View on our website.

GIBSON DUNN

White Collar Defense & Investigations Update September 30, 2024

DOJ Updates Its Evaluation of Corporate Compliance Programs Guidance Focused on AI and Emerging Technologies

Although this latest round of updates is not as extensive as the 2023 iteration, it includes significant additions that may have meaningful implications for companies as they seek to align their compliance programs with DOJ's expectations.

On September 23, 2024, the Criminal Division of the U.S. Department of Justice ("DOJ") announced the latest revision of its Evaluation of Corporate Compliance Programs (the "ECCP") since its last update in March 2023. The ECCP serves as the Criminal Division's guidance for its prosecutors to evaluate companies' compliance programs when making corporate enforcement decisions. This guidance is also often consulted by companies seeking to ensure their compliance programs are effective and would hold up under DOJ's scrutiny. Principal Deputy Assistant Attorney General ("DAAG") Nicole M. Argentieri announced the revision of the ECCP during her remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute held in Grapevine, Texas on September 23, 2024.

The most significant revisions of the ECCP center on three areas: (1) evaluation and management of risk related to new technologies, such as artificial intelligence ("AI"); (2) further emphasis on the role of data analysis; and (3) whistleblower protection and anti-retaliation. The key updates in these three areas are discussed below, and a comparison between the 2023 and 2024 ECCP versions can be found here.

(1) AI and Emerging Technologies

Perhaps the most significant update in this new iteration of the ECCP is the heightened focus on how organizations proactively identify, assess, mitigate, and manage the risks associated with their use of emerging technologies, including AI. This emphasis reflects DOJ's increasing focus on companies' use of data and technology and its stated expectation that companies' approach to risk management will be proactive rather than reactive.

AI and more advanced data analytics tools hold great promise for companies' management of risk. Nevertheless, these capabilities also create risk. Although DOJ appears to recognize the promise, the revisions to the ECCP track DOJ's concerns about how AI and other technologies can be misused. For example, in February 2024, Deputy Attorney General ("DAG") Lisa Monaco announced that DOJ would seek sentencing enhancements where offenses were made significantly more dangerous by the misuse of AI. The following month, DAG Monaco drew a parallel to corporate criminal prosecutions, stating that "[w]hen our prosecutors assess a company's compliance program . . . they consider how well the program mitigates the company's most significant risks," emphasizing that for a growing number of businesses, this "now includes the risk of misusing AI." In the same remarks, DAG Monaco announced that she had directed the Criminal Division to "incorporate assessment of disruptive technology risks—including risks associated with AI—into its guidance on Evaluation of Corporate Compliance Programs."

The position taken by DOJ in the latest ECCP is summarized by DAAG Argentieri in her recent remarks: "prosecutors will consider whether the company is vulnerable to criminal schemes enabled by new technology, such as false approvals and documentation generated by AI. If so, we will consider whether compliance controls and tools are in place to identify and mitigate those risks, such as tools to confirm the accuracy or reliability of data used by the business. We also want to know whether the company is monitoring and testing its technology to evaluate if it is functioning as intended and consistent with the company's code of conduct."

The updated ECCP outlines how companies will be expected to tailor their compliance programs to identify and manage the risks of AI. Corporations deploying AI will need to consider whether:

- their risk assessment processes consider and appropriately document their use of AI and other new technologies and how the risk level for intended use cases has been determined (e.g., in circumstances where the particular use of AI creates particular risks, such as confidentiality, privacy, cybersecurity, quality control, bias, etc.);
- the AI systems they are deploying have a sufficient degree of human oversight, especially for high-risk uses, and whether the performance of those systems is being assessed by reference to an appropriate "baseline of human decision-making" (e.g., the expected standard to which human decision-makers would be held for a given use case);
- appropriate steps have been taken to prioritize and minimize the identified risks—including the potential for misuse of those technologies by company insiders—by implementing compliance tools and controls (e.g., through monitoring, alerts, technical guardrails, continuous testing, human review, or confirming the accuracy or reliability of data); and
- they are continuously monitoring and testing their technology to evaluate if it is functioning "as intended," both in their commercial business and compliance program,

and consistent with the laws and the company's code of conduct. If there are significant deviations in performance, for example where an AI tool makes an inappropriate decision, prosecutors will look at how quickly a company is able to detect and subsequently correct errors and any subsequent decisions.

