Paul, Weiss

2025 Year in Review

National Security

Paul, Weiss

Client Memorandum

January 23, 2026

2025 Year in Review: National Security

Key Topics

Executive Summary

In 2025, businesses faced a dynamic national security landscape marked by rapid policy shifts and far-reaching and consequential regulatory and enforcement action. The dominant trend was the expansion and creative application of existing national security regulatory tools, and the innovation of new regulatory processes to achieve national security goals. Below, we survey 2025's most consequential legal developments in national security and highlight the challenges on the horizon for 2026.

2025 at a Glance

In the past year, U.S. national security policy continued to converge with economic policy, with regulators taking more aggressive steps in line with an "all tools" approach that tightened inbound and outbound investment controls, recalibrated export controls on advanced computing and AI-related technologies, furthered the expansion of, and experimentation with tariff authorities, and paired sanctions and law-enforcement initiatives with sectoral regulators such as the Federal Communications Commission (the "FCC") to harden supply chains.

- **CFIUS recalibration and fast-track.** CFIUS advanced a broader "economic security is national security" posture, previewed a fast-track review pathway for trusted allied investors, and signaled streamlined, time-bound mitigation. The U.S. government also sharpened sectoral focus (including agriculture via the U.S. Department of Agriculture's ("USDA")

Farm Security Action Plan), increased non-notified enforcement and monitoring, and employed more assertive remedies, from a "golden share" in Nippon Steel–U.S. Steel to a presidential divestiture order in Suirui–Jupiter.

- **U.S. export controls pivot on advanced compute**. The Commerce Department rescinded the AI Diffusion Rule and shifted toward amplifying knowledge-based controls aimed at preventing diversion of advanced technologies to prohibited end uses and end users, particularly People's Republic of China ("PRC") military and intelligence actors. To close the year, several licensing decisions green-lit advanced-compute deployments in the Middle East and permitted sales of mid-tier chips to China under stringent conditions.

- **The new relevance of tariffs**. Policymakers relied on both traditional and novel statutory authorities to expand tariffs significantly throughout the year, leveraging the new duties to negotiate trade deals with multiple trading partners. While awaiting the Supreme Court's decision on the novel use of the International Emergency Economic Powers Act ("IEEPA") as authority for imposing tariffs, enforcers continue to aggressively pursue enforcement of tariff evasion, and policymakers are actively exploring new tariffs based on alternative legal authorities.

- **Sanctions recalibration and cartel terrorist designations**. In 2025, the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") and the U.S. State Department prioritized using terrorism-designation authorities against major drug cartels, designating several groups as terrorist organizations and creating broad exposure to legal risk for commercial touchpoints in affected regions. In parallel, the lifting of comprehensive sanctions on Syria, the designation two major energy companies in Russia, and cross-program actions against Iranian energy flows, particularly through trade with the PRC, reshaped business risk assessments and cross-border deal considerations. The end of 2025, into early 2026, introduced uncertainty over the future of U.S. sanctions on Venezuela's energy sector, as well as its government more generally. Our full analysis of the 2025 sanctions landscape can be found in our anti-money laundering and sanctions year-in-review publication.[1]

- **The all-tools approach: New tools in the toolbox**. New outbound investment and data security regulatory regimes took effect, and policymakers deployed new and existing sectoral regulatory regimes to harden supply chains. 2025 marked a year of increased creativity and flexibility across federal and state agencies in the pursuit of national security goals.

Where to Focus in 2026

- **Outbound investment expansion**. The National Defense Authorization Act for Fiscal Year 2026 ("2026 NDAA") established a statutory outbound investment regime that expands the existing regulatory regime's scope to include covered countries beyond China, broadens what counts as a covered transaction and who counts as a covered foreign person, adds hypersonic and quantum technologies to the list of restricted technologies, and tasks the Treasury Department with implementing notification and prohibition rules backed by potential IEEPA sanctions.

- **Prepare export control compliance programs for the Affiliates Rule**. One of 2025's most consequential export control developments was the creation of the Affiliates Rule. The rule's one-year postponement gave businesses a welcome chance to prepare for its new effective date in November 2026.

- **Tariff landscape in flux**. In the year ahead, we may see the use of new IEEPA-based measures or the leveraging of more traditional tariff-authorizing authorities, should there be a Supreme Court decision that may be unfavorable to the current IEEPA tariff regime. Renewed government scrutiny of the *de minimis* exemption coupled with an enforcement focus on preventing evasion may shift compliance costs across sectors, with heavy impacts on supply chain players.

- **Sanctions remain dynamic**. Syria's gradual re-opening, increased pressure on Russia's energy sector, and uncertainty around Venezuela-related sanctions present uncertainty going into 2026. We expect enforcement in the coming year will continue to target PRC-linked procurement networks, Iran-related energy flows, and entities OFAC considers "gatekeepers" of the U.S. financial system (i.e., investment advisors, private equity firms, other non-bank financial institutions). Expect heightened maritime monitoring—including AIS integrity and closer cargo scrutiny—particularly for businesses with higher risk of exposure to Russia, China, and Iran, in line with the heightened focus on trade-related evasion tactics.

- **White-collar enforcement of cartel terrorist designations expected**. With the anniversary of the bulk of 2025's cartel terrorist organization designations fast-approaching, we expect to see in 2026 the results of the U.S. Department of Justice's ("DOJ") prioritization of white-collar enforcement targeting cartel-linked criminal activity in prosecutions that

leverage the broad scope and long reach of a U.S. law that prohibits the provision of material support to designated terrorist organizations.

- **Operationalize DOJ Data Security Program compliance**. Enforcement of DOJ's new regulatory regime governing cross-border data transactions is expected in 2026. To prepare for more aggressive action, companies should map cross-border data flows, classify bulk "sensitive" personal and U.S. government-related data, screen counterparties in countries of concern, and stand up controls for restricted transactions amid licensing and advisory guidance gaps.

CFIUS & Outbound Investment Regulation

You Should Know

- "**Economic security is national security**." The America First Investment Policy, published in February 2025, made explicit that the Administration views these concepts as inextricably linked.[2] The Policy specified that "all necessary legal instruments, including. . . CFIUS" would be used "to restrict PRC-affiliated persons from investing in" certain sectors deemed sensitive or strategic. Throughout 2025, CFIUS did not limit itself to considering whether a company performs on U.S. government contracts or has advanced technologies with military applications, but instead more broadly evaluated the company's importance to the U.S. economy.

- **CFIUS streamlining and fast-tracking**. 2025 CFIUS reforms provided for a fast-tracked process for certain lower risk investors. Policymakers also announced streamlined mitigation procedures that move away from CFIUS's prior reliance on complex, indefinite mitigation agreements.

- **Focus on farmland**. The USDA issued a plan for CFIUS review of acquisitions of farmland. This move is consistent with CFIUS's focus on real estate and land investment by foreign actors. Six states implemented new or further restrictive foreign ownership restrictions on land, all of which included China on their respective lists of restricted countries.[3]

- **Different treatment for passive investment**. Businesses should be aware of the continued differential treatment given to passive investment, as opposed to active investment. CFIUS and the broader policy environment remain supportive of passive investment.

- **Statutory outbound investment rules**. In the 2026 NDAA, Congress enacted expansive new outbound investment restrictions. Among other things, the bill expands the list of countries of concern and adds and expands coverage to two new technologies.

CFIUS Policy Developments

- **America First Investment Policy**. The America First Investment Policy, issued in February 2025, outlined a shifting federal government approach to foreign investment.[4] The new approach shifts the focus of CFIUS review from case-by-case mitigation toward a more categorical restriction of capital investments into sensitive sectors from adversarial countries, along with the implementation of more concrete and time-bound mitigation agreements.

- **Fast-track process**. The Policy proposes a streamlined, "fast track" review of investments from "allied and partner sources" in order to facilitate the flow of friendly capital into the country. This process will expand the current, narrow "excepted investor" concept, which serves only to except those investors from CFIUS review of certain otherwise mandatory filings. The Policy appears to be calling for the creation of a pseudo- "Known Investor" program for certain repeat foreign investors. Details on the new process have been limited, with the U.S. Department of the Treasury announcing in May 2025 that it intends to launch a pilot program for the process.[5]

- **Streamlining mitigation**. Going forward, CFIUS "will cease the use of overly bureaucratic, complex, and open-ended 'mitigation' agreements" in favor of agreements that will "consist of concrete actions that companies can complete within a specific time frame, rather than perpetual and expensive compliance obligations." This comes as welcome news following an uptick in CFIUS mitigation agreements since the implementation of the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA").[6] In 2022 and 2023, nearly one quarter of all notice filings reviewed by the Committee resulted in mitigation, and by the end of 2024, the Committee was monitoring 242 active agreements. In 2024, however, CFIUS mitigated only about 9% of notices and terminated 25 agreements—signaling a moderation in mitigation practices. This shift on mitigation may also be bolstered by the implementation of other regulatory authorities to address potential foreign investment risks, such as DOJ's Data Security Program.[7]

- **Welcoming passive investment**. U.S. policymakers continue to welcome genuinely passive foreign minority investments, with CFIUS's rules excluding from "covered control transactions" minority investments "solely for the purpose of passive investment" and treating standard minority-shareholder protections as non-controlling. However, even non-controlling investments in businesses involving "critical technologies," "covered investment critical infrastructure," or "sensitive personal data" can still be "covered investments" if the foreign investor gains access to material non-public technical information, board rights, or involvement in substantive decision-making.

