ALERT MEMORANDUM

DOJ Announces Revisions to Compliance Guidance Focused on AI, Whistleblower Reporting, and Other Areas

September 26, 2024

On September 23, 2024, Principal Deputy Assistant Attorney General Nicole M. Argentieri announced revisions to the Department of Justice ("DOJ"), Criminal Division's compliance guidance, known as the Evaluation of Corporate Compliance Programs ("ECCP"), which is used by DOJ prosecutors to assess the effectiveness of a company's compliance program in the context of a corporate investigation.[1] The updated compliance guidance incorporates changes that will focus on a company's use of Artificial Intelligence ("AI")[2] and other technologies, its use of data analytics as part of the compliance function, the incorporation of "lessons

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

WASHINGTON

David A. Last
+1 202 974 1650
dlast@cgsh.com

NEW YORK

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Elizabeth (Lisa) Vicens
+1 212 225 2524
evicens@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Andres Saenz
+1 212 225 2804
asaenz@cgsh.com

PALO ALTO

Jennifer Kennedy Park
+1 650 815 4130
jkpark@cgsh.com

Matthew M. Yelovich
+1 650 815 4152
myelovich@cgsh.com

[1] Speech, "Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute," (Sept. 23, 2024), *available at* https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks-society. The revised ECCP is available here.

[2] The updated ECCP adopts the definition of artificial intelligence set forth in the Office of Management and Budget's Memo M-24-10 dated March 28, 2024, titled "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," *available at* https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

learned" to continuously enhance corporate compliance programs, and whistleblower reporting.[3]

PDAAG Argentieri also provided updates on the DOJ's most recent pilot programs: the Compensation Incentives and Clawbacks Pilot Program and the Corporate Whistleblower Awards Pilot Program, as well as how these programs and a wider set of changes to the DOJ's Corporate Enforcement Policy ("CEP") have been implemented in recent resolutions.

I. Assessing and Managing Risks from AI Tools and Emerging Technologies

Following a directive from Deputy Attorney General Lisa Monaco to the DOJ Criminal Division to assess disruptive technology risks and misuse of AI in particular, the newest ECCP guidance reflects efforts to analyze how companies are using new technologies, including AI, in their business, and whether that use is accompanied by an appropriate assessment of the potential risks and vulnerabilities that those technologies may present, as well as an alignment with the company's code of ethics. The amended ECCP guidance emphasizes the extension of risk assessments to the incorporation of new and emerging technologies.

Going forward, DOJ will expect companies to proactively consider how AI tools and other new technologies may affect a company's ability to comply with criminal laws, and will assess how new technologies are incorporated into the company's wider enterprise risk management system. For example, as noted by PDAAG Argentieri, DOJ will consider whether a company is particularly "vulnerable to criminal schemes enabled by new technology, such as false approvals and documentation generated by AI."[4] Among other issues identified in the updated guidance, DOJ will be looking for companies to address:

- Specific steps taken to mitigate potential risks associated with the use of technology, including the potential for deliberate or reckless misuse of technologies, including by company insiders;
- Whether the company has adopted measures to evaluate and curb potential negative or unintended consequences arising out of its use of technologies, both on the business side of its operations, as well as in its compliance program;
- Any controls monitoring or testing to best ensure that AI and other technologies are being used for intended purposes and functioning properly, including whether the company has a framework for monitoring the use of such technologies in adherence with applicable law and its code of conduct;
- The baseline of human decision-making being used by the company to assess AI and how accountability over the use of AI is supervised and enforced; and
- Employee training on the use of AI and other emerging technologies.[5]

II. Use of Data and Analytics Tools to Assess and Enhance Effectiveness

Aside from being able to prevent, detect, and remediate misconduct, the revised ECCP emphasizes the importance of having a process in place for the company to periodically evaluate the compliance program it has designed and implemented. That process should also focus on continuous improvement through the collection and analysis of data that is leveraged to strengthen the program.

The new revisions to the ECCP stress a mantra of "be ready to show your work." Many of the new revisions are framed in terms of how a company collects and utilizes its data to improve performance:

[3] DOJ last revised its compliance guidance in March 2023, focusing in particular on issues related to third-party messaging and ephemeral communications, and compensation structures and clawbacks. Details related to the previous revisions from March 2023 can be found on our blogpost here.

[4] *supra* n.1.

[5] *See* ECCP (Sept. 2024) at 3-4.

