

ALERT

DOJ Refreshes Guidance for Prosecutors on Evaluating Corporate Compliance Programs — Renewed Focus on Data, Resourcing, and Evolution of Programs

June 5, 2020

WHAT: The Department of Justice (DOJ) Criminal Division announced revisions to its year-old guidance for Criminal Division prosecutors on the evaluation of corporate compliance programs.

WHEN: DOJ released the revised guidance on June 1, 2020.

WHAT DOES IT MEAN FOR INDUSTRY: The new version refines the various factors against which compliance programs will be measured in the event DOJ is tasked with a determination of how, and whether, to penalize an entity as part of a criminal investigation and resolution. Among the key factors added to the guidance were changing the previous focus from the traditional “tone at the top” to a broader fostering of a culture of compliance and ethics “at all levels of the company,” and including a culture of compliance “from the middle.” The new guidance continues to emphasize the collection and use of data, both for continuous testing and improvement of existing compliance programs as well as to demonstrate proper resourcing for compliance-related employees. DOJ prosecutors will ask companies to “show their work” with hard data collected over the life of a program.

Overall, the guidelines reiterate the value DOJ places on regularly testing, reviewing, and updating corporate compliance programs to account for evolving risks and circumstances. The guidelines, which first started as a smaller series of questions posed by then-DOJ Fraud Section compliance consultant Hui Chen, were first released in 2017

Authors

Kevin B. Muhlendorf
Partner
202.719.7052
kmuhlendorf@wiley.law

Brandon J. Moss
Partner
202.719.7554
bmoss@wiley.law

Practice Areas

Government Contracts
Internal Investigations and Compliance Programs
White Collar Defense & Government Investigations

and last revised in 2019. The newest iteration, released on June 1, 2020, includes additional information reflecting the importance DOJ places on companies ensuring that compliance programs are dynamic and being updated to fit changing circumstances. In releasing the new guidance, Criminal Division head Brian Benczkowski said the revisions were “based on our own experience and important feedback from the business and compliance communities.”

The Revisions

As an initial matter, DOJ has added detail to its assertion that prosecutors make an “individualized determination in each case,” requiring that they consider factors such as “the company’s size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company’s operations, that might impact its compliance program.” New language includes a directive that prosecutors should evaluate programs both at the time of the offense and at the time of a charging decision and resolution – to emphasize the credit potentially given for remedial actions after a compliance failure is recognized. The revised guidance follows the same structure as the prior iteration, dividing these questions into three categories: (1) program design; (2) program application; and (3) program efficacy.

Program Design

In line with the charge to individually analyze each company’s program, the revised policy urges prosecutors to determine “why the company has chosen to set up the compliance program the way that it has, and why and how the company’s compliance program has evolved over time.” The policy also permits prosecutors to credit risk-based compliance programs that provide sufficient resources to evaluate “high-risk transactions” even if the program “fails to prevent an infraction.”

Building on the prior policy’s instruction to consider whether a company’s risk assessment is “periodically updated,” the revised version asks: “Is the periodic review limited to a ‘snapshot’ in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls?” The repeated focus in the guidelines on the use of “data” in updating compliance programs demonstrates how important it is to document why a company makes the changes it does. To that end, the revised guidance further asks whether the company has “a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company’s own prior issues or from those of other companies” in the same industry or region.

The revised guidance also focuses on employee access to company compliance policies, procedures, and training. The addition of questions asking if policies and procedures have “been published in a searchable format for easy reference,” and whether the company tracks employee access to policies in order to understand whether certain “policies are attracting more attention from relevant employees” again points to the collection of “data” in which DOJ expects companies to engage to understand the effectiveness of their compliance programs. With respect to training, DOJ again emphasizes the difference between companies of different size, sophistication, and industry, acknowledging that some companies provide training and advice as needed, whereas others provide “more targeted training sessions to enable employees to timely identify

and raise issues to appropriate compliance, internal audit, or other risk management functions.” With any training, DOJ queries whether the company provides “a process by which employees can ask questions arising out of the trainings” and a procedure for employees who fail post-training testing. This addition seems to amplify the earlier guidance about making sure trainings are in the right languages – DOJ will not credit “training” that does not actually improve employees’ understanding of the importance of compliance. With that in mind, the new guidance also asks whether a company evaluates “the extent to which the training has an impact on employee behavior or operations.”

With respect to internal reporting and investigations, companies are expected to “take measures to test whether employees are aware of” reporting mechanisms such as hotlines and to test their effectiveness by tracking reports from “start to finish.” The new guidance explicitly includes language asking whether third parties have access to a company’s reporting mechanism.