- **USDA Farm Security Action Plan**. In 2025, the USDA issued the National Farm Security Action Plan, which takes steps to improve how existing authorities are used with respect to foreign investments in U.S. agriculture. First, the plan sets out measures to ensure better compliance with, and enforcement of, the Agricultural Foreign Investment Disclosure Act of 1978 ("AFIDA"), which requires foreign individuals and entities to report their holdings of U.S. farmland. Second, the plan takes steps to ensure that USDA is more integrated into the CFIUS process and that CFIUS is using the full extent of its authorities over real estate transactions. Going forward, we expect that CFIUS will engage in more significant scrutiny of agricultural investments.

CFIUS Case Reviews

2024 Annual Report Overview

- **Reduction in CFIUS filings for 2024**. The number of filings was down slightly from 2023, although 2024 saw a slight uptick in the number of declarations compared to the prior year. Both 2023 and 2024, in turn, fell well below the 440 total filings of 2022, which remains the highest annual total for CFIUS. Given the general alignment of CFIUS filings to cross-border M&A activity, we expect the number of filings in 2025 to be roughly similar to 2024, if not somewhat lower. With several years of experience post-FIRRMA, it appears that CFIUS filings have found their level with approximately 300–400 filings per year.

- **Decline in filings related to sensitive technologies**. Although overall filing volumes slowed down modestly, activity shifted meaningfully away from industries that present classic national security touchpoints. The data for 2024 show sharp contractions in filings associated with semiconductors and related electronics, scientific research and development, and aerospace.[8] Given the ongoing focus on the U.S. domestic supply chain security and advanced manufacturing, particularly in chips and electronics, this could be a signal that foreign investors are now more likely either to structure for passivity or to defer transactions altogether rather than invite scrutiny through a CFIUS filing.

- **Bifurcation between trusted allies and higher-risk jurisdictions**. Filings and clearances have increasingly bifurcated between trusted allies—who saw record-high declaration clearance rates—and higher-risk jurisdictions, where parties gravitated toward full notices, longer timelines and, in some cases, deal abandonment. Looking ahead, this pattern is likely to endure. The Committee's willingness to police non-notified transactions and its emphasis on compliance create strong incentives for parties to avoid voluntary notices in sensitive industries unless a filing is mandatory or otherwise advantageous. At the same time, the Committee's continued focus on advanced computing, artificial intelligence, quantum, and biotechnology suggests that it views a wide range of technologies as sensitive technologies.

Enforcement and Compliance

- **Expanded enforcement activity**. As contemplated by its 2025 budget justification, CFIUS has continued to enhance its enforcement posture to include non-notified transactions, mitigation monitoring, and international engagement. This trend is likely to continue, and companies should anticipate increased outreach on non-notified deals, tighter post-closing oversight, and expanded international coordination.

- **Golden share mitigation agreements**. CFIUS continued to tailor its use of mitigation agreements to risks specific to transactions and investors. Notably, 2025 saw the use of a "golden share," whereby the United States becomes a shareholder in a company, to resolve the government's national security concerns with Nippon Steel's acquisition of U.S. Steel.[9] Although CFIUS has a long-standing practice of requiring companies to engage in governance-related mitigation efforts, the golden share mitigation in Nippon Steel demonstrated the use of national security tools to allow the government to engage more directly in the operations of a mitigated business.

- **Requiring divestments**. Enforcement actions pursued in 2025 demonstrate the Committee's willingness to divest foreign owners when mitigation cannot sufficiently address residual risk. For example, in July 2025, the government ordered Suirui to divest all interests in Jupiter Systems within 120 days, barred access by Suirui personnel to Jupiter's non-public code and systems pending divestment, required weekly compliance certifications, and subjected any buyer to a 30-day CFIUS

non-objection period.[10] Treasury stated that CFIUS identified risks of compromising products used in military and critical-infrastructure environments. The Suirui order underscores the Committee's readiness to mandate post-closing divestitures where mitigation cannot resolve national security concerns.

- **HieFo divestment order**. On January 2, 2026, an Executive Order required HieFo, a Delaware corporation controlled by PRC citizens, to divest all interests it acquired from EMCORE Corporation, including its digital chips and wafer design, fabrication, and processing businesses. This followed a finding of "credible evidence" that the transaction threatens U.S. national security. The directive—an uncommon use of divestment—underscores that CFIUS will pursue enforcement even in unfiled, smaller-value deals and that divestment remains a remedial option when mitigation cannot eliminate risk. The E.O. also highlights two clear themes: a continuing focus on advanced semiconductor capabilities and an all-tools approach to protecting U.S. technological advantage.

Outbound Investment Regulation

- **Outbound Investment Security Program**. The U.S. government took its first significant effort to restrict outbound foreign direct investment with the effectiveness of regulations, issued under the International Emergency Economic Powers Act ("IEEPA"), implementing the Outbound Investment Security Program ("OISP"), in January 2025.[11] For the first time, the OISP imposed categorical prohibitions and notification requirements on certain U.S. person investments in entities directly or indirectly controlled by Chinese nationals or entities that are engaged in research, development or manufacturing involving any of three categories of national security technologies or products: semiconductors and microelectronics, certain AI systems, and quantum information technologies.

- **COINS Act becomes law**. The Comprehensive Outbound Investment National Security Act of 2025 (the "COINS Act") was arguably the most significant development in the field in 2025. It became law as a part of the 2026 NDAA at the end of 2025.[12] The new provisions have the potential to impact a wide range of investment activity, particularly for private equity investment firms.

  - **High level takeaways**. The COINS Act establishes a new statutory regime to regulate outbound investment that codifies and expands the existing outbound investment security regime. It does so by ratifying the President's existing authority under IEEPA to regulate foreign investment, amending the Defense Production Act ("DPA") and creating new statutory authorities.[13] Among other important changes, the COINS Act broadens outbound investment restrictions from the previous focus on China, adding five additional countries of concern.

  - **Sanctions authority**. In addition, the COINS Act ratifies the existing OISP regulatory regime by explicitly confirming the president's authority under IEEPA to impose sanctions on certain covered persons to prevent U.S. persons from investing in or purchasing the debt of the covered person. The Act provides that the president may exercise this authority "to the extent necessary to prohibit any United States person from investing in or purchasing significant amounts of equity or debt instruments of a foreign person that is determined to be a covered person."

  - **Delegation to Treasury**. The COINS Act gives the Secretary of the Treasury Department the authority to regulate a range of outbound transactions. First, the statute requires the Treasury Department to promulgate rules to require that U.S. persons who engage in certain transactions submit a written notification of the transaction to the Secretary of the Treasury after the completion date of the transaction.[14] Second, subject to certain exceptions, the COINS Act provides that the Secretary may prohibit United States persons and their controlled foreign entities from "knowingly engaging in a covered national security transaction in any prohibited technology."[15]

  - **Exemptions**. The Act also creates a variety of exemptions and instructs the Treasury Department to set up processes by which regulated entities can gain additional clarity about the scope of the restrictions.[16]

  - **Scope**. The COINS Act includes a broad definition of "covered national security transaction."[17] It encompasses the acquisition of equity interests, the provision of certain loans or financing agreements, the entrance into joint ventures, the acquisition of real estate, and limited partner investments. The statute also defines "covered national security transaction" to include "knowingly directing prohibited transaction or notifiable transactions," further broadening the scope of potential exposure for U.S. persons.[18]

- **Changes from Outbound Investment Regulations**. Among other things, the major changes to OISP's existing rules relate to the definitions of "covered foreign person," "country of concern," and restricted technologies.

- **Directing liability**. The Act expands on the "knowingly directing" provision in the existing OISP regulations, adding coverage for those who "knowingly direct[] notifiable transactions.[19]

- **Countries of concern**. Under the COINS Act, a "covered national security transaction" must involve a "covered foreign person," or a "country of concern." The COINS Act expands the list of countries of concern in the OISP beyond China, to include Cuba, Iran, the Democratic People's Republic of Korea, Russia, and Nicolas Maduro-controlled Venezuela.[20]

- **New restricted and prohibited technologies**. The COINS Act adds two new restricted and prohibited technologies: hypersonic systems and quantum information technologies.[21]

Export Controls

Major Export Control Policy Developments

2025 was packed with significant export control policy changes focused on restrictions and controls applicable to exports to China, and particularly on exports relating to AI and advanced semiconductor technology. Changes included the rollback of major policy initiatives announced earlier in 2025 and new policies to tighten controls on exports to China.

You Should Know

- **Focus on integrated circuits**. Recent licensing decisions appear to reflect an effort by U.S. policymakers to maintain American dominance in the market for advanced integrated circuits ("IC"s) that are used to power the training and development of frontier AI models, while also limiting the competitiveness of China's domestically produced and less capable ICs. The U.S. strategy focuses on blunting the market forces that have fueled efforts by China's chipmakers to develop domestic capability to produce cutting-edge advanced ICs that can compete with leading American-made chips.

- **New legislation and continued debate**. In December 2025, the Chair of the House Foreign Affairs Committee introduced a bill—the AI OVERWATCH Act—seeking to grant Congress the authority to block sales of advanced ICs more capable than Nvidia's H20 chip in a manner similar to Congress's review of foreign military sales.[22] The dynamic export control policy debate around advanced ICs appears likely to intensify in 2026, and companies with investments in this sector should continue to monitor these developments closely.