— "How is the company leveraging available data to evaluate vendor risk during the course of the relationship with the vendor?"[6]

— "To what extent does the company have access to data and information to identify potential misconduct or deficiencies in its compliance program?"[7]

— "Can the company demonstrate that it is proactively identifying either misconduct or issues with its compliance program at the earliest stage possible?"[8]

The updated ECCP guidance notes that DOJ will not only look at whether compliance personnel have access to all relevant data sources, but also the extent to which the company is "leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of components of compliance programs."[9] In this regard, DOJ will be evaluating whether compliance programs have the tools to improve their efficiency and effectiveness through measurable metrics, including the commercial value of investments in compliance and risk management, the quality of data sources, and the accuracy and precision of the data analytics models themselves. DOJ also will look at whether resources have been proportionately allocated across different functions within the company, particularly with an eye towards understanding how assets, resources, and technology available to the compliance and risk management functions compare to those available elsewhere in the company.[10] In particular, DOJ will assess whether there is an imbalance between the technology and resources used by the company to identify and capture market opportunities, as compared to those used to detect and mitigate risk. This question will be especially important for technology companies and others leveraging cutting edge tools in other aspects of their business. The ECCP signals that businesses should ensure that such levels of sophistication are included not only on the business side of the house, but also in their compliance teams' toolkit. By the same token, discrepancies between the advanced technologies used for business lines and less advanced technologies for compliance may be perceived more negatively by DOJ in the context of evaluating the company's compliance program.

III. Incorporating "Lessons Learned" Into Program Enhancements and Training

In her announcement of the ECCP revisions, PDAAG Argentieri noted, "[C]ompanies should be learning lessons from both the company's own prior misconduct and from issues at other companies to update their compliance programs and train employees."[11] This suggests that DOJ will ask whether companies have adopted continuous monitoring and incorporated "lessons learned" to not only design a more effective compliance program at the outset, but also whether the company periodically re-evaluates its program over time. In other words, has the company taken "lessons learned" internally (as well as from other companies) to improve and enhance the effectiveness of its program?

Clear opportunities to incorporate "lessons learned" are through trainings that are regularly updated and focused on evolving risks not only for the company, but also in the industry in which the company operates.[12] This means that misconduct by others can serve as an instructive case study for a company operating in a similar industry or geography.[13] As with other aspects of the compliance program, DOJ will ask what companies have done to ensure that employees meaningfully engage in training sessions and absorb the information and issues being covered.

Under the revised ECCP guidance, DOJ also will consider whether a compliance program has a track record of preventing or detecting misconduct, as well as whether the company has treated potential misconduct as an isolated incident, as opposed to a

[6] *Id.* at 9.
[7] *Id.* at 19.
[8] *Id.*
[9] *Id.* at 13.
[10] *Id.*
[11] *supra* n. 1. *See also* ECCP (Sept. 2024) at 18.
[12] *See* ECCP (Sept 2024) at 6.
[13] *Id.* at 3.

data point in a more holistic map. Compliance practitioners should be ready to answer questions concerning prior responses to instances of misconduct and how the company has addressed reports of potential misconduct and risks over time.[14]

IV. Strengthening Whistleblower Reporting

The ECCP was further revised to incorporate changes related to whistleblower reporting, including the company's reporting channel and protections against retaliation. These revisions come on the heels of DOJ's recently announced Whistleblower Awards Pilot Program, announced in early August 2024, and aimed at incentivizing potential whistleblowers to come forward with actionable information in exchange for monetary awards, similar to what has been done by other federal agencies, such as the SEC and CFTC.[15] Collectively, the revisions address the goals of the DOJ whistleblower program to: (1) encourage employees to speak up and report misconduct; (2) reinforce the importance of anti-retaliation; (3) make sure that employees trust and are willing to use the whistleblower program; and (4) use the information drawn from the company whistleblower channel as data points to improve the compliance program overall.[16]

Aside from *what* companies do to promote whistleblower programs and policies, DOJ will be evaluating *how* companies assess employee willingness to report misconduct. This could potentially be accomplished by company surveys or tracking the success of the program over time across various reporting metrics and in different jurisdictions where the company operates. The ability to do so effectively will likely require collecting data and demonstrating to DOJ the company's methodology for analyzing such data, including categories of key metrics and analysis of reporting trends over time.

Unsurprisingly, in the context of an investigation, DOJ will evaluate how well the company advertises its whistleblower program, including through trainings, as well as the incentives and other means of recognizing how individuals use it. One new update to the ECCP guidance asks, "Does the company train employees on internal reporting systems *as well as external whistleblower programs and regulatory regimes*?"[17] (emphasis added). This suggests that the Criminal Division may consider corporate efforts to promote and train employees on the availability of the DOJ whistleblower program, and potentially that of other regulators. Under the DOJ Pilot Program and other policies, such as the CEP and ECCP, companies that have measures in place to incentivize whistleblowers in the first instance, protect them once a report is made, and self-report in appropriate circumstances, may obtain benefits through cooperation credit, penalty reductions, and potentially a declination.

V. M&A Revisions

The revised ECCP also expanded on prior guidance related to M&A transactions.[18] Importantly, companies involved in M&A transactions should focus on their processes for combining and integrating their critical enterprise resource planning systems and their risk mitigation functions. Planning ahead for compliance oversight, consolidated risk assessments, organization of policies and procedures, and post-close audits will be crucial to the successful integration of merged and acquired entities. In line with the recent "M&A Safe Harbor Policy" announced by DOJ at the end of last year, companies may benefit from a "safe harbor" where they detect, voluntarily self-report, and implement measures to remediate and prevent future misconduct identified through the M&A process within the time periods outlined in the policy.[19]

VI. DOJ Updates From Recently Announced Pilot Programs

PDAAG Argentieri also provided updates on two Criminal Division Pilot Programs: (1) the Compensation Incentives and Clawbacks Pilot

[14] *Id.* at 18.
[15] Our overview of the DOJ's Whistleblower Awards Pilot Program can be found here.
[16] *See* ECCP (Sept. 2024) at 7.
[17] *Id.*
[18] *Id.* at 9.
[19] Our summary of voluntary self-disclosure guidance in the M&A context can be found here.

