

## [Updates](#)

March 07, 2023

### DOJ Announces Shift Toward Corporate Enforcement for Sanctions and Export Control Violations



Deputy Attorney General (DAG) Lisa Monaco once again delivered groundbreaking [remarks](#) at the American Bar Association (ABA) National Institute on White Collar Crime (ABA White Collar Conference) on March 2, 2023, this time heralding a new era of corporate enforcement aimed at addressing U.S. national security priorities. Last spring, as the United States enacted sanctions against Russia, DAG Monaco described sanctions as "the new FCPA (Foreign Corrupt Practices Act)" in terms of Department of Justice (DOJ) priorities, sending shockwaves through the world of corporate compliance. Since then, DOJ has borne out that promise, largely through an aggressive campaign championed by [Task Force KleptoCapture](#), resulting in a large number of [criminal cases targeting individual defendants](#).

In this most recent announcement, DAG Monaco set a new tone, announcing that enforcement of national security-related violations—most notably sanctions evasion and export control violations—against *corporations* would be among the top priorities of DOJ. Later in the day, Matthew Axelrod, assistant secretary for export enforcement within the Department of Commerce (DOC) Bureau of Industry and Security (BIS), drove home that point. He emphasized that companies should no longer view export control and sanctions violations as "technical violations," but would be well-advised to view them as enterprise risks given the prioritization these issues are receiving within the various government enforcement agencies, including as a corporate criminal enforcement priority within DOJ. Further highlighting this new landscape, the Department of Treasury Office of Foreign Assets Control (OFAC) spoke at the ABA White Collar Conference for the first time ever on March 2. DOJ, BIS, and OFAC issued their first-of-its-kind joint [compliance guidance](#) the same day, relating to third-party intermediary risks.

It was a day filled with sea-change announcements for sanctions and export control enforcement, but the takeaway was simple: Sanctions and export controls are the new FCPA in terms of corporate enforcement priorities and related compliance expectations. The Money Laundering and Asset Recovery Section (MLARS) has already begun conducting sanctions- and export-related investigations.

## **New and Improved DOJ National Security Division**

In her remarks, DAG Monaco suggested that DOJ will be working to add capabilities to the National Security Division (NSD), similar to the Fraud Division, which has had significant success in prosecuting FCPA violations against corporations over the past few decades. NSD's Counterintelligence and Export Control Section (CES), formerly the Counterespionage Section, has always handled complex white-collar cases, such as economic espionage and export control violations, and that longstanding expertise will likely be expanded and supported by substantial additional bandwidth. DAG Monaco shared details as to several significant changes to DOJ's NSD that will herald a new era of corporate enforcement focusing on national security priorities, including:

- Shifting the focus from terrorism-related crimes (which typically involve individuals and non-state actors) to threats related to state-sponsored activities (such as by Russia, China, and North Korea), which more heavily implicate cross-border corporate activity.
- Adding more than 25 new prosecutors to NSD.
- Adding a new chief counsel for corporate enforcement role at NSD.
- Issuing joint guidance with BIS and OFAC relating to corporate compliance expectations.

## **New Guidance on Third-Party Intermediaries and Compliance**

Beyond the recent slew of Task Force KleptoCapture enforcement actions, the enforcement community further evidenced its conviction to this mission by issuing the unprecedented joint corporate compliance guidance relating to sanctions and export control compliance the same day as DAG Monaco's announcements.

This guidance, promulgated jointly by DOJ, OFAC, and BIS (the Agencies), focused on steps companies can take to mitigate the risks of sanctions and export control violations involving third-party intermediaries, such as agents, intermediary customers, and distributors, who may facilitate efforts by other parties to evade U.S. restrictions. The guidance sets out a series of red flags to help businesses identify when third-party intermediaries may be engaged in efforts to evade sanctions and export controls, including notably:

- Use of corporate vehicles to obscure (1) ownership, (2) source of funds, or (3) countries involved, particularly sanctioned jurisdictions.
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration.
- Internet Protocol (IP) addresses that do not correspond to a customer's reported location data.
- Payment coming from a third-party country or business not listed on the End-User Statement or other applicable end-user form.
- Transactions involving entities with little or no web presence.
- Routing purchases through certain transshipment points commonly used to illegally redirect restricted items to Russia or Belarus (e.g., China (including Hong Kong and Macau), Armenia, Turkey, and Uzbekistan).

The guidance also advises caution with respect to entities that use complex sales and distribution models, as this may obscure visibility into the ultimate end users of an organization's technology and services. While the list of red flags in the guidance is not exhaustive, it reflects factors U.S. enforcement agencies will focus on when evaluating corporate compliance relating to the involvement of intermediary entities.

## **New Compliance Program Expectations**

In addition to the red flags, the guidance re-emphasized the corporate compliance program expectations set out in prior guidance from the Agencies—including the OFAC [guidance](#) titled "A Framework for OFAC Compliance Commitments," issued in May 2019. The guidance also provides new clarification as to the compliance program expectations for organizations. In particular, organizations' risk-based compliance programs must be "effective," as described in the guidance. The guidance does not expressly define the term "effective" or how an organization will be assessed for "effectiveness," but it provides that an "effective" risk-based compliance program should include management commitment (including compensation incentives), risk assessment, internal controls, testing, auditing, and training. "Effective" compliance programs employ a risk-based approach to sanctions and export controls compliance by developing, implementing, and routinely updating a compliance program, depending on the organization's size and sophistication, products and services, customers and counterparties, and geographic locations.

The guidance clarifies the Agencies' due diligence expectations within an organization's risk-based compliance program. Specifically the guidance provides that as a "best practice," due diligence should not only be conducted on an organization's customers, but also on intermediaries and counterparties that are involved in customer transactions. In this regard, the guidance notes that optimal compliance programs should include controls tailored to the risk the business faces, such as diversion by third-party intermediaries.

The guidance also references "compensation incentives" as a component to an "effective" compliance program. In her comments, DAG Monaco notes that she announced last September that DOJ would examine corporate compensation programs to shift the burden of corporate malfeasance away from uninvolved shareholders onto those more directly responsible, and that companies should ensure that executives and employees are personally invested in promoting compliance. Nothing grabs attention or demands personal investment like having skin in the game, through direct and tangible financial incentives. DAG Monaco further noted that she asked DOJ's Criminal Division to talk to practitioners, consult with regulators, and develop guidance on how to reward corporations with compliance-promoting compensation programs.

The guidance also highlighted the voluntary self-disclosure policies of each of the enforcement agencies implicated, emphasizing the benefits of adopting procedures designed to detect wrongdoing internally and voluntarily report to regulators.

## **What Does This Mean?**

The upshot is that companies can expect that sanctions violations and export controls violations will be increasingly pursued with the same level of resources and vigor that we have come to expect from DOJ with regard to FCPA enforcement. DOJ has provided a helpful roadmap in explicitly modeling changes to the NSD after the Fraud Section. Companies should consider following suit by carefully updating and evaluating the effectiveness of their existing risk-based compliance programs, as appropriate based upon the guidance; assessing their sanctions and export control risks; and leveraging their anti-corruption compliance infrastructure to prioritize these risk areas.

For matters related to sanctions and export control compliance, corporations should consult with experienced counsel.

© 2023 Perkins Coie LLP

## **Authors**

## **Explore more in**

[White Collar & Investigations](#) [Financial Transactions](#) [Government Contracts](#) [International Trade](#)  
[Data Security Counseling and Breach Response](#) [Forest Products](#) [Mining](#) [Oil & Gas](#)

## **Related insights**

Update

[\*\*The FY 2025 National Defense Authorization Act: What's New for Defense Contractors\*\*](#)

Update

[\*\*January Tip of the Month: Trump Executive Orders Challenge DEI Programs\*\*](#)