- **New Affiliates Rule expected in November 2026**. When the pause on the BIS Affiliates Rule ends in November 2026, the Rule will usher in significant new Export Administration Regulations ("EAR")compliance requirements for exporters, with some estimates suggesting that an additional 20,000 unlisted entities will become subject to Entity List export restrictions and licensing requirements.[23]

Major Developments

- **Rescission of the AI Diffusion Framework**. In May 2025, the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") announced it would rescind and not enforce the AI Diffusion Interim Final Rule just two days before it was set to take effect. The original AI Diffusion Framework, announced in January 2025, had attempted to establish a global, tiered licensing system for advanced computing ICs, related servers, and closed-weight AI model weights.[24] In announcing the rescission, policymakers expressed concerns that the AI Diffusion Framework would have prevented U.S. companies from exporting America's AI technology stack to trusted U.S. allies, and signaled a new approach to restricting China's access to advanced ICs and computing power.

- **Amplification of knowledge-based catch-all controls for advanced ICs**. U.S. policymakers' efforts to restrict the diffusion of advanced-computing to China did not end with the AI Diffusion Rule. Instead, regulatory action shifted to amplifying existing knowledge-based export controls—export restrictions that are triggered by an exporter's knowledge of an intended prohibited end user or end use of the exported item—that restrict exports of advanced ICs and AI compute to weapons of mass destruction-related end uses and military or military-intelligence end users and end uses. As it rescinded the AI Diffusion Rule in May 2025, BIS simultaneously issued a trio of complementary documents—a policy statement,[25] EAR General Prohibition 10 ("GP10") guidance,[26] and industry red-flag/due-diligence guidance[27]—sharpening the use of the EAR's existing knowledge-based controls to prevent the diversion of AI-related technologies to primarily Chinese military end users and end uses.[28]

  - **Highlighting prohibited end-use and end-user risks**. BIS's Policy Statement flagged the risk that exports of advanced ICs could be used to train an AI model that would be used for a prohibited military-intelligence end use or end

user. The Policy Statement also warned of consequences for those exports: enforcement action and the addition of foreign parties to the Entity List. The policy statement effectively increased the exposure of advanced IC market participants to enforcement and Entity List risk.

- **Targeting China-made chips**. BIS's GP10 Guidance also warned exporters of the "high probability" that China's domestically produced advanced ICs had been developed and produced without required licenses from BIS in violation of the EAR, and specifically named certain China-made chips (e.g., select Huawei Ascend ICs) as presumptively subject to export restrictions for that reason. BIS warned parties engaging in transactions involving China's domestically produced chips that those transactions would risk violating the EAR's GP10, which prohibits commercial activities that involve an item exported or to be exported with knowledge that a violation of the EAR has occurred, is about to occur, or is intended to occur in connection with the item. The guidance increased enforcement risk for companies that purchase or use China-made advanced ICs.

- **New red flags, more diligence is due**. For advanced ICs, BIS's Industry Guidance outlined a non-exhaustive list of 11 additional red flags and accompanying diligence requirements that those red flags would trigger. The guidance had the effect of significantly expanding the diligence expectations for advanced IC exports, and the accompanying enforcement risk for exporters who fail to satisfy them.

- **Use of expansive "Is Informed" letters to restrict semiconductor technology exports to China**. In May 2025, BIS sent "Is Informed" letters to the three largest developers of electronic design automation ("EDA") technology used in the production of advanced ICs. While BIS has traditionally issued "Is Informed" letters to impose targeted licensing requirements on a specific exporter's transfers to a specific purchaser or consignee, the May 2025 letters imposed licensing requirements broadly applicable to all transfers of EDA software and technology when a party to the transaction was located in China or was a Chinese military end user wherever located.[29] Although BIS later rescinded the licensing requirements imposed by the letters in July 2025, the novel and expansive use of the "Is Informed" process indicates BIS's willingness to chart new regulatory territory as it moves aggressively to restrict China's access to American semiconductor technologies.[30]

- **New Affiliates Rule—Coming November 2026**. In October 2025, BIS announced a long-expected "Expansion of End-User Controls to Cover Affiliates of Certain Listed Entities" (the "Affiliates Rule"). The Affiliates Rule dramatically expanded the scope of end-user licensing requirements imposed by the Entity List by including certain foreign affiliates that are 50% or more owned, directly or indirectly, by listed parties—a significant policy change that mirrors similar provisions applicable to economic sanctions programs administered by the Treasury Department.[31] A month later, on November 1, the Administration announced a one-year pause on the implementation of the Affiliates Rule as part of a diplomatic agreement with China, giving companies a full year to prepare for the new rule.[32]

- **Novel application of the Entity List to foreign subsidiaries of U.S. companies**. In October 2025, BIS made novel use of the Entity List, when BIS for the first time added to the Entity List the foreign subsidiary of a U.S. public company. In listing Arrow China Electronics Trade Co. Ltd., BIS accused the company of facilitating the procurement of U.S.-origin electronic components found in unmanned aircraft systems ("UAS") operated by Iranian proxies in the Middle East.[33] In November 2025, only a month later, BIS removed Arrow China and its aliases from the Entity List after the company committed to strengthening its export compliance program.[34] The precedent set by the Arrow China listing decision, however, makes clear that foreign subsidiaries of U.S. companies are now exposed to Entity List risk.

- **Introduction and expansion of ICTS controls**. In 2025, BIS exercised its authorities to regulate Information and Communication Technology and Services ("ICTS") transactions to impose controls on the import of connected vehicles. Issued in January 2025 and effective beginning in March 2025, BIS's Office of Information and Communications Technology and Services ("OICTS") issued a final rule—"Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles" (the "Connected Vehicles Rule")—banning the sale or import of connected vehicles containing certain hardware or software linked to China or Russia, regardless of manufacturing origin.[35] The Connected Vehicles Rule currently applies only to passenger vehicles, but in September 2025, BIS announced initial plans to extend similar controls to Chinese-made trucks and drones through interim final rules,[36] later narrowing the scope of those controls by withdrawing the drone proposal on January 8, 2026, after the FCC effectively banned the importation of most foreign-made drones by adding them to its Covered List in a major regulatory action we discuss below.[37]

- **Rollback of open-ended VEU export authorizations**. Beginning in 2007, BIS's Validated End-User ("VEU") program facilitated exports of high-technology items from the United States to pre-approved companies in China and India, allowing shipments under a general authorization that would otherwise require individual export licenses.[38] In 2024, BIS extended the VEU program to cover overseas data centers, aiming to further global AI development in a way that "minimize[d] risk to national security."[39] In September 2025, however, BIS ended the VEU program, describing it as a regulatory loophole that put U.S. companies at a competitive disadvantage, and revoked VEU authorizations for the Chinese facilities of several leading semiconductor manufacturers in favor of an annual license renewal process.[40]

- **Licensing policy trends**. Licensing decisions also served as a major instrument of export control and foreign policymaking in 2025.

  - **Middle-East AI chip deployments**. In November 2025, BIS and other agencies approved export licenses for high-profile advanced IC deployments in the Middle East. This included cloud and data-center initiatives by major U.S. firms, as well as Nvidia's advanced Blackwell chips to be exported to the United Arab Emirates and the Kingdom of Saudi Arabia subject to strict security, reporting, diligence, and end-user validation requirements.[41]

  - **China chip licenses**. In December 2025, the government announced that Nvidia would be authorized to sell its advanced H200 AI chips to China, subject to the requirements that the chips be inspected in the United States before being shipped to Chinese customers, that the U.S. government receive a 25% share of sales, and that sales be restricted to U.S. government-approved customers. The H200 chips are less capable than the Blackwell chips that were authorized for export to U.S. allies in the Middle East in November 2025, but far more capable than China's domestically produced advanced ICs and the "downgraded" H20 chips that Nvidia had previously been authorized to export to China.[42]

DOJ and BIS Export Control Enforcement Developments

Export control enforcement—civil and criminal—was a priority for DOJ's National Security Division ("NSD") and BIS in 2025, with unlawful exports of advanced ICs and related technology to Chinese entities in violation of Entity List restrictions driving individual and corporate enforcement actions.

You Should Know

- **Focus on ICs**. Another 2025 enforcement trend likely to continue in 2026 was the focus on enforcing controls on the exports of advanced ICs and related technologies. These 2025 efforts propelled a major corporate resolution with a large semiconductor technology company and criminal charges against several individuals for attempting to smuggle advanced ICs to China.

- **Self-disclosure incentives remain**. NSD has continued to emphasize and incentivize corporate voluntary self-disclosure ("VSD"). In 2025, prosecutors approved favorable resolutions of export control enforcement actions where companies voluntarily disclosed wrongdoing and fully cooperated with DOJ throughout the investigation and remediation.

- **Enhanced due diligence**. Companies can act now to decrease the risk of facilitating unlawful exports by implementing enhanced customer due diligence where red flags are present, such as orders from and payments by new customers that lack an established industry presence or track record for the purchase and use of advanced ICs.

Enforcement Highlights

- **Corporate enforcement focus on the semiconductor industry**. As further evidence of the semiconductor industry's strategic significance to national security, semiconductor industry export control enforcement was a top priority for NSD and BIS in 2025.