(2) Emphasis on Data

Another key area of revisions to the ECCP confirms DOJ's increasing focus on the use of data for compliance purposes, expanding on DOJ's existing guidance:

- The most extensive revisions in this area stress the importance of ensuring that compliance personnel maintain access to company data to assess the effectiveness of the compliance program—including leveraging data analytics tools to create efficiencies in compliance operations and measure the effectiveness of compliance components. This is an area on which DOJ's Matt Galvin, Counsel for Compliance & Data Analytics at the Criminal Division's Fraud Section, has focused, including with regard to DOJ's own use of data analytics and the government's expectation that companies will incorporate data-driven approaches to compliance as well. During a PLI program in June 2023, Galvin referred to data as "a function of transparency" in an organization. The revisions to the ECCP make clear that compliance personnel should have access equal to that of the business teams to all relevant data, assets, resources, and technology. This expectation on DOJ's part was previewed by Galvin during the recent 15th Annual Global Ethics Summit in April 2024, where he emphasized that a delta between the use of data analytics by business and compliance teams will draw DOJ's attention. The ECCP now includes additional questions testing whether the company is appropriately using data analytics tools to measure the effectiveness of compliance programs, the quality of its data sources, and the accuracy of any data analytics models it employs.
- Other revisions in the ECCP concern data in the context of third-party management with a particular focus on vendor risk. Prosecutors will gauge whether the third-party risk management process allows for the review of vendors in a timely manner, and whether the company leverages available data to evaluate vendor risk in the course of its relationship with the vendor. This is consistent with DOJ's increasing scrutiny of companies' approach to third-party management practices and their ability to assess risks associated with broader categories of third parties emerging as potential new sources of compliance risk.
- With regard to M&A transactions, among several revisions, DOJ now guides prosecutors to consider whether companies "account for migrating or combining critical enterprise resource planning systems as part of the integration process." This again demonstrates an emphasis on control over and access to corporate information.
- In examining whether the compliance program works in practice, the revised guidance spells out more specifically that prosecutors should "consider whether the company's compliance program had a track record of preventing or detecting other instances of misconduct, and whether the company exercised due diligence to prevent and detect criminal conduct." Prosecutors are now instructed to look at how a company uses data to "gain insights into the effectiveness of its compliance program" and the breadth of non-compliant conduct, beyond criminal conduct, that it is able to prevent.

(3) Whistleblower Reporting

In early August this year, the Criminal Division released guidance regarding the new DOJ Corporate Whistleblower Awards Pilot Program. This month's revisions to the ECCP align it with the pilot program's goals by including a paragraph on companies' "Commitment to Whistleblower Protection and Anti-Retaliation" under the "Confidential Reporting Structure and Investigation Process" section.

In that paragraph, the new guidance advises prosecutors to consider several factors, including whether the company has an anti-retaliation policy; whether it trains employees on both internal and external anti-retaliation and whistleblower protection laws; and how employees who reported misconduct are disciplined in comparison to others involved in the misconduct (meaning whether reporting misconduct is a mitigator impacting a company's disciplinary response). It also asks whether the company trains employees on both internal reporting systems and "external whistleblower programs and regulatory regimes."

The ECCP also now directs prosecutors to consider whether and how an organization "incentivize[s] reporting" and whether an organization trains its employees on "external whistleblower programs and regulatory regimes." Both of these concepts may prove tricky for organizations to address.