Program; and (2) the Corporate Whistleblower Awards Pilot Program.

Compensation Incentives and Clawbacks Pilot Program.[20] Each new corporate resolution since the announcement of the Pilot Program has required that the resolving company include criteria related to compliance in its compensation and bonus system. As explained by PDAAG Argentieri, DOJ is "asking companies to provide clear metrics both to reward compliance-promoting behavior and to deter misconduct."[21] Companies resolving with the DOJ have also received fine reductions under the Pilot Program where they have demonstrated efforts to withhold bonus compensation from culpable employees and others who had supervisory authority over those engaged in misconduct and knew of, or were willfully blind to, the misconduct.[22]

Corporate Whistleblower Awards Pilot Program.[23] PDAAG Argentieri also noted that, although the whistleblower program has been operational for less than two months, DOJ has "received tips from over 100 individuals to date, with more coming in every day."[24] Given this volume of reports and the Pilot Program's "120-day" timeline for companies to self-report misconduct identified through their own whistleblower channels, PDAAG Argentieri's advice demonstrates DOJ's approach very clearly: "[N]ow 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."[25]

VII. Key Takeaways

DOJ's revisions to the ECCP underscore important themes and signals from the Criminal Division to companies and their compliance departments in recent years. As PDAAG Argentieri explained, DOJ will "take notice of companies that make the right choices and invest in and support effective compliance programs. When compliance officers have the necessary resources to do their jobs — and a seat at the table in the boardroom to have their voices heard — companies are better situated to prevent, detect, and stay ahead of misconduct when it occurs." She explained further that companies that take those actions, in addition to cooperating and remediating misconduct, "put themselves in the best position to achieve the most favorable outcomes" when dealing with DOJ.[26] Some key takeaways from the recent revisions of the ECCP guidelines:

— First, companies should be leveraging new technologies in a way that enhances, rather than disrupts, corporate compliance. Risk management includes assessing the risks of using new technologies, including testing and monitoring the performance of AI and other emerging technologies to ensure that there are guardrails on their use.

— Second, in line with DOJ's recent announcements regarding the Whistleblower Awards Pilot Program, companies are encouraged to spread the message of their program (and the whistleblower channel in particular) through policies and training, and to reinforce anti-retaliation protections to their employees. While DOJ has incentivized individuals to directly report misconduct in key areas, including financial fraud, foreign and domestic corruption, and private healthcare fraud, it has also incentivized those same individuals to first make their reports through corporate whistleblower channels. Given the timeframe outlined by DOJ in the

[20] "The Criminal Division's Pilot Program Regarding Compensation Incentives and Clawbacks" (Mar. 3, 2023), *available at* https://www.justice.gov/criminal/criminal-fraud/file/1571941/dl. Our summary of the Compensation Incentives and Clawbacks Program can be found on our blogpost here.
[21] *supra* n.1.
[22] *Id.*
[23] Criminal Division Corporate Whistleblower Awards Pilot Program, *available at* https://www.justice.gov/criminal/criminal-division-corporate-whistleblower-awards-pilot-program. Our summary of the DOJ Whistleblower Pilot Program can be found on our blogpost here.
[24] *supra* n. 1.
[25] *Id.*
[26] *Id.*

whistleblower program and CEP (*i.e.*, 120 days after receiving the internal whistleblower report), companies must act quickly and efficiently to assess, scope, and investigate the conduct at issue and determine appropriate next steps. Companies need to ensure their whistleblower channels are optimized to receive reports and respond appropriately.

— Third, continuing a running theme from the DOJ over the past couple years, companies should invest in their compliance programs, particularly with respect to using and leveraging data and, where possible, data analytics tools. Companies that make appropriate investments in compliance today will be in a much better position if DOJ ever comes knocking on their door in the future. Using data to improve the effectiveness of a compliance program and to monitor trends, spot weaknesses, and enhance overall functioning will only make the company stronger and better positioned. Under the new guidance, companies should evaluate the technologies being used elsewhere in the organization to capture competitive advantages and determine whether those same technologies can be applied to improve the compliance program.

— Finally, these same data sources and analytics tools can be used to implement "lessons learned" and measure how well a compliance program is reaching employees. The guidance is focused squarely on how a company's compliance program is able to continuously improve, apace with changes that are already taking place across business divisions. Companies that invest in compliance using a similar data-driven approach will be best equipped to prevent, detect, and remediate potential gaps, and benefit from the DOJ's various programs in the event of a DOJ or other regulatory investigation.

…

CLEARY GOTTLIEB