  - **Alpha & Omega Semiconductor**. In June 2025, BIS announced a civil settlement with Alpha and Omega Semiconductor Limited ("AOS") for 15 EAR violations involving unauthorized exports of EAR99 items to Huawei Technologies Co., Ltd. Critically, after Huawei was placed on the Entity List, AOS continued shipments based on incomplete legal advice, violating U.S. export control laws. BIS imposed a civil penalty of $4,250,000, along with denial of export privileges for one year if payment terms are not met.[43]

  - **Cadence Design Systems**. In July 2025, Cadence Design Systems, Inc. ("Cadence") reached criminal and civil resolutions with NSD and BIS over unlawful exports of EDA hardware, software, and semiconductor-design technology through third parties to a Chinese military-linked university on the Entity List. Cadence pleaded guilty to conspiracy to

violate the export control laws, agreed to pay over $140 million in penalties, and accepted multi-year probation with compliance reporting requirements. NSD credited Cadence's cooperation and remediation, while noting the national security harm caused by the offense and that the company had not self-disclosed the misconduct.[44]

- **Corporate criminal declinations incentivize self-disclosures of national security offenses**. Continuing a trend begun in 2024, and consistent with broader corporate enforcement policy statements by DOJ leadership in 2025, companies that made VSDs of criminal violations of export control and related national security laws to NSD, fully cooperated against culpable employees and executives, and remediated the misconduct continued to receive favorable treatment from NSD in 2025, with resolutions often coordinated with BIS and OFAC. Each of the VSDs that resulted in declinations by NSD led directly to the successful prosecution of culpable employees of the disclosing entity.
  - **Universities Space Research Association ("USRA") Declination**. In April 2025, NSD announced it was declining the prosecution of USRA after it self-disclosed an employee's unlawful export of U.S. flight control/optimization software to a Chinese university on the Entity List. NSD's announcement highlighted USRA's rapid self-disclosure, proactive cooperation, and extensive remediation. USRA's cooperation contributed to the successful prosecution of its former employee, Jonathan Soong, who pleaded guilty to violating U.S. export control laws and was sentenced to 20 months of imprisonment.[45]
  - **Private equity declination under DOJ M&A Safe Harbor Policy**. In June 2025, NSD announced DOJ's first-ever declination of a prosecution of an acquiring entity under the DOJ M&A Safe Harbor Policy, which was rolled out in 2024. White Deer Management, a private equity firm, self-disclosed to NSD sanctions and export control violations that it uncovered at its newly acquired portfolio company, Unicat Catalyst Technologies, not long after the acquisition. The VSD led to a criminal investigation that resulted in the CEO and founder of the company pleading guilty to several offenses. The portfolio company also benefitted, with Unicat entering into a non-prosecution agreement, pursuant to which it paid criminal forfeiture. The criminal resolution was coordinated with OFAC and BIS civil settlements that credited the forfeiture payment against the civil penalties. NSD cited White Deer's prompt disclosure, proactive cooperation, and remediation as grounds for the declination.[46]
  - **MilliporeSigma's VSD results in successful prosecutions of individuals**. In September 2025, Gregory Muñoz, a MilliporeSigma salesperson, was sentenced to 18 months in prison for his role in a scheme to fraudulently obtain and export laboratory research products to China. DOJ credited MilliporeSigma's rapid VSD to NSD and proactive cooperation for the successful prosecution of Muñoz and multiple co-conspirators.[47] In 2024, MilliporeSigma obtained a declination from NSD, the first discretionary declination under NSD's VSD policy.[48]
- **Criminal enforcement of advanced IC export control evasion schemes**. In the second half of 2025, NSD and other DOJ components announced criminal prosecutions of individuals engaged in schemes to illegally export advanced ICs to China, resulting in arrests, guilty pleas, and seizures of advanced ICs. The fact patterns revealed in public charging documents highlight common tactics used by criminal networks to evade export controls and carry compliance lessons for both semiconductor industry participants and third-party service providers that risk GP10 liability for facilitating the purchase or unlawful export of advanced ICs.[49] Key red flags include:
  - **The use of front companies without extensive commercial experience in advanced IC deployments**. Evasion networks used new or repurposed domestic shell companies with incongruent business lines to purchase from U.S. manufacturers large volumes of servers and advanced ICs in order to mask their true intent to unlawfully export them to end users in China.
  - **The use of transshipment hubs**. Evasion networks routed shipments through third countries (e.g., Canada, Malaysia, Singapore, and Thailand) and transshipment intermediaries and funded purchases by U.S. front companies using funds transfers from Chinese entities to conceal the intended destination of the advanced ICs in China.
  - **Mislabeling and misdirection**. Evasion networks falsified end user information, prepared false invoices and descriptions, misrepresented shipment paperwork, and created "fake contracts" to frustrate screening.
  - **Drop-ship or "bill-to/ship-to" anomalies**. Some evasion networks purchased advanced ICs for delivery to freight forwarding companies, while the payments originated from Chinese entities.

Tariffs

In 2025, the U.S. government deployed an array of trade policy tools that contributed to progress in several reciprocal trade negotiations with trading partners.

You Should Know

- **Tariffs as a key policy tool**. Regulators have imposed tariffs in efforts to combat cross-border migration and the fentanyl trade, reshore American manufacturing to counterbalance trade deficits, bolster national security, and punish foreign governments for judicial actions or other unfavorable behavior.
- **Increased focus on trade fraud**. Federal authorities have prioritized enforcement against so-called origin washing practices and sophisticated transshipment schemes designed to bypass trade restrictions. This shift increasingly leverages the False Claims Act and multi-agency investigations to treat customs evasion as a direct threat to U.S. national security.
- **Supreme Court review**. The use of IEEPA to impose tariffs made it to the Supreme Court at the end of 2025. Should the Supreme Court strike down the use of IEEPA to impose tariffs, or significantly limit the scope of such authority in 2026, importers can be expected to sue to protect their rights to obtain refunds of duties paid.
- **New tariffs on the horizon**. The Commerce Department initiated several trade investigations under Section 232 of the Trade Expansion Act of 1962 ("Section 232") in 2025, and as those investigations conclude in coming months, more Section 232 tariffs can be expected across industries. An adverse ruling in the Supreme Court on the government's IEEPA tariffs may also prompt policymakers to impose tariffs under other, more established authorities.[50]

Novel Use of IEEPA

The cornerstone of tariff policy in 2025 was the novel use of IEEPA to impose tariffs. IEEPA authorizes the president to address any "unusual and extraordinary" external threat to the "national security, foreign policy, or economy of the United States, if the president declares a national emergency with respect to such threat." Although presidents have previously relied on IEEPA to impose sanctions (i.e., comprehensive embargoes and blocking sanctions), in 2025, the Administration took the position that IEEPA's authorization for the president to "regulate" importation also encompasses the authority to tariff those imports.

- **Reciprocal and fentanyl tariffs**. The most significant category of IEEPA tariffs was the "reciprocal" tariffs imposed in April 2025. These tariffs apply to most imports from almost all U.S. trading partners. The tariffs imposed on imports from Canada, Mexico, and China to address trade in fentanyl also were predicated on IEEPA and have had a significant impact on the cross-border movements of goods.
- **Secondary tariffs**. Another category is IEEPA-based non-reciprocal or "secondary" tariffs, which can be imposed on countries that trade with a country subject to U.S. sanctions. This is the first time that tariffs have been employed in such fashion.

Expanded Use of Section 232

Section 232 authorizes the president to charge duties on certain imports while the U.S. Department of Commerce investigates whether those products are being imported in such quantities and under such circumstances that they pose a national security risk. In 2025, Section 232 was used to impose tariffs on various imports such as steel, aluminum, and certain derivative goods; copper and copper derivative products; trucks, buses, automobiles, and automobile parts; and timber, lumber, and upholstered wooden furniture and kitchen cabinets, the latter three of which have subsequently been postponed. The U.S. Department of Commerce is also actively investigating the national security effects of other imports such as pharmaceuticals (reportedly excluding generic pharmaceuticals), semiconductors, wind turbines, medical consumables and equipment, robotics and industrial machinery, and unmanned aircraft systems.[51] This has already resulted in the imposition of tariffs on certain semiconductors, effective on January 14, 2026.[52]

Elimination of the *De Minimis* Exception

At the end of August 2025, the Administration ended the "de minimis" tariff exemption, under which foreign goods valued under $800 could enter the United States duty- and tax-free, for all countries.[53] Now, many low-cost goods are subject to tariffs, with the Administration already collecting over $1 billion in tariff revenues on those goods.[54] Many international postal and shipping services throughout Asia and Europe have temporarily halted shipments to the United States while they reorient their paperwork and payment processes.[55] As of October 2025, postal traffic to the United States was 70% lower than it had been before the exception was eliminated.[56]

Blunted Impact of Tariffs

The economic impact of the tariffs has not been as severe as economists initially predicted, due in part to recent trade deals and tariff exemptions. For example:

- **Originating goods**. The IEEPA-based tariffs targeting imports from Canada and Mexico are not currently being applied to goods that are treated as "originating" goods under the rules of origin set forth in the United States-Canada-Mexico Agreement.
- **Section 232**. In addition, the reciprocal tariffs initially imposed in April 2025 are not being applied to imports of products, such as pharmaceuticals and semiconductors, that are the subject of separate pending Section 232 investigations. A reprieve was also recently announced for certain agricultural commodities, such as bananas, beef, and coffee and tea, because domestic growth and production of these commodities cannot meet demand.[57]
- **Trade deal**. Furthermore, U.S. trade deals with the European Union, China, Japan, South Korea, Cambodia, Malaysia, Thailand, and Vietnam, among others, resulted in substantially lowered or reversed tariffs and reciprocal tariffs. For example, the EU agreed to a capped 15% reciprocal tariff.[58]
- **Market changes**. Other factors contributing to the tariffs' blunted impact include importers switching to domestic producers and countries subject to lower tariffs and U.S. companies importing more products earlier in the year in anticipation of tariffs.

