retaliation policies, few companies engage in efforts to evaluate whether employees feel comfortable making compliance-related reports.

Adapting to Emerging Technologies

Consistent with the last iteration of the ECCP, which focused on data preservation in the era of ephemeral messaging applications, the revised ECCP again stresses the need for companies to adapt to new technologies.

Prosecutors will consider what emerging technologies a company is using to conduct business, whether the company has conducted a risk assessment with respect to that technology, and whether the company has proactively sought to mitigate risks associated with the use of that technology. The ECCP's revisions are particularly focused on the risks posed by artificial intelligence ("AI").

Companies that utilize AI and other emerging technologies are expected to develop internal controls that ensure the technology is being deployed in a manner that adheres to the law and the company's code of conduct. This requirement may have a significant impact on the health care sector. As an example, insurers who use AI to assist with the prior authorization process should ensure that their implementation efforts have sought to mitigate unintended consequences that could stem from use of this technology (e.g., false approvals). A successful compliance program also should include mechanisms that allow for its continuous modernization over time.

Data Access and Resources for Compliance Professionals

DOJ expects a company's compliance function to be adequately resourced. The revised ECCP directs prosecutors to evaluate how the resources, assets, and technology available to a company's compliance and risk management function compares to those available to other aspects of the business. As a result, the Department will consider whether there is an imbalance in the resources dedicated to obtaining market opportunities versus those dedicated to detecting and mitigating risks.

Compliance professionals should also have the means to access data sources they need to perform their duties effectively. Finally, companies should consider whether they are adequately leveraging data analytics and other tools in a manner that bolsters their compliance systems. Given that federal agencies are increasingly using data analysis to identify potential non-compliance (particularly in the health care sector), companies should be actively using data analysis in their compliance auditing and monitoring activities.

Connection to DOJ's Efforts to Incentivize Voluntary Self-Disclosure of Corporate Misconduct

On the day that the revised ECCP was issued, Principal Deputy Assistant Attorney General Nicole M. Argentieri delivered an accompanying [speech](#) to the Society of Corporate Compliance and Ethics. As expected, her remarks focused heavily on the Department's efforts to incentivize companies to voluntarily self-disclose their misconduct.

She explained that under the new Whistleblower Awards Pilot Program, DOJ has already "received tips from over 100 individuals to date, with more coming in every day." When deciding whether to voluntarily self-disclose, Ms. Argentieri acknowledged that companies will assess not only the benefits of self-reporting, but also the risk that DOJ will learn about the misconduct from other

sources, such as whistleblowers. DOJ's intention in creating the Whistleblower Awards Pilot Program was to "alter that calculus" by maximizing the chances that it becomes aware of corporate misconduct. Under this new policy regime, with misconduct less likely to remain undetected, DOJ has increased the pressure on companies to voluntarily self-disclose what they learn as soon as possible after they learn it.

Accordingly, the same day that the Criminal Division issued the Whistleblower Awards Pilot Program, it also amended its Corporate Enforcement and Voluntary Self-Disclosure Policy (the "CEP").^[3] The amendment to the CEP clarifies that a company that voluntarily self-reports misconduct to DOJ within **120 days** of receiving an internal whistleblower report may be eligible for a presumption of a declination—if the company voluntarily self-discloses **before** DOJ contacts the company.

Ms. Argentieri ended her speech with a clear call to action: "I hope today you'll take this message back to your companies: now is the time to make the necessary compliance investments to help prevent, detect, and remediate misconduct. And when you uncover misconduct: **call us before we call you.**"

Key Takeaways

- Companies should evaluate their hotlines and other internal reporting mechanisms to ensure that they are effective in application.
- Whistleblower complaints should be taken seriously, and when a company becomes aware of potential misconduct, it must assess as quickly as possible whether a voluntary self-disclosure is appropriate.
- Compliance programs must be adequately funded, resourced, and able to adapt to newly emerging technologies.

[1] This constitutes the first update to the ECCP since March of 2023. Our analysis of the previous 2023 update can be found [here](#).

[2] Our analysis of the Whistleblower Awards Pilot Program can be found [here](#).

[3] Our analysis of the previous iteration of the CEP can be found [here](#).

©1994-2025 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.

National Law Review, Volume XIV, Number 281

Source URL: <https://natlawreview.com/article/doj-reinforces-emphasis-voluntary-self-disclosure-latest-updates-evaluation>