

Guiding Your Company Through Trump's New Latin America Enforcement Policy

Article By:

Seth D. DuCharme

Thomas F. Kokalas

Jeffery B. Vaden

Margaret B. Beasley

Madeline Fogel

Shortly after President Trump's second inauguration, his executive branch took steps to further one of his signature promises: securing the southern border. While these actions primarily impact immigration laws, several executive orders, such as designating drug cartels and their affiliates as "terrorist organizations," have increased the legal and compliance risk environment for both US and foreign companies.

While regulations pertaining to known terrorist organizations like ISIS and Al-Qaeda have been part of the global sanctions and anti-money laundering framework for quite some time, the addition of Mexican, Central and South American drug cartels to this list introduces new and complex risks for companies conducting cross-border business in these jurisdictions. To prevent violating these new requirements, companies should evaluate their Latin American operations and work to establish strong controls and compliance measures to ensure that they do not do business with or unwittingly provide material support to these organizations.

Below we provide an overview of the new directives and explain how businesses should prepare for the new regulations.

Executive Actions Look South

On his first day in office, President Trump issued a series of executive orders focused on this issue, including E.O. 14157, "[Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists](#)"; E.O. 14161, "[Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats](#)" and E.O. 14159, "[Protecting the American People Against Invasion](#)" (together, the January 20 E.O.s). And on

February 5, her first day in charge of the Justice Department, Attorney General Pam Bondi issued several memoranda providing guidance on how the Department will shift its priorities and make additional resources available to reflect the administration's focus on the southern border: the [Bondi Memorandum regarding Charging, Plea Negotiations, and Sentencing](#) and the [Bondi Memorandum regarding Total Elimination of Cartels and Transnational Criminal Organizations](#) (together, the Bondi Memoranda).

The Bondi Memoranda prioritize enforcement actions directed at, in part, the “*total elimination* of Cartels and Transnational Criminal Organizations (TCOs)” and the historic threats from widespread illegal immigration, dangerous cartels, transnational organized crime, gangs, human trafficking and smuggling, fentanyl and opioids, terrorism and other sources. To eradicate these threats, DOJ will enhance its focus on investigations related to immigration enforcement, human trafficking and smuggling, transnational organized crime and cartels and gangs.

Specific to white collar enforcement, the Department will now be prioritizing investigations into companies that provide material support or resources to designated foreign terrorist organizations (FTOs) or bribe foreign government officials to facilitate the criminal operations of cartels and TCOs under the Foreign Corrupt Practices Act (FCPA).

As the administration adds to the list of cartel-related entities that fall under these new designations, risk for companies doing business abroad will increase. For example, E.O. 14157 ordered the Secretary of the State to recommend additional cartels and organizations for designation as FTOs or Specially Designated Global Terrorists (SDGTs) with a focus, but not limitation, on cartels operating in certain portions of Mexico. While we await these designations, which the Secretary of State was supposed to have recommended on February 3, Congressman Chip Roy (TX-21) reintroduced the Drug Cartel Terrorist Designation Act, which would direct the designation of the Gulf Cartel, the Cartel Del Noreste, the Cartel de Sinaloa, and the Cartel Jalisco Nueva Generacion as FTOs and codify E.O. 14157 into law.

Increased Risk for Companies Operating in Mexico, Central and South America

While it is likely that at least some of the soon-to-be-designated entities already have sanctioned individuals under the US Department of Treasury's Office of Foreign Asset Control's regulations, we anticipate that the list will grow significantly. Making the matter more complicated, however, is that cartels, their affiliated entities and the persons that control these organizations have embedded themselves across many business areas in Latin America. So, the designation as an FTO is significant for several reasons:

- **Specific criminal law:** It is a criminal offense under 18 U.S.C. § 2339B for companies and individuals to knowingly provide *material support* to FTOs, a sanction that does not currently exist under an SDN designation. The government broadly defines “[material support](#)” to include providing an FTO with *any* property (tangible or intangible) or services, including currency, financial services, lodging, personnel, and transportation. Thus, any transaction with an FTO could be viewed as providing “material support” to a terrorist organization that could result in significant fines and penalties for the organization. This includes “fees” that cartels routinely charge companies to operate in certain areas.

In one notable example of a prosecution under § 2339B, French building materials manufacturer [Lafarge pled guilty in 2022](#) to a one-count criminal information charging conspiracy to provide material support and resources in Northern Syria from 2013 to 2014 to

the Islamic State of Iraq and al-Sham (ISIS) and the al-Nusrah Front (ANF), both US-designated FTOs. According to court documents, Lafarge and its Syrian subsidiary schemed to pay ISIS and ANF in exchange for permission to operate a cement plant in Syria, which enabled the subsidiary to obtain approximately \$70.3 million in revenue.