Pending Supreme Court Litigation

In *Trump* v. *V.O.S. Selections* and *Learning Resources* v. *Trump*, the Supreme Court is considering whether IEEPA authorizes the president to issue tariffs under recent Executive Orders—specifically, tariffs on China, Mexico, and Canada tied to fentanyl trafficking and illegal immigration, as well as reciprocal tariffs. Before the Court are two questions: (1) whether IEEPA authorizes such tariffs and (2) if so, whether the statute violates the non-delegation doctrine by usurping Congress' Article I taxing powers. A decision is expected in early 2026.

Even if the Court determines that IEEPA does not authorize the imposition of tariffs, other statutory authorities could support future tariffs. In addition to Section 232, Sections 122 and 301 of the Trade Act of 1974 and Section 338 of the Tariff Act of 1930 all provide more limited authorities to impose tariffs.[59]

New Law Enforcement Focus on Trade Fraud

In 2025, federal prosecutors and law enforcement agencies concentrated resources on tariff evasion and other forms of trade fraud, producing a spate of significant civil and criminal enforcement actions in an enforcement trend that is likely to accelerate in 2026.

- **CBP list**. In July 2025, the Administration directed U.S. Customs and Border Protection ("CBP") and the U.S. Department of Commerce to publish a list of facilities used in tariff circumvention schemes.[60]
- **DOJ Task Force**. In August 2025, DOJ created a "Trade Fraud Task Force," consisting of DOJ's Civil and Criminal Divisions and the Department of Homeland Security, to "aggressively pursue enforcement actions against any parties who seek to evade tariffs and other duties."[61] As part of this effort, DOJ restructured the Criminal Division Fraud Section's specialized Market Integrity and Major Fraud Unit to make tariff evasion and trade fraud a higher priority, renaming the group the Market, Government, and Consumer Fraud Unit.[62]
- **New incentives**. In addition to these structural changes, DOJ implemented new incentives to encourage the private sector's cooperation in furthering these enforcement priorities, specifically encouraging whistleblowers to come forward to "help identify fraud schemes involving an array of imported products."[63]

Among other notable actions:[64]

- In March 2025, an importer and its two owners paid $8.1 million to settle a False Claims Act ("FCA") dispute related to knowing customs evasion. The FCA claims had alleged that the company caused false information to be submitted to the government regarding imports of wood flooring. This highlights the value of the FCA, which contains a whistleblower provision, in enforcing trade-related misconduct within businesses.[65]

- In August 2025, CBP announced a $400 million duty evasion enforcement action focused on the transshipment of Chinese-made goods through Southeast Asia to disguise their country of origin and evade U.S. import duties on Chinese goods.[66]
- In November 2025, multiple members of an Indonesian jewelry company were charged with a "large-scale duty and tariff evasion scheme," stemming from conduct allegedly intended to evade over $86 million in duties and tariffs on jewelry products imported into the United States.[67]
- In December 2025, DOJ announced two separate enforcement actions in the trade fraud space—one resulting in a North Carolina-based distributor paying a $54.4 million fine for violations of the FCA related to knowingly failing "to pay duties owed on tungsten carbide products imported from . . . China," while the other dealt with a plastic resin distributor's voluntarily disclosed scheme of falsifying Country of Origin declarations in order to avoid duties on goods of Chinese origin, which resulted in a negotiated financial resolution and a guilty plea from the distributor's Chief Operating Officer.[68]

More aggressive audits of duties are expected to continue into 2026 as the federal government continues to prioritize trade fraud enforcement.

Transactional Implications of Economic Sanctions

In 2025, OFAC continued to impose and adjust sanctions affecting transactions with Russia, Syria, and China, including Chinese trade with links to Iran. Key developments are highlighted below, while our full analysis of the 2025 sanctions landscape and expectations for the year ahead can be found within our *Economic Sanctions and Anti-Money Laundering Developments: 2025 Year in Review*.[69]

You Should Know

- **Continued focus on Russia**. Businesses transacting with Russian entities must continue to remain vigilant about sanctions risk. In 2025, OFAC added more Russian oil companies to its sanctions list and imposed major penalties on two U.S. private investment firms for engaging in transactions with a sanctioned oligarch.
- **Syria shift**. 2025 marked a shift in the relationship between the U.S. and Syria and saw a corresponding lifting of comprehensive Syria sanctions with the repeal of the executive order providing for such sanctions. Both Congress and sanctions regulators took steps to open Syria to U.S. businesses, although some challenges remain for business re-entry into Syria.
- **China risk**. Agencies continue to target China-related misconduct through both the Hong Kong Autonomy Act and non-China specific sanctions programs. Enforcement risk is particularly high where transactions with Chinese entities implicate Iran-related sanctions, and in the chemical, technology, and maritime sectors.

Russia-Related Sanctions and Compliance Challenges

OFAC continues to emphasize the importance of maintaining risk-based sanctions compliance programs to mitigate exposure to Russia-related activities, including dealings with persons blocked under E.O. 14024 and those operating in the technology, defense, construction, aerospace, and manufacturing sectors.

- **New sanctions against Russian oil companies**. In October 2025, OFAC added Russian oil companies Rosneft and Lukoil to the Specially Designated National ("SDN") List. OFAC warned of potential secondary sanctions risks for foreign financial institutions and non-U.S. persons engaging in significant transactions with SDNs.[70]
- **Continued enforcement: GVA Capital and IPI Partners**. In June 2025, OFAC imposed a $216 million penalty on Silicon Valley venture capital firm GVA Capital for knowingly managing investments for an SDN, Russian oligarch Suleiman Kerimov.[71] And in December 2025, OFAC settled for $11.5 million with private equity firm IPI Partners for accepting investments from entities the firm should have known were controlled by Kerimov.[72]
- **Exit taxes**. Russia mandates a minimum contribution or "exit tax" for foreign companies divesting assets, typically at or above 35 percent of the transaction value with reports of potential increases to the amount. OFAC does not consider this exit tax to be "ordinarily incident and necessary to" operations in Russia; thus, U.S. persons making such payments may require a specific OFAC license. These "taxes" affect deal economics of transactions involving Russian assets, accelerate the need for earlier cash outflows, and increase documentation burdens. In 2023, companies paid $1.2 billion in exit taxes, and in 2024, another $1.5 billion.

- **Licensing bottlenecks**. Foreign companies face protracted and uncertain exit timelines due to regulatory approvals and licensing bottlenecks. Because exits depend on Russian clearances, closing timelines can be delayed.

Syria-Related Developments

The United States, European Union, and United Kingdom have lifted comprehensive sanctions targeting Syria, creating opportunities to re-engage, subject to certain limitations and preexisting contractual commitments. Companies considering re-entry into Syria should evaluate residual U.S. sanction risks, the adequacy of their screening and export control compliance, and existing contractual restrictions on Syria-related activity.

- **Lifting comprehensive Syria sanctions**. In May 2025, OFAC issued GL 25, easing long-standing sanctions that had restricted U.S.-nexus transactions involving persons or entities located in Syria. Then, in June 2025, the United States repealed Syria sanctions. The U.S. Department of State issued a waiver that temporarily removed the risk of "secondary sanctions" from non-U.S. persons engaging in transactions with Syria. This relief allows renewed engagement with Syrian counterparties but does not unblock previously frozen property. The 2026 NDAA added additional Syria sanctions relief by repealing the Syria Civilian Protection Act of 2019, a secondary sanctions regime that had imposed sanctions on foreign persons engaged in certain transactions linked to the Assad regime.[73]

China-Related Sanctions and Compliance Considerations

OFAC used non-proliferation and Iran-related authorities to target China-based actors involved in illicit procurement of oil and Iranian energy flows. The actions signaled increased exposure for supply chains in chemicals, electronics, and maritime trade.

- **Procurement networks and brokers**. In May 2025, OFAC designated Hong Kong- and China-based firms and intermediaries for supplying dual-use materials to Iran's defense and UAV programs, imposing full blocking and, in some cases, adding secondary-sanctions exposure.[74] In October 2025, OFAC added PRC nationals tied to WMD/missile and UAV procurement networks, highlighting a focus on individual brokers and logistics intermediaries.[75]

- **Iran energy actions touching PRC trade**. In October 2025, Treasury also targeted Iran's energy export apparatus, including a China-based crude terminal and a Shandong "teapot" refinery alleged to handle Iranian-origin cargoes, warning of heightened secondary-sanctions risk for foreign financial institutions involved in significant dealings.[76]

- **Maritime compliance expectations for China-facing operations**. Treasury's updated guidance to mitigate Iran-related sanctions risk urged end-to-end cargo verification, AIS-integrity warranties, and audit/termination rights specifically for transactions involving PRC/Hong Kong counterparties and China-bound cargoes.[77] The guidance underscored deceptive-shipping and opaque PRC/Hong Kong ownership red flags for traders, carriers, port agents, and buyers operating in or trading into China.[78]

Cartel Enforcement and Foreign Terrorist Designations

Throughout 2025, federal regulators and enforcers targeted Latin American drug cartels, leveraging new foreign terrorist organization ("FTO") designations made in early 2025 to target economic activity that funded or benefitted the cartels.[79]

You Should Know

- **New FTO designations**. In 2025, the State Department designated 13 Latin American drug cartels as FTOs,[80] followed by designations of Muslim Brotherhood chapters in Egypt, Lebanon, and Jordan in early 2026.[81]

- **Material support statute's broad scope**. While cartel drug trafficking and money laundering activity has always been illegal, designating cartels as FTOs exposes businesses that operate in cartel-influenced regions to the risk of liability under an expansive U.S. criminal law with extraterritorial reach that prohibits providing material support or resources to FTOs. Under the material support statute, engaging in otherwise legal commercial activity with cartel-linked individuals and entities could expose businesses to prosecution if they are aware of their cartel links.

