Export Controls Without Borders: How Foreign-Made Products Trigger U.S. Criminal Liability

Robert J. Anello, Partner

As recent enforcement activity demonstrates, a company does not need an American factory, American employees, or American exports to be subject to American export controls. If a company manufactures items abroad using technology originating from the U.S. and exports those items to U.S.-restricted entities, the company can be subject to American criminal jurisdiction. The risk calculus for multinational companies to avoid U.S. prosecution has changed sharply in recent months. Expanded regulatory provisions and heightened national security priorities have combined to extend U.S. export control enforcement far beyond companies operating on American soil. At the center of this shift is the Foreign-Direct Product Rules ("FDPR"). Once an obscure regulatory provision, the FDPR now extends the scope of U.S. export controls to certain foreign-made items. Willful violations of the FDPR bring criminal consequences under the Export Control Reform Act ("ECRA"), including up to 20 years' imprisonment and $1 million in criminal fines. FDPR prosecutions align with the Justice Department's commitment to strong enforcement of export controls to protect against national security threats. Companies that recognize internal FDPR violations may find a safe harbor – if they are willing to self-disclose, cooperate, and remediate.

The June 2026 resolution involving Robert Bosch GmbH ("Bosch") can help companies to evaluate their export enforcement risk. Between 2020 and 2024, two Bosch German subsidiaries exported approximately $72.4 million worth of foreign-produced sensors and automotive software to Huawei Technologies and its affiliates without the U.S. export licenses required under the FDPR. Bosch's trade compliance personnel misunderstood the FDPR's scope, erroneously concluding that the regulation applied only to physical goods and not software, and failed to act on warnings from third-party companies that flagged potential FDPR issues. Bosch voluntarily disclosed its conduct to the DOJ's National Security Division ("NSD") and the U.S. Commerce Department's Bureau of Industry and Security ("BIS") before the company finished its own internal investigation. The government then launched its inquiry. Bosch maintained that notwithstanding the mistakes uncovered by the internal investigation in the application of the FDPR, Bosch did not believe those mistakes rose to the level of acting "willfully", as required for criminal violations, and were "unintentional." On June 17, the DOJ's National Security Division ("NSD") announced that it had declined to prosecute Bosch under its 2026 Corporate Enforcement and Voluntary Self-Disclosure Policy ("CEP") – the first such declination by the NSD. Consistent with the CEP, the NSD imposed disgorgement in the amount of $11,430,098.00. That same day, BIS announced a parallel civil administrative settlement with Bosch imposing $36,184,680 in penalties. The Bosch resolution is both a success story and a cautionary tale: U.S. export control jurisdiction has expanded, compliance expectations are rising, and enforcement agencies are working in concert.

The Expansive Jurisdiction of the FDPR

The FDPR, codified in the U.S. Export Administration Regulations, has been significantly expanded in recent years through additions of entity-specific foreign-direct product rules (targeting named companies), destination specific rules (targeting named countries) and rules that apply to semiconductor manufacturing equipment. The effect is that the FDPR requires even non-U.S. companies with non-U.S. factories utilizing U.S. technology at any stage in their design or production to comply with U.S. export rules, or

obtain authorization to ship to restricted parties or destinations. A component of a product manufactured entirely in Germany, using production equipment that incorporates U.S.-origin software, can be subject to U.S. export licensing requirements under the FDPR.

The Growth of the FDPR

The FDPR's current prominence belies its origins as an obscure Cold War-era provision. Introduced in 1959, the rule was designed to prevent the transfer of U.S.-derived technology to Soviet bloc nations and was rarely invoked for most of the next six decades. Then in May 2020, BIS expanded the FDPR to target Huawei Technologies specifically. By applying the FDPR to Huawei's supply chain, BIS effectively cut off the company from advanced chips produced by foundries outside the United States.

In February 2022, the FDPR was deployed again as part of the U.S. sanctions response to Russia's invasion of Ukraine, restricting Moscow's access to foreign-made electronics, avionics, and other dual-use goods. Then, in October 2022, BIS issued sweeping new export controls targeting China's advanced semiconductor, artificial intelligence, and supercomputing sectors, layering additional FDPR provisions that were further expanded in October 2023 and again in December 2024 to cover semiconductor manufacturing equipment and high-bandwidth memory. The cumulative effect of these expansions of the reach of the FDPR has been to transform the statute from a dormant regulatory tool into the primary mechanism through which the United States asserts extraterritorial control over global technology supply chains.

The Corporate Enforcement Policy in Action

The NSD resolution with Bosch speaks of systemic—albeit unintentional—compliance failures: the company's trade compliance personnel were "ill-equipped to provide accurate guidance on the FDPR," erroneously concluding that the rule applied only to physical goods (not software) and ignored "several missed opportunities where third-party companies identified potential applications of the FDPR." Despite external warnings, sales continued for years. Despite any missteps, however, the government recognized the company's voluntary self-disclosure, full cooperation, timely remediation, and the absence of aggravating circumstances – the four factors necessary to earn a declination of prosecution under the 2026 CEP. Bosch's declination marks the first time the NSD has applied the 2026 CEP, and only the second declination under the CEP overall (following the Criminal Division's Fraud Section declination regarding Balt SAS, a French medical device company, on March 19, 2026). The NSD's declination agreement explains what Bosch did to earn the company the most favorable resolution. Prior to closing its own investigation, Bosch disclosed findings from its investigation and turned over all relevant facts and documents to the NSD and BIS. Bosch maintained that its mistakes did not amount to willful misconduct. Additionally, Bosch engaged external counsel, made significant organizational changes (such as adding 66 employees to Bosch's trade compliance organization), and expanded U.S. export control screening tools as part of the company's remediation efforts.

The NSD also recognized the adequacy of BIS's $36 million penalty against the company and imposed disgorgement in the amount of approximately $11.4 million to be paid within 30 days of the agreement. The financial ramifications, however, pale in comparison to the effects criminal charges may have had on the company.

The Bigger Picture: DOJ's National Security Enforcement Posture

The Bosch declination should not be interpreted as a retreat from enforcement. On March 30, 2026, the NSD stated that "enforcing export control and sanctions laws is a top priority" and furthers the NSD's mission to "protect and defend the United States against the full range of national security threats." Secretary of Commerce Howard Lutnick has similarly emphasized the importance of enforcement of export controls related to China.

More broadly, the enforcement landscape reflects a convergence among government entities that companies cannot afford to ignore.

DOJ and BIS are coordinating criminal and civil investigations, sharing information and aligning enforcement. The addition of export control enforcement to the NSD's portfolio, which historically was dominated by counterterrorism and espionage cases, signals that trade compliance failures are now treated as national security threats in their own right. The Bosch declination is an example of the government's deliberate policy choice to use the full weight of the federal enforcement apparatus to deter export control violations, particularly those involving controlled technology transfers to China and other strategic competitors.

Practical Implications for Multinational Companies

One of the most striking aspects of the Bosch matter is that third-party companies flagged potential FDPR issues, but those warnings were not adequately captured or acted upon by Bosch. These facts underscore the need for compliance programs that include formal mechanisms for receiving, documenting, and escalating third-party notifications regarding potential export control exposure. A compliance system that lacks intake protocols for external warnings is, in the government's view, fundamentally deficient.

Bosch's decision to self-disclose to the NSD and BIS while its internal investigation was still ongoing was critical to securing its declination. Waiting until an investigation is complete may sacrifice the timeliness that DOJ credits. Companies should establish internal protocols that trigger early legal assessment and escalation of potential export control issues to senior management and outside counsel, enabling disclosure decisions to be made on a timeline that satisfies the CEP's expectations.

Securing a declination also required Bosch to undertake substantial remediation, not merely to self-report. Companies should consider: (a) engaging specialized external counsel with export control expertise at the earliest sign of a potential violation; (b) conducting a comprehensive internal investigation, including a close review of affected transactions; (c) implementing organizational restructuring of the company's trade compliance function, including additional headcount and reporting lines; (d) deploying enhanced screening tools and classification procedures, particularly for software and technology transfers; (e) retraining personnel on the FDPR's application to both physical goods and software; and (f) establishing monitoring and audit functions to identify and prevent future violations.

Corporate officers, compliance personnel, and business-line executives also should understand that a declination against a company does not immunize individuals. A company's cooperation may involve disclosure of information regarding individual conduct, leaving open the possibility of individual prosecution for those responsible for the compliance failures or who had knowledge of the violative conduct.

Conclusion

The current enforcement environment demands that multinational companies treat U.S. export controls not as a peripheral regulatory concern, but as a real company risk. The expansion of the FDPR, the coordination between DOJ and BIS, and the extension of the CEP to national security matters collectively have raised both the stakes and the standards. Companies should audit their FDPR exposure across all foreign operations, strengthen escalation protocols to ensure that third-party warnings and internal red flags reach decision-makers, and develop an integrated criminal-civil disclosure strategy that can be activated on short notice. Export control enforcement is a top priority of the current Administration, so the time is now for companies to update compliance systems and personnel on the scope of the FDPR.