Published on *The National Law Review* https://natlawreview.com

DOJ Stresses AI Risk and Whistleblower Protection in Revised Corporate Compliance Guidance

Article By:

Matthew D. Krueger

Olivia S. Singelmann

On Monday, September 23, DOJ's Criminal Division announced updates to its guidance for evaluating corporate compliance programs ("ECCP"). Principal Deputy Assistant Attorney General Nicole Argentieri also delivered remarks regarding the changes during a speech at the Society of Corporate Compliance and Ethics. The revisions to the ECCP emphasize that an effective compliance program must:

- Conduct appropriate risk assessments and implement compliance programs after a merger or acquisition;
- Consider risks associated with emerging technologies like artificial intelligence (AI), both in commercial operations and the compliance program itself;
- Include robust whistleblower protections; and
- Be accessible and adequately resourced with both financial and data resources.

We have provided a redline here that compares the prior version of the ECCP (updated March 2023) with the new version, to reflect all changes. Below, we give background on the ECCP, summarize the changes, and explain their implications.

The ECCP Guides DOJ's Charging and Resolution Decisions and Incentivizes Robust Compliance Programs

DOJ has increasingly used the ECCP as a key tool to incentivize changes in corporate compliance programs. The ECCP instructs prosecutors how they should assess corporate compliance programs in making decisions about whether to bring charges against a company and how to resolve cases, including the potential of reduced penalties and even declination of prosecution. Consequently, the ECCP helps companies understand the DOJ's expectations for what DOJ will consider an "effective" compliance program.

DOJ's updated ECCP should be considered against the backdrop of DOJ seeking to increase enforcement against "white-collar crime." DOJ continually has reminded companies that it will use "all the tools in its toolbox" to prosecute corporate crime, both through expanded incentives and

higher expectations of companies. In March 2024, we discussed the potential impact on companies following Deputy Attorney General Lisa Monaco's remarks regarding the DOJ's integration of disruptive technologies, such as AI and ephemeral messaging, into its evaluation of corporate compliance efforts. This emphasis also is reflected in DOJ's 2023 modifications to its Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy, which addressed companies' responsibility to preserve materials on collaboration tools and ephemeral messaging platforms. And last month, we discussed the implications of DOJ's whistleblower reward pilot program on companies' internal investigations and self-disclosure considerations. The DOJ has simultaneously launched an individual self-disclosure pilot program.

Changes to the ECCP Emphasize Forward-Thinking and Proactive Compliance

This week's updates to the ECCP demonstrate the DOJ's desire to encourage progressive, dynamic compliance programs that deter unethical conduct. Argentieri's speech emphasized that well-resourced compliance departments mean companies are "better situated to prevent, detect, and stay ahead of misconduct when it occurs."[1] We highlight key changes to the ECCP here.

1. *Risk Assessments and Integration of Compliance After Mergers and Acquisitions*

The revised ECCP stresses the importance of effectively integrating a compliance program when companies go through mergers, acquisitions, or other transactions. Although the prior ECCP discussed this issue briefly, DOJ's latest revisions call for greater scrutiny of post-deal compliance efforts. Companies should consider conducting risk assessments on newly acquired divisions and should adapt policies and procedures to account for new risks.

2. *The Impact of New Technologies in Commercial and Compliance Operations*

A key change to the revised ECCP is direction to consider whether companies are addressing risks associated with new technologies, including AI. This consideration is twofold: Companies must adequately address risks presented by the use of new technologies both in their commercial operations and in the compliance program itself. For example, companies should implement controls to prevent insiders' misuse of commercial technologies as well as controls ensuring the reliability and trustworthiness of technology used in monitoring compliance. Companies should conduct risk assessments regarding the use of new technologies in their everyday operations and in monitoring compliance. Adequate training in the use of artificial intelligence and other new technologies is the bare minimum for an effective compliance program.

Relatedly, companies should have processes in place to update technology policies and procedures as new technologies emerge and transform. Thus, compliance programs should be integrated into the business in such a way that the programs can seamlessly adapt to new technologies or commercial transactions. Such integration will require frequent risk assessments and monitoring to ensure that what sounds good on paper works in practice.

3. *Whistleblower Policies*

The revised ECCP bolsters guidance regarding whistleblower protection and anti-retaliation policies and practices. Companies, at a minimum, should have an anti-retaliation policy and train employees regarding internal and external reporting mechanisms and whistleblower protection laws. Whistleblowers must be protected, and companies' responses to reports of misconduct should demonstrate "that there is no tolerance for retaliation."[2]

Companies must also timely investigate and respond to whistleblower's reports, and reporting channels should be structured such that all potential compliance complaints reach the compliance department for appropriate investigation. Relatedly, companies should consider the DOJ's whistleblower awards pilot program and the incentives it presents for employees and companies to self-report wrongdoing.

4. *Compliance Resources*

Finally, the revised ECCP placed more emphasis on resource allocation to compliance programs. Prosecutors are directed to consider the budgets allocated to compliance programs, and companies should consider assigning a commercial value to their compliance investments. Resources allocated to capturing business should not be disproportionately larger than those allocated to compliance. Compliance programs should be adequately funded and staffed, and compliance staff should have access to data and tools needed to meaningfully evaluate the company's compliance. Data analytics tools also should be leveraged to evaluate the effectiveness of the company's compliance program.

At bottom, the DOJ's updates to the ECCP emphasize what has been the DOJ's message for many years now: When it comes to compliance, companies should put their money where their mouths are. Lip service alone will not be viewed as having an "effective" corporate compliance program.

---

[1] Nicole Argentieri, Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute (Sept. 23, 2024).

[2] *Id*.

National Law Review, Volume XIV, Number 270