- **Civil liability risk**. In addition to criminal penalties, the FTO designations open the door to regulatory enforcement and private civil enforcement for significant financial damages. The Anti-Terrorism Act ("ATA") provides a private cause of action for, among other things, any U.S. national "injured . . . by the reason of an act of international terrorism."[82] This allows private parties to sue corporations for their actions which support designated terrorist groups, thus creating the possibility of significant tort liability and prolonged litigation, with private ATA cases against major businesses in some cases continuing for decades after a criminal resolution with DOJ.[83]

- **Mitigation**. Extractives, agriculture, construction, and manufacturing businesses all face heightened risk from cartel enforcement—as do industries supporting these operations such as financial institutions, payment processors, security contractors, transportation providers, and logistics providers. To mitigate risk, businesses should consider steps to map operations and counterparties in regions with a heightened cartel presence to identify vulnerabilities, as well as screening more broadly than sanctions lists to capture FTO designations and adverse media.

The "Material Support" statute

The most significant impact of the cartel designations is not on the cartels themselves but on the wide variety of otherwise legitimate enterprises whose businesses may transact with cartel-linked individuals and businesses.

- **Key features of the material support statute**. The statute provides that "[w]hoever knowingly provides material support or resources to a foreign terrorist organization, or attempts to do so" shall face criminal penalties, including up to 20 years in prison.[84] The statute applies to a wide range of otherwise legal activity.
  - "**Knowingly**." The statute requires only proof that a defendant provided material support or resources to an FTO "knowingly"—it is not a defense that the defendant did not agree with the FTO's goals.
  - "**Material support or resources**." The statute criminalizes the provision of property, funds, services, personnel, facilities, lodging, transportation, training, or expert advice to an FTO.
  - **Extraterritorial reach**. The statute is not limited to U.S. persons or U.S.-dollar transactions and has been used to prosecute those who support FTOs abroad with minimal, if any, connection to the United States.
- **DOJ enforcement priority**. DOJ has changed internal procedural rules to streamline approvals for cartel-related terrorism investigations and prosecutions.[85] And prosecutors across DOJ have prioritized cartel-related corporate enforcement:
  - In May 2025, DOJ Criminal Division Acting Assistant Attorney General Matthew Galeotti issued a memorandum that emphasized that "[m]aterial support by corporations to [FTOs], including recently designated Cartels" will be an enforcement priority.[86]
  - In December 2025, the Chief of the Criminal Division of the U.S. Attorney's Office for the Eastern District of New York, an office known for its high-profile prosecutions of cartel leaders like El Chapo and for being the only U.S. attorney's office to have ever prosecuted a company for providing material support to an FTO in the *Lafarge* case, announced that the office is re-tasking white collar criminal prosecutors to focus on cartel-related enforcement.[87]
- **Corporate enforcement precedent**. DOJ's NSD has used the material support statute and related sanctions laws in the past to bring cases against corporate defendants who make "security payments" and provide other forms of support to designated terrorist organizations.[88] Prior cases which may serve as precedents for charges against businesses who transact with cartel members include:
  - **Chiquita Brands International Inc**. In 2007, Chiquita Brands International Inc. pleaded guilty and paid a $25 million fine to resolve charges that the company violated economic sanctions by making more than 100 "security payments"—totaling more than $1.7 million—to a Colombian paramilitary organization designated as an FTO and Specially Designated Global Terrorist.[89]
  - **Lafarge S.A.** In 2022, French cement company Lafarge S.A. and its Syrian subsidiary pleaded guilty and agreed to pay more than $778 million to resolve charges that the company conspired to provide material support to an FTO based on more than $6 million in payments to ISIS and another FTO in exchange for protection, permission to operate a cement plant during the Syrian Civil War and to purchase raw materials from FTO-controlled suppliers.[90]
- **Cartel-related material support prosecutions in 2025**. Prosecutions in 2025 demonstrate that DOJ is already beginning to use the material support statute to target a broad range of conduct that supports FTO-designated cartels.
  - In May 2025, DOJ charged two South Texas business owners with conspiring to provide material support to the Mexican cartel CJNG, designated as an FTO in February 2025.[91] The indictment alleged that the defendants provided support to the cartel in the form of U.S. currency, apparently as payment for crude oil that the cartel had stolen in Mexico and then smuggled into the United States by fraudulently declaring the oil as waste and petroleum distillates.[92] The indictments

contain notices that DOJ intends to seek a $300 million forfeiture money judgment if the defendants are convicted of the charged material support conspiracy.

- In September 2025, DOJ unsealed an indictment charging a senior member of the CJNG with providing material support to the FTO through a timeshare fraud scheme.[93] The charging documents reference multiple Mexican banks, several shell companies, a resort, and a hotel chain all entangled in the scheme.

- In December 2025, DOJ announced material support charges against nearly two dozen individuals in the District of Nebraska in connection with cyber-enabled thefts targeting ATMs known as "ATM jackpotting," in which attackers use malware and physical access to an ATM to force the ATM to dispense all its cash on command.[94] DOJ alleged that the funds obtained from the ATM jackpotting thefts were used to support the drug cartel Tren de Aragua, an organization designated as an FTO in February 2025.[95]

Related Legal Risk

- **Civil liability under the ATA**. The ATA creates a civil cause of action for U.S. nationals who are victims of an act of international terrorism committed by an FTO against any person or entity who "aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism"[96] The ATA creates significant additional risk of civil liability—beyond the risk of criminal prosecution—for businesses operating in regions of Latin America under the influence of FTO-designated cartels. A notable example of the long tail of ATA liability risk is a recent $38.3 million civil jury verdict in 2024 for ATA plaintiffs against Chiquita Brands arising from the company's dealings with a Colombian cartel designated as an FTO and as a Specially Designated Global Terrorist that was the subject of a criminal resolution with DOJ in 2007.[97]

- **OFAC and FinCEN**. The Treasury Department has also taken several actions that signal increased attention to cartel-related sanctions enforcement.

  - In March 2025, OFAC issued an alert urging companies with operations in geographies "in which the designated cartels are active" to "assess their existing sanctions compliance programs to ensure controls are sufficient to minimize sanctions exposure."[98]

  - In May 2025, the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") published an additional alert asking financial institutions to monitor for possible cartel activity in connection with oil and gas dealings along the southern border.[99] The alert—published around the same time as DOJ's prosecution of the U.S. oil business owners discussed above—cautioned that U.S. oil importers and others in the oil industry face heightened risk because of the proliferation of oil smuggling schemes run by designated drug cartels.

  - In December 2025, FinCEN announced an investigation targeting U.S. money services businesses operating near the southern border, further highlighting the Administration's focus on using "all tools to stop terrorist cartels."[100]

2025's New National Security Tools

In 2025, the U.S. government added new tools to its "all tools" approach to protecting national security. New legislative and regulatory regimes included the creation of a national security-focused data protection regime, the expansion of the FCC's Covered List to include entire categories of foreign technology,[101] a first-of-its-kind enforcement of a "Team Telecom" mitigation agreement,[102] and a new statute focused on protecting the U.S. biotechnology supply chain from foreign adversaries.

DOJ's National Security Division Data Security Program

A major regulatory change occurred in 2025 with the implementation of DOJ's Data Security Program (the "DSP"), which was issued in January 2025, with staggered effective dates of April 8 and October 6, 2025. The DSP created a new national security-driven framework that restricts or prohibits transfers of U.S. bulk "sensitive" personal data and U.S.-government-related data to "countries of concern" such as China, Russia, and Iran.[103] The DSP applies broadly to U.S. and foreign persons doing business in or with the United States. Unlike data privacy laws, the DSP cannot be waived by individual consent, as its purpose is to protect national security interests rather than consumer privacy. To protect against inadvertent violations, companies that collect, process, or transfer data should consider steps to quickly assess applicability, map cross-border data flows, and update compliance programs and counterparties accordingly given the DSP's breadth and rapid rollout. Our full analysis of the new regulatory landscape under the DSP can be found in our *2025 Year in Review: Cybersecurity and Data Protection*.[104]

The FCC's Emergence as a Potent National Security Regulator

In March 2025, Chairman Carr announced that the FCC would center national security in the Commission's regulatory policymaking agenda, with the appointment of his National Security Counsel as the first director of the FCC's new Council on National Security.[105]

You Should Know

- **Major changes**. A raft of national-security-focused policy changes followed the FCC's March 2025 announcement, setting the stage for more regulatory actions and enforcement action in 2026.[106]
- **Preparing for more**. The Commission's aggressive moves to expand its national security regulatory authority in 2025 portend further efforts to exercise that authority to exclude foreign manufacturers and their equipment from the U.S. market. Companies that rely on technologies subject to heightened federal government scrutiny for national security reasons should consider steps to stay abreast of rapidly developing, novel uses of statutory authority.
- **Mitigation measures**. Telecoms should consider expediting "rip-and-replace" capital investment strategies to stay ahead of a potential revocation of previous equipment approvals that could compel them to immediately cease using legacy network equipment provided by Covered Entities such as Huawei and ZTE. Business still using Hikvision and Dahua security cameras, video management systems, and other solutions face a similar risk of unexpected liability.

