CLIENT ALERT · JUNE 2026

The Bosch Settlement: Five Lessons on U.S. Export Controls for Multinationals

On June 17, 2026, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) announced a $36,184,680 settlement with Robert Bosch GmbH over shipments that two of Bosch's non-U.S. subsidiaries made to Huawei between September 2020 and September 2024. On the same day, the Department of Justice's National Security Division declined to prosecute Bosch, the first declination issued under the Department's Corporate Enforcement Policy, citing the company's voluntary self-disclosure, cooperation, and remediation. Bosch separately agreed to disgorge roughly $3.6 million in profits, which BIS credited against its penalty.

BIS used its charging letter to set out, in a fair amount of detail, how a transaction between two non-U.S. companies comes within U.S. jurisdiction and how red flags can be missed inside a large, decentralized organization. DOJ used the declination to show the benefit of prompt disclosure and cooperation, even in a national security context. The value of the matter lies less in anything particular to Bosch than in how ordinary the underlying conditions are: a globally distributed manufacturer, foreign operating subsidiaries at some remove from headquarters compliance, items that appeared uncontrolled on their face, software moving alongside hardware, and a major Asian customer to keep supplied. Those are everyday operating conditions of most multinationals with manufacturing or sales exposure in China and the wider region. Five points stand out.

1. Non-U.S. subsidiaries are squarely within reach of U.S. export controls

Neither Bosch subsidiary was in the United States, and the products were manufactured abroad, yet the transactions were subject to U.S. jurisdiction. The items, MEMS sensors from Bosch Sensortec GmbH and CycurHSM automotive firmware from ETAS GmbH, fell within the Foreign Direct Product Rule (FDPR), which extends the application of U.S. export controls to certain foreign-made items produced with U.S.-origin technology, software, or equipment. Because Huawei and its affiliates are on BIS's Entity List, any item subject to the Export Administration Regulations (EAR) requires a BIS license, yet none was obtained.

The items were classified EAR99, the catch-all category for goods that are not specifically controlled. Some compliance teams treat an EAR99 classification as the end of the inquiry, and this case is a reminder that it should not be. An EAR99 item can still come under EAR controls by virtue of the FDPR, and a transaction occurring entirely outside the United States can still require U.S. authorization when the counterparty is on the Entity List. Companies with supply chains in Asia should be mindful that the FDPR's Entity List provisions reach precisely the kind of foreign-to-foreign sales to Chinese customers that a classification-only review would clear.

The practical response is to run the FDPR analysis as a distinct step, separate from product classification, and to re-run it whenever an Entity-Listed party or one of its affiliates is involved. That analysis should account for the U.S.-origin tooling, software, and technology used in foreign

production, and it should extend to EAR99 items rather than screening them out at the classification stage. A "made abroad, uncontrolled item" conclusion is better treated as a question than an answer.

2. A compliance program is measured by actions

According to the settlement materials, the potential application of the FDPR was identified at points over the period in question but did not result in the shipments being halted. That sequence, rather than the absence of a program, is what the resolution turned on. Concerns of this kind tend to arise through supplier certifications, counterparty correspondence, or internal trade-compliance review, and they emerge against a backdrop of substantial prior enforcement in this area, including the record-setting $300 million penalty in the 2023 Seagate matter for Huawei-related FDPR violations. The question in the Bosch case was not whether the information existed, but how it was routed, who assessed it, and whether the team fielding it had the facts and resources necessary to stop a shipment.

The distinction regulators draw is between an organization that escalates and resolves a warning and one that receives information suggesting a problem and does not act on it. A program that generates signals but lacks the authority, or the practical ability, to halt a transaction provides limited mitigation. A recurring structural vulnerability, present in many large organizations and not unique to any one of them, is the placement of an export-controls judgment with personnel who also carry commercial responsibility for the same transaction.

An antidote is to build escalation paths that end in a genuine stop order. Concerns raised by suppliers, customers, distributors, internal trade staff, or outside counsel should route to a person with sufficient authority to suspend a transaction, with a documented record of how such concerns were resolved.

3. Software now carries the same export-controls exposure as hardware

A meaningful portion of the Bosch case relates to software. The CycurHSM automotive firmware, not only the physical MEMS sensors, was subject to the EAR under the FDPR. A contributing factor identified in the case was the view that the FDPR reached only physical goods and not software, a misconception that is not uncommon across industries and regions.

Export controls programs were historically built around tangible goods, engineering drawings, and production equipment. As products increasingly took the form of software, items like firmware, code, cloud-enabled features, security tools, and over-the-air updates have carried the same jurisdictional exposure as hardware, and occasionally more. The exposure is especially easy to overlook where software is delivered separately from the hardware it supports, or updated remotely after sale.

A sound response would be to bring software, firmware, and licensing teams inside the export controls purview rather than treating code as outside it. Classification and FDPR analyses should cover embedded and downloadable software, over-the-air updates, and cloud functionality; engineering and product teams should understand that the medium does not change the analysis; and screening should flag software deliveries to restricted parties exactly as it flags shipments of hardware.

4. Voluntary self-disclosure changes the outcome, even on national security

DOJ's National Security Division declined to prosecute, expressly crediting Bosch's voluntary disclosure, full cooperation, remediation, and the absence of aggravating circumstances. The Assistant Attorney General for National Security framed the declination as a demonstration of the benefits available to companies that come forward early and assist fully.

This is the first declination the National Security Division has issued under the Department's Corporate Enforcement Policy. It does not mean that self-disclosure equals no costs; the company still paid a $36 million BIS penalty and disgorged its profits, not to mention legal and other advisor fees. But the case establishes that even multi-year conduct involving Huawei and the FDPR can be resolved without criminal charges if a company self-reports early on, cooperates, and remediates credibly. After a period in which national security matters seemed to sit outside the ordinary disclosure calculus, this case confirms that the calculus still applies.

The lesson is to treat the disclosure decision as a deliberate, time-sensitive analysis. When a potential FDPR or Entity List issue arises, a company should move quickly to scope it, preserve the relevant records, and weigh voluntary self-disclosure to both BIS and DOJ.

5. Export controls are a board-level item of governance

The vulnerability the Bosch matter illustrates is not the absence of a program; it is the more familiar tension between a compliance flag and commercial pressure, here the imperative to keep a significant customer supplied through a period of constrained allocation, together with the question of where in the organization the judgment is made. Those are governance and best-practices questions, and they are increasingly ones that boards are expected to oversee.

The trade compliance function should have genuine authority to halt transactions, and such authority should be insulated from the commercial line that benefits from the sale. Periodic reporting on export-controls and Entity List exposure should reach the board or its audit or risk committee; escalation should not end at a manager who has a quota; and a relevant enforcement precedent or credible warning should be routed to legal and to board-level risk oversight rather than resolved within the commercial team.

Conclusion

What should interest executives and practitioners alike in the Bosch resolution is just how ordinary the underlying conditions are. A distributed manufacturing footprint, foreign subsidiaries operating independently of headquarters compliance, items that look uncontrolled on their face, software shipped alongside hardware, and the commercial pull of a major Asian customer are everyday circumstances for a global business. Multinationals with significant Asia-facing supply chains should take note that the fact pattern is common, the exposure is significant, and the controls to manage it are worth building before they are tested.