Recognizing the outsized role third parties play in many compliance failures, especially in the Foreign Corrupt Practices Act (FCPA) realm, the revised guidance includes some nuanced changes to its third-party language. Continuing with the theme of being able to “show your work,” prosecutors will look to see if a company has documented “the business rationale” for involving any third party in a transaction “and the risks posed by third-party partners.” In explicitly stating that prosecutors will look for those records, DOJ is not so subtly reminding entities that the failure to do that analysis may suggest the use of third parties for inappropriate purposes or sham transactions. Finally, and again highlighting the importance of the dynamic nature of compliance, prosecutors will have to determine whether the company engages “in risk management of third parties throughout the lifespan of the relationship or primarily during the onboarding process.” In other words, is your third-party management “set it and forget it,” or does a company periodically test for third-party compliance issues?

This emphasis on outside parties continues with a renewed focus on mergers and acquisitions. Compliance programs are expected to include not only initial due diligence on targets, but also “a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls.” Prosecutors will also query whether a company has a procedure for “conducting post-acquisition audits[] at newly acquired entities.” Much like with the continual need to monitor true third-party due diligence, DOJ is signaling that after a merger or acquisition, a company needs to test the implantation of any compliance changes made to the target company. This is especially important with entities acquired overseas and in places with a less rigorous compliance culture than in the United States. And, in a footnote at the end of the guidelines, new language states that if a company claims that foreign law affects how it designs or implements a program, prosecutors should ask for an explanation of how that decision was reached and how the company attempted to maintain the effectiveness of its core compliance program when faced with such a limitation.

Program Application

Compliance officers seeking better and more bountiful resources will undoubtedly appreciate DOJ's amplification of its previous focus on proper resourcing of the compliance function. The new guidance not only focuses on "resourcing," but also on whether those implementing the program are "empowered to function effectively." The revisions emphasize that "[e]ven a well-designed compliance program" may not succeed if it is "under-resourced" and that compliance must be promoted "at all levels of the company," including a strong commitment from middle management.

In a very important addition to the guidance, DOJ now explicitly states that it will evaluate "[d]ata resources and access." Echoing its previous statements about the use of data to test the effectiveness of a compliance program, the new guidance has prosecutors asking whether "compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions" and whether "any impediments exist that limit access to relevant sources of data." This focus on access to data flows directly from the concept of questioning whether the compliance function is "empowered." If the compliance function is not empowered to obtain the data it needs to test, DOJ is likely to look at a program as nothing more than a paper program and not one it is willing to credit.

Finally, a notable addition in the implementation section is the question of whether a company's compliance personnel "monitor its investigations and resulting discipline to ensure consistency." While certainly an important metric, it does place the DOJ's prosecutors in the position of playing a human resources role, something for which they are uniquely unsuited.

Program Efficacy

The section on program efficacy was little changed from the prior version, with the notable addition of a question asking whether the company "review[s] and adapt[s] its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks." This simply serves as a reminder of the importance DOJ places on the dynamic, rather than static, nature of compliance programs.

Key Takeaways

Through twenty pages of questions, the key takeaways are readily apparent in the additions to the guidance discussed above. But distilled to their essence, DOJ wants companies to be able to demonstrate that compliance programs were intentional, well-reasoned, and dynamic. In order to prove that to DOJ, companies should focus on three goals.

First, data is key. Programs that do not include the collection and analysis of data to test and improve the program's structure and implementation will fail DOJ's scrutiny.

Second, decisions related to compliance issues need to be documented. Not only does documentation allow a company to show DOJ the steps it took in the event of a compliance failure, but the process of compiling the documentation lends itself to a conclusion that the decision was a well-reasoned and considered one. DOJ is

clearly signaling that while compliance failures will inevitably happen, if a company can show that the decisions leading up to the failure were intentional and well meaning, and were followed by remedial action, prosecutors should be more willing to issue a declination.

Finally, a compliance program is only as good as the people implementing it. From executives at the top to employees in the field, DOJ wants to see compliance programs that are thoughtful in how they educate employees, empower compliance officials, and remediate problems when they are uncovered.

Conclusion

Even though the updated guidance does not substantially change what DOJ has said for years about the central tenets of an effective compliance program, it does offer important additional details that, collectively, create a more sophisticated roadmap for companies seeking to improve their existing compliance programs. While no compliance program is foolproof, with the benefit of having examined many programs, DOJ's latest guidance can both help prevent compliance failures and, if utilized properly, assist in a defense if those compliance failures face DOJ review.