Expansion of Covered List Controls

In 2025, the FCC revised its rules to strengthen the "Covered List and has used the Covered List in novel ways that creates new risks for companies across sectors.

Under the Secure and Trusted Communications Networks Act of 2019, the FCC has maintained for the last five years a Covered List, which includes certain manufacturers or equipment or services that the FCC has determined "pos[e] an unacceptable risk to the national security of the United States or the safety and security of United States persons."[107] When a company is added to the Covered List, new FCC equipment authorizations are prohibited for covered equipment, which in turn prevents the import, marketing, sale, or operation of any new covered equipment from the date on which the listing takes effect.[108]

- **Extending Covered List review to previously authorized equipment**. The Commission took several steps to broaden the scope of Covered List review.
  - **Expansion**. The first shift came in October 2025, when the FCC moved to further strengthen the Covered List as a national security policy tool. Previously, the Covered List review process applied only to new devices. Under the FCC's new policy, however, the Commission can extend a Covered List review to previously authorized devices, and the Commission can thus "revoke existing authorizations" and effectively stop imports and prohibit sales or support of already authorized covered devices based on updated security assessments.[109]
  - **Proposed rulemaking**. The Commission also adopted a Further Notice of Proposed Rulemaking that would strengthen the FCC's ability to use the Covered List to regulate component parts of authorized devices. The Notice of Proposed Rulemaking also provides that modifications to authorized devices require a new application for FCC certification.[110]
- **Novel use of the Covered List to address the threat from foreign UAS**. The second major move from the Commission came in December 2025, with new steps to regulate commercial drones to address the risk that foreign-made components could "enable persistent surveillance, data exfiltration, and destructive operations over U.S. territory, including over World Cup and Olympic venues and other mass gathering events."[111]
  - **Regulating an entire class of equipment**. In addressing this risk, the FCC did not simply list specific equipment or name UAS manufacturers. For the first time, the FCC added to the Covered List an entire class of equipment of foreign origin, identifying the listed equipment as "uncrewed aircraft systems" ("UAS") and UAS-critical components produced in foreign countries," more commonly referred to as drones.[112]
  - **No restriction on existing approvals**. The FCC has made clear that the new listing does not "prevent retailers from continuing to sell, import, or market devices" already approved by the Commission and that the new restrictions only "apply to new device models," allowing companies to continue U.S. sales of older models. In early January 2026, the effect of the listing was further tempered by the FCC's decision to temporarily exempt certain UAS and UAS

components specifically identified ("blue listed") by the Defense Contract Management Agency or that qualify as "domestic end products" under the Buy American Standard.[113]

- **Impact on consumer drones**. The UAS listing, however, will continue to impact the largest manufacturers of consumer drones, which produce most of the world's drones in China.[114] The new listing aligns with actions taken by the Administration to curb the presence of foreign aircraft in U.S. airspace, including warnings that drone supply chains require additional protections against "undue foreign influence and exploitation."[115]

Other FCC National Security Actions in 2025

- **Submarine cables, bad labs, and spy gear**. In addition to significant Covered List changes the FCC also adopted rules aimed at improving undersea cable security,[116] reviewed and revoked the certifications of electronics approval labs ("bad labs") located in China,[117] and closed loopholes to make it more difficult for spy gear to be sold in the country.[118]

- **Team Telecom mitigation**. The FCC capped 2025 with the first-ever enforcement action for violations of a mitigation agreement supervised by the U.S. government's interagency "Team Telecom," following a referral by DOJ's NSD, which chairs Team Telecom.[119] The action, via an FCC Order and Consent Decree with Marlink, requires a $175,000 voluntary contribution, tighter access controls, and a multi-year compliance plan centered on screening and DOJ notifications for foreign-person employee access to U.S. communications infrastructure and records.

The BIOSECURE Act

Congress has also enacted new prohibitions related to U.S. government contracting with certain biotechnology companies in the 2026 NDAA, which included in Section 851 an updated version of the BIOSECURE Act.[120]

This prohibits government agencies from procuring or obtaining "any biotechnology equipment or service produced or provided by a biotechnology company of concern" and sets up a process to designate those entities.[121] Subject to certain exceptions, the Act also prohibits government agencies from contracting with (1) entities that use biotechnology equipment or services produced or provided by a biotechnology company of concern after the Act's effective date in performance of the government contract or (2) entities that "know[]"that the performance of a government contract will require goods or services from a biotechnology company of concern.[122]

You Should Know

- **Wide impact on biotechnology sector**. The BIOSECURE Act has important implications for a range of businesses. In particular, it creates new risk for pharmaceutical and other biotechnology companies that may rely on goods or services from entities that could be designated as biotechnology companies of concern.

- **Importance of 1260H List**. The Act elevates the importance of the Department of War's "Section 1260H" list of Chinese military companies, slated to be next updated in January 2026.

- **Long-term strategic impact**. Given the extended timeline on which the Act is to come into effect, for many biotechnology companies, the Act's most immediate practical impact may be felt in the need to reassess long-term strategic plans that may carry new risk from vendor and co-development agreements with biotechnology companies, such as those located in China, which now now at risk of being listed as biotechnology companies of concern.

The Act's Key Provisions

- The Act provides two mechanisms to list a biotechnology company as a "company of concern:"

  - **1260H List**. "[B]iotechnology company of concern" includes an entity that is (1) involved in biotechnology equipment or services and (2) is listed on the Department of War's Section 1260H list of Chinese military companies.[123]

  - **OMB List**. The Act directs the Office of Management and Budget ("OMB") to publish a list of companies of concern based on recommendations from certain Executive Branch agencies.[124]

- **Limitations and Exclusions**. The Act's prohibitions are subject to several exceptions.

  - **General exclusions**. The Act has exclusions, including that the provisions in the Act do not apply to the acquisition of healthcare services overseas for U.S. government employees and their dependents, to the acquisition and use of lawfully

compiled human multiomic data that are commercially or publicly available, or to the procurement of products or related supplies in direct response to a declared public health emergency.[125]

- **Medicaid and Medicare limitations**. The Act makes clear that its prohibitions will not prevent payments for drugs under Medicaid and Medicare Part B.[126]
- **Case-by-case exclusions**. The Act authorizes the head of an executive agency to waive the Act's provisions on a case-by-case basis for an initial period of one year with the approval of the director of OMB, stipulated that notice is provided to the applicable Congressional committees within 30 days of granting such waiver.[127]

- **Timeline**. It could be quite some time—as long as two-and-a-half years—before the BIOSECURE Act's prohibitions begin to come into effect. The Act requires a sequence of regulatory actions by multiple agencies to trigger the prohibitions.[128] These include OMB publishing a list of countries of concern[129] as well as revisions to the Federal Acquisition Regulation.[130]

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Daniel J. Gerkin
+1-202-223-7407
dgerkin@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Melinda Haag
+1-628-432-5110
mhaag@paulweiss.com

Elizabeth Hanft
+1-212-373-3664
ehanft@paulweiss.com

Nicole Kar
+44-20-7601-8657
nkar@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Loretta E. Lynch
+1-212-373-3000

Mark F. Mendelsohn
+1-212-373-3337
mmendelsohn@paulweiss.com

Nathan Mitchell
+1-202-223-7422
nmitchell@paulweiss.com

Ian C. Richardson
+1-202-223-7405
irichardson@paulweiss.com

Nicole Succar
+1-212-373-3624
nsuccar@paulweiss.com

Benjamin Klein
+1-202-223-7317
bklein@paulweiss.com

Samuel Kleiner
+1-212-373-3797
skleiner@paulweiss.com

Associates Neil Chitrao, Noah Cohen, Rachel Gallagher, Rakhi G. Kundra, Yanna Lee, Rana Matared, Jacob R. Schulz, Michael Shepard, Joshua R. Thompson and David T. Wong and law clerk Charlotte G. Cooper contributed to this Client Memorandum.

[1] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments - 2025 Year in Review* (Jan. 21, 2026), available here.

[2] The White House, *America First Investment Policy* (Feb. 21, 2025), available here.

[3] The National Agricultural Law Center, *2025 Legislative Recap: Continued Expansion of State-Level Foreign Ownership Restrictions* (Oct. 7, 2025), available here.

[4] The White House, *America First Investment Policy* (Feb. 21, 2025), available here.

[5] U.S. Dep't of the Treasury, Press Release, *U.S. Department of the Treasury Announces Intent to Launch Fast Track Pilot Program for Foreign Investors* (May 8, 2025), available here.

[6] Paul, Weiss, *Final CFIUS Regulations Implementing the Foreign Investment Risk Review Modernization Act of 2018 Are Now in Effect* (Feb. 27, 2020), available here.

[7] Paul, Weiss, *DOJ Issues Final Rule Restricting the Transfer of Certain Sensitive U.S.-Person Data* (Jan. 17, 2025), available here; *see also* John Carlin, et al., *DOJ Data Security Rule Has Ticking Clock for Companies to Comply*, BLOOMBERG LAW: U.S. LAW WEEK (May 20, 2025), available here.

[8] CFIUS, Annual Report to Congress: CY 2024 (2024).