Other Notable Additions

In addition to the three main areas discussed above, the revised guidance contains a few other noteworthy revisions in other areas:

- The revised guidance makes the paragraph dealing with "Risk-Tailored Resource Allocation" in the "Risk Assessment" section more general, removing examples of "low risk" and "high risk areas," and instead opting for a broader consideration of whether the company "deploy[s] its compliance resources in a risk-based manner with greater scrutiny applied to greater areas of risk."
- The revisions specify that compliance training should be tailored specifically to the "particular needs, interests, and values of relevant employees," including being tailored to the relevant industry and geographical region.
- Under "Autonomy and Resources," and particularly in relation to funding and resources, the revised guidance now asks whether the company has "a mechanism to measure the commercial value of investments in compliance and risk management." In our experience, this is not a common activity of corporate compliance functions, although some certainly do undertake such efforts.

Six Key Takeaways

The updated ECCP is likely to impact significantly how companies tailor their compliance programs to address risks arising out of AI and emerging technologies, reflecting the rapid and dynamic adoption of these technologies across business sectors. To put these requirements into practice, companies will need to build effective governance frameworks and internal policies dealing with emerging technologies and specifically addressing the new challenges and risks they pose.

Here are six other key takeaways from our reading of the updates:

1. **Scope**. Companies will need to assess and consider carefully whether technical solutions they deploy may fall under the expanded ambit of the guidance. The ECCP defines AI broadly in accordance with the Office of Management and Budget's March 2024 memo, which expressly states that "no system should be considered too simple to qualify as covered AI due to a lack of technical complexity," and where the definition includes "systems that are fully autonomous, partially autonomous, and not autonomous, and it includes systems that operate both with and without human oversight." Companies will need to assess and consider carefully whether technical solutions they deploy may fall within this definition.

2. **Risk-based compliance**. The guidance continues to emphasize that compliance resources should be deployed based on the degree of risk, with greater scrutiny applied to greater areas of risk. The threshold for effective compliance will therefore rely on the design and execution of proactive and effective risk assessments that focus on the actual use cases in which new technologies are being deployed. For example, the risks associated with certain AI tools may vary substantially depending on the use cases for which they are deployed. The guidance also refers to the "baseline of human decision-making" that is used to assess the risk of an AI tool. This concern is reflected in prior comments by DAG Monaco that "[d]iscrimination using AI is still discrimination." That will require companies to think carefully about the purpose for which they are deploying new technologies such as AI, and whether such technology is effectively meeting that purpose (without running afoul of legal requirements). Strategies employed by companies in this area should be designed for accountability, transparency, and continuous evolution.

3. **Accountability and transparency**. Companies are expected to ensure that their new technologies function transparently, and that decisions influenced by these technologies are subject to human review where necessary. The guidance emphasizes that the "black box" nature of some AI systems, and the fact that they might require more third-party management, is not an excuse for failing to meet legal standards. Any compliance program that deploys AI will therefore need to include effective and consistent diligence and procurement standards for third-party models or tools used, staff internal experts with technical competence, ensure that the compliance function is using the data at the company's disposal to detect risks, and maintain sufficient visibility of how new technologies are functioning in practice and how they are impacting the business.

4. **Continuous monitoring and access to data**. The dynamic nature of new technologies, and in particular AI, reinforces the need for regular and possibly more frequent risk assessments and re-evaluation of compliance program effectiveness and monitoring (including testing, which may encompass automated risk detection and real-time monitoring, for high-risk use cases). Moreover, in addition to detecting decisions made by AI that do not meet compliance standards, companies must also be prepared to correct those decisions quickly. Organizations will need to be nimble in adapting compliance systems to fast-evolving legal and technical standards related to AI, as well as rapid technological development. There is already an abundance of practical guidance, including by federal agencies, on best practices in AI governance and compliance, but it has largely been intended for voluntary use (for example, the AI Risk Management Framework released by the National Institute of Standards and Technology (NIST), which the ECCP expressly cites as a resource). The new DOJ guidance indicates that there will be increased regulatory scrutiny on how companies deploying new technologies are choosing to interpret and implement these best practices. Beyond the realm of emerging technologies though, simply articulating an expectation that compliance functions access and monitor corporate data as, for example, a finance or audit function may, could signal

a shift in compliance staffing, with compliance officers more often needing to have accounting or technological backgrounds.

5. **Resource allocation**. The guidance puts companies on notice that in making charging decisions DOJ may now examine whether companies are devoting adequate resources and technology to AI risk management and compliance and to gathering and leveraging company data for compliance purposes. This suggests that any company investing in new technology development or deployment will need to consider whether appropriately proportional resources are being allocated to compliance, including as compared with overall expenditure on such new technologies.

6. **Approach to compliance reporting**. The revisions and additions in relation to whistleblower reporting and anti-retaliation may result in a gradual increase in whistleblower reports by encouraging enhancements to reporting systems that enable employees to feel more secure in reporting misconduct. In addition to ensuring that their anti-retaliation policies are robust and effectively communicated to employees, companies will likely feel the need to allocate additional resources to handle a potential rise in whistleblower reporting in the long term. They will also need to grapple with what they could do to "incentivize" whistleblowing, and whether and how to train employees to report to third parties, in addition to internal corporate channels. While companies typically train employees on the *internal* procedures for reporting and anti-retaliation protections, it remains to be seen how companies put into practice DOJ's guidance to train employees on "external whistleblower programs and regulatory regimes" and how DOJ will react to those practices in the context of enforcement.

Conclusion

While the regulatory landscape for AI and other emerging technologies remains unsettled, it is all but certain from the latest revisions of the ECCP that DOJ has its eyes firmly set on the way these new technologies will shape and increase companies' risk exposure. Along with the other changes in the ECCP outlined here, companies will have to consider carefully and proactively the compliance implications new technologies will bring to their business.

DOJ's updated guidance underscores the need for companies to evaluate their programs, update their policies and procedures where needed, and stay abreast of how technology can be used to boost—as well as skirt—compliance controls. Our team has deep experience with these issues and is well positioned to assist companies with tackling them as DOJ is set to intensify its focus on this area.

The following Gibson Dunn lawyers prepared this update: F. Joseph Warin, Patrick Stokes, Stephanie Brooker, Michael Diamant, Eric Vandevelde, Oleh Vretsona, Frances Waldmann, Victor Tong, José Madrid, and Kate Goldberg.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these issues. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of Gibson Dunn's White Collar Defense and Investigations, Anti-Corruption and FCPA, or Artificial Intelligence practice groups:

Artificial Intelligence:

Keith Enright – Palo Alto (+1 650.849.5386, kenright@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Robert Spano – London/Paris (+33 1 56 43 13 00, rspano@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213.229.7186, evandevelde@gibsondunn.com)
Frances A. Waldmann – Los Angeles (+1 213.229.7914,fwaldmann@gibsondunn.com)

White Collar Defense and Investigations / Anti-Corruption and FCPA:

Washington, D.C.
F. Joseph Warin (+1 202.887.3609, fwarin@gibsondunn.com)
Stephanie Brooker (+1 202.887.3502, sbrooker@gibsondunn.com)
Courtney M. Brown (+1 202.955.8685, cmbrown@gibsondunn.com)
David P. Burns (+1 202.887.3786, dburns@gibsondunn.com)
John W.F. Chesley (+1 202.887.3788, jchesley@gibsondunn.com)
Daniel P. Chung (+1 202.887.3729, dchung@gibsondunn.com)
M. Kendall Day (+1 202.955.8220, kday@gibsondunn.com)
Stuart F. Delery (+1 202.955.8515, sdelery@gibsondunn.com)
Michael S. Diamant (+1 202.887.3604, mdiamant@gibsondunn.com)
Gustav W. Eyler (+1 202.955.8610, geyler@gibsondunn.com)
Melissa Farrar (+1 202.887.3579, mfarrar@gibsondunn.com)
Amy Feagles (+1 202.887.3699, afeagles@gibsondunn.com)
Scott D. Hammond (+1 202.887.3684, shammond@gibsondunn.com)
George J. Hazel (+1 202.887.3674, ghazel@gibsondunn.com)
Adam M. Smith (+1 202.887.3547, asmith@gibsondunn.com)
Patrick F. Stokes (+1 202.955.8504, pstokes@gibsondunn.com)
Oleh Vretsona (+1 202.887.3779, ovretsona@gibsondunn.com)
David C. Ware (+1 202.887.3652, dware@gibsondunn.com)
Ella Alves Capone (+1 202.887.3511, ecapone@gibsondunn.com)
Nicole Lee (+1 202.887.3717, nlee@gibsondunn.com)
Lora Elizabeth MacDonald (+1 202.887.3738, lmacdonald@gibsondunn.com)
Bryan Parr (+1 202.777.9560, bparr@gibsondunn.com)
Pedro G. Soto (+1 202.955.8661, psoto@gibsondunn.com)

New York
Zainab N. Ahmad (+1 212.351.2609, zahmad@gibsondunn.com)
Reed Brodsky (+1 212.351.5334, rbrodsky@gibsondunn.com)
Mylan L. Denerstein (+1 212.351.3850, mdenerstein@gibsondunn.com)
Karin Portlock (+1 212.351.2666, kportlock@gibsondunn.com)

Mark K. Schonfeld (+1 212.351.2433, mschonfeld@gibsondunn.com)
Orin Snyder (+1 212.351.2400, osnyder@gibsondunn.com)

Dallas
David Woodcock (+1 214.698.3211, dwoodcock@gibsondunn.com)

Denver
Ryan T. Bergsieker (+1 303.298.5774, rbergsieker@gibsondunn.com)
Robert C. Blume (+1 303.298.5758, rblume@gibsondunn.com)
John D.W. Partridge (+1 303.298.5931, jpartridge@gibsondunn.com)
Laura M. Sturges (+1 303.298.5929, lsturges@gibsondunn.com)

Houston
Gregg J. Costa (+1 346.718.6649, gcosta@gibsondunn.com)

Los Angeles
Michael H. Dore (+1 213.229.7652, mdore@gibsondunn.com)
Michael M. Farhang (+1 213.229.7005, mfarhang@gibsondunn.com)
Diana M. Feinstein (+1 213.229.7351, dfeinstein@gibsondunn.com)
Douglas Fuchs (+1 213.229.7605, dfuchs@gibsondunn.com)
Nicola T. Hanna (+1 213.229.7269, nhanna@gibsondunn.com)
Poonam G. Kumar (+1 213.229.7554, pkumar@gibsondunn.com)
Marcellus McRae (+1 213.229.7675, mmcrae@gibsondunn.com)
Eric D. Vandevelde (+1 213.229.7186, evandevelde@gibsondunn.com)
Debra Wong Yang (+1 213.229.7472, dwongyang@gibsondunn.com)

San Francisco
Winston Y. Chan (+1 415.393.8362, wchan@gibsondunn.com)
Charles J. Stevens (+1 415.393.8391, cstevens@gibsondunn.com)

Palo Alto
Benjamin Wagner (+1 650.849.5395, bwagner@gibsondunn.com)

London
Patrick Doris (+44 20 7071 4276, pdoris@gibsondunn.com)
Sacha Harber-Kelly (+44 20 7071 4205, sharber-kelly@gibsondunn.com)
Michelle Kirschner (+44 20 7071 4212, mkirschner@gibsondunn.com)
Allan Neil (+44 20 7071 4296, aneil@gibsondunn.com)
Matthew Nunan (+44 20 7071 4201, mnunan@gibsondunn.com)
Philip Rocher (+44 20 7071 4202, procher@gibsondunn.com)

Paris
Benoît Fleury (+33 1 56 43 13 00, bfleury@gibsondunn.com)
Bernard Grinspan (+33 1 56 43 13 00, bgrinspan@gibsondunn.com)

Frankfurt
Finn Zeidler (+49 69 247 411 530, fzeidler@gibsondunn.com)

Munich
Kai Gesing (+49 89 189 33 285, kgesing@gibsondunn.com)
Katharina Humphrey (+49 89 189 33 155, khumphrey@gibsondunn.com)
Benno Schwarz (+49 89 189 33 110, bschwarz@gibsondunn.com)

Hong Kong
Kelly Austin (+1 303.298.5980, kaustin@gibsondunn.com)
Oliver D. Welch (+852 2214 3716, owelch@gibsondunn.com)

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm,
please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists,
please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at gibsondunn.com