- **Extraterritorial reach:** Restrictions on dealing with FTOs expands the reach of US regulators to non-US entities. While SDNs restrictions have certain reach to allow the United States to sanction extra-territorial actors, they are largely aimed at US entities and transactions involving US entities — 18 U.S.C. § 2339B has no such limitation. In other words, just as with Lafarge, a non-US company doing business with an FTO in Latin America can be prosecuted through the extraterritorial reach of 18 U.S.C. § 2339B. Indeed, there is precedent for such charges: [Chiquita Banana pled guilty in 2007](#) to making payments to an FTO (the AUC in Colombia) and agreed to pay a fine of \$25 million. E.O. 14157 increases the risk of similar prosecutions in the future.
- **Civil liability:** Under the civil liability provisions of the Anti-Terrorism Act, 18 U.S.C. § 2333, a company can be directly liable for engaging in an act of international terrorism by providing material support to an FTO, or indirectly under the aiding and abetting provision for knowingly providing substantial assistance to the perpetrators of an attack committed, planned, or authorized by an FTO. The Act allows plaintiffs to recover treble damages, plus the cost of the suit, including attorney's fees, which can add up exponentially.
- **Civil forfeiture:** While current sanctions regimes allow US authorities to freeze assets of sanctioned entities, authorities may not take title to those assets without proving in court that the assets are related to a criminal offense. An FTO designation and related statutes will likely make it easier for the government to carry this burden, and even lighten it by arguably reducing the need to show a nexus to the United States.

How Companies Should Prepare

The combination of these new areas of risk and DOJ's new focus on FTOs, TCOs, and SDGTs has important implications for companies conducting business internationally, particularly in Mexico and other parts of Latin America where cartels that are (or will be) designated as FTOs and TCOs are active. But that is not to say the companies cannot do business in the region. Rather, the risk can be mitigated and managed through robust policies, internal controls and compliance procedures. For example, companies should:

- **Conduct third-party due diligence:** In a heightened regulatory framework, a company needs to know the counterparties it does business with to determine whether they are a sanctioned or designated party. In addition, doing business with third parties like vendors, agents or "finders," consultants, and distributors or sales representatives can increase your compliance associated risks. Conducting enhanced due diligence is the best way to detect potential problem areas and prevent liability. Effective due diligence should be tailored to the company's business and risks associated with that business and may include:
 - Media/internet searches.
 - OFAC sanctions list searches.
 - Commerce Department entity list searches.
 - Beneficial ownership reviews.
 - Politically exposed person reviews.
 - Company/business registries searches.
 - Site visits.
 - Litigation records reviews.
 - Corporate and leadership references.

- **Be aware of red flags:** A company should know what to look for while conducting due diligence. Red flags may include:
 - Failure of potential partners to maintain appropriate government registrations.
 - Negative media and/or reference reports, particular those that suggest non-compliant or unlawful conduct.
 - Requests for excessive fees or commissions, cash payment, or excessive discretionary funds.
 - The third-party refuses to provide reasonable information to assess ownership information, or says “don’t worry about it,” or “you don’t want to know.”
 - Agreements that include vaguely or improperly described services.
- **Use internal controls:** Robust compliance programs utilize a system of internal controls that help provide “reasonable assurances” that transactions are properly authorized and do not violate anti-money laundering rules or sanctions regulations. Implementing effective internal accounting and compliance controls not only ensures the reliability of financial reporting but it reduces the susceptibility that a company unwittingly provides material support to a designated terrorist organization or any of its affiliates. Along with internal accounting controls, it is important to establish a culture of integrity and ethics and put mechanisms in place to monitor compliance and report non-compliance.
- **Update your compliance program:** The hallmarks of a good compliance program include, among other things:
 - A high-level commitment to corporate compliance policy by directors and senior management.
 - Clearly articulated and visible written policies.
 - Documentation of the purpose of all payments.
 - Periodic risk-based assessments that addresses the individual circumstances of the company.
 - Proper oversight and independence with appropriate funding resources.
 - Training and guidance that is effectively communicated to all directors, officers and employees.
 - Internal reporting system for confidential, internal reporting of compliance violations.
 - Effective process for responding to, investigating and documenting allegations of violations.
 - Enforcement that incentivizes compliance and disciplines violations.
 - Effective training and oversight of third-party relationships.
 - Monitoring and testing of the effectiveness of the compliance program.