[9] Howard Lutnick (@howardlutnick), [Post stating that the President secured a perpetual "Golden Share" as part of Nippon Steel's acquisition of U.S. Steel], X (June 14, 2025, 12:28 p.m.), available here.

[10] Paul, Weiss, *Executive Order Requires Chinese Owners to Divest From U.S. Technology Company* (July 21, 2025), available here.

[11] *See* 31 C.F.R. pt. 850 (Nov. 15, 2024), available here; Paul, Weiss, *2024 Year in Review: CFIUS, Outbound Investments and Export Controls* (Dec. 6, 2024), available here; Paul, Weiss, *Treasury Department Issues Final Rule Regulating Outbound Investment to Protect National Security* (Dec. 6, 2024), available here.

[12] *National Defense Authorization Act for Fiscal Year 2026*, Pub. L. No. 119-60 available here.

[13] *See, e.g.*, *id.* at §§ 8511(b)–(c) (IEEPA); § 8521 (DPA).

[14] *Id.* at§ 802(a).

[15] *Id.* at § 801(a).

[16] *See, e.g.*, *id.* at § 801(c) (Exemptions); § 801(e)(2).

[17] *Id.* at § 809(4)(A).

[18] *Id.* at § 809(4)(A)(vi).

[19] *See* 31 C.F.R. § 850.303(a).

[20] § 809(2).

[21] §§ 809(7), 809(10).

[22] *See* House Foreign Affairs Committee, Press Release, *Chairman Mast Introduces AI OVERWATCH Act to Secure America's Technological Dominance* (Dec. 19, 2025), available here; Maggie Eastland, *Congress Revisits Export Curbs in Wake of Trump's H200 Approval*, BLOOMBERG LAW (Dec. 19, 2025), available here. [Broken Link]

[23] *See, e.g.*, WireScreen, Press Announcement, *WireScreen Identifies More Than 20,000 Chinese Entities Affected by the U.S. BIS 50 Percent Affiliates Rule* (Oct. 20, 2025), available here.

[24] Bureau of Indus. & Sec. ("BIS"), U.S. Dep't of Com., *Framework for Artificial Intelligence Diffusion*, 90 Fed. Reg. 12345 (Jan. 15, 2025), available here.

[25] BIS, U.S. Dep't of Com., *BIS Policy Statement on Controls that May Apply to Advanced Computing Integrated Circuits and Other Commodities Used to Train AI Models* (May 13, 2025), available here.

[26] BIS, U.S. Dep't of Com., *Guidance on Application of General Prohibition 10 (GP10) to People's Republic of China (PRC) Advanced-Computing Integrated Circuits (ICs)* (May 13, 2025), available here.

[27] BIS, U.S. Dep't of Com., *Industry Guidance to Prevent Diversion of Advanced Computing Integrated Circuits* (May 13, 2025), available here.

[28] *See* The White House, *Winning the Race, America's AI Action Plan* (July 2025), available here.

[29] *See* Siemens, *A Statement from Tony Hemmelgarn* (June 4, 2025), available here; Reuters, *Exclusive: Synopsys halts China sales due to US export restrictions, internal memo shows* (May 30, 2025), available here; Cadence Design Systems, Inc., SEC Form 8-K (May 29, 2025), available here.

[30] *See* CNBC, *U.S. lifts chip software curbs on China in sign of trade truce* (July 2, 2025), available here.

[31] The Affiliates Rule also introduced a "most-restrictive owner" standard, a new Red Flag, changes to the foreign direct product rule ("FDPR"), and a narrow temporary general license. Paul, Weiss, *New Commerce Rule Applies Entity List and Other Restrictions to 50% or Greater Owned Foreign Affiliates* (Oct. 2, 2025), available here.

[32] The White House, *Fact Sheet: President Donald J. Trump Strikes Deal on Economic and Trade Relations with China* (Nov. 1, 2025), available here; Paul, Weiss, *White House Announces One-Year Suspension of Export Controls "Affiliates" Rule* (Nov. 6, 2025), available here.

[33] BIS, U.S. Dep't of Com., *Additions to the Entity List*, 90 Fed. Reg. 48193 (Oct. 9, 2025) (15 C.F.R. pt. 744), available here.

[34] BIS, U.S. Dep't of Com., *Revisions to the Entity List*, 90 Fed. Reg. 50858 (Nov. 12, 2025) (15 C.F.R. pt. 744), available here.

[35] BIS, U.S. Dep't of Com., *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, 90 Fed. Reg. 5360 (Jan. 16, 2025) (15 C.F.R. pt. 791), available here; BIS, U.S. Dep't of Com., *Connected Vehicles (CV): Overview*, available here (last visited Nov. 17, 2025).

[36] BIS, U.S. Dep't of Com., *Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems*, 90 Fed. Reg. 271 (proposed Jan. 3, 2025) (to be codified at 15 C.F.R. pt. 791), available here; BIS, U.S. Dep't of Com., *Securing the Information and Communications Technology and Services Supply Chain: Medium- and Heavy-Duty Connected Vehicles*, (proposed Sept. 5, 2025) (to be codified at 15 C.F.R. pt. 791), available here. While these final rules are pending, the President imposed a 25% tariff on imported trucks in October 2025, effective November 1, 2025. *See* The White House, *Adjusting Imports of Medium- and Heavy-Duty Vehicles, Medium-and Heavy-Duty Vehicle Parts, and Buses into the United States* (Oct. 17, 2025), available here. Tariffs on imported passenger vehicles were implemented earlier in the year. *See* The White House, *Fact Sheet: President Donald J. Trump*

Adjusts Imports of Automobiles and Automobile Parts into the United States (March 26, 2025), available here (The President signed a proclamation on March 26, 2025 that imposed a 25% tariff on imported passenger vehicles and certain automobile parts under Section 232 of the Trade Expansion Act of 1962, citing national security concerns. Tariffs on the associated auto parts went into effect on May 3, 2025.).

[37] Reuters, *U.S. Commerce Department drops plan to impose restrictions on Chinese-made drones* (Jan. 9, 2026), available here.

[38] BIS, U.S. Dep't of Com., *Validated End-User Authorization FAQ* (Jan. 23, 2017), available here.

[39] Paul, Weiss, *U.S. Government Eases Export Control Restrictions for AI Chips Bound for Qualifying Data Centers* (Oct. 3, 2024), available here.

[40] BIS, U.S. Dep't of Com., *Revocation of Validated End-User Authorizations in the People's Republic of China*, 90 Fed. Reg. 42321 (Sept. 2, 2025) (15 C.F.R. pt. 748), available here. *See also*, BIS, U.S. Dep't of Com, Press Release, *Department of Commerce Closes Export Controls Loophole for Foreign-Owned Semiconductor Fabs in China* (Aug. 29, 2025), available here. BIS will continue to approve licenses for ongoing operations at existing facilities but not for expansions or upgrades.

[41] U.S. Dep't of Com., Press Release, *Statement on UAE and Saudi Chip Exports* (Nov. 19, 2025), available here; *see also* Microsoft, *Microsoft's $15.2 billion USD investment in the UAE* (Nov. 3, 2025), available here.

[42] Reuters, *US to allow Nvidia H200 chip shipments to China, Trump says* (Dec. 9, 2025), available here.

[43] BIS, U.S. Dep't of Com., *Order Relating to Alpha and Omega Semiconductor Incorporated* (June 24, 2025), available here.

[44] Paul, Weiss, *U.S. Software and Semiconductor Company Resolves Criminal and Civil Export Control Enforcement Actions With Guilty Plea, Payment of $140 Million* (Aug. 6, 2025), available here.

[45] National Security Division, U.S. Dep't of Justice, *In re Universities Space Research Association* (Apr. 23, 2025), available here.

[46] Paul, Weiss, *DOJ Announces First Ever Declination of Prosecution of an Acquiring Company for Sanctions Violations Under DOJ's M&A Safe Harbor Policy* (June 20, 2025), available here.

[47] U.S. Dep't of Justice, Press Release, *Company Insider Sentenced To 18 Months In Prison For Fraudulently Obtaining Laboratory Research Products For Illegal Export To China* (Sept. 9, 2025), available here; *see also* National Security Division, U.S. Dep't of Justice, *Ringleader and Company Insider Plead Guilty to Defrauding Biochemical Company and Diverting Products to China Using Falsified Export Documents* (May 22, 2024), available here.

[48] Paul, Weiss, *DOJ National Security Division Issues First Declination Under Voluntary Self-Disclosure Program* (May 24, 2025), available here.

[49] National Security Division, U.S. Dep't of Justice, *Two Chinese Nationals Arrested on Complaint Alleging they Illegally Shipped to China Sensitive Microchips Used in AI Applications* (Aug. 5, 2025), available here; National Security Division, U.S. Dep't of Justice, *U.S. Citizens and Chinese Nationals Arrested for Exporting Artificial Intelligence Technology to China* (Nov. 20, 2025), available here.

[50] Ana Swanson, *Tariffs Are Here to Stay, Even if the Supreme Court Rules Against Trump*, New York Times (Nov. 5, 2025), available here.

[51] BIS, U.S. Dep't of Com., *Advancing national security through technology leadership and vigilant export controls*, available here.

[52] The White House, *Adjusting Imports of Semiconductors, Semiconductor Manufacturing Equipment, and Their Derivative Products into the United States* (Jan. 14, 2026), available here.

[53] The White House, *Suspending Duty-Free De Minimis Treatment for All Countries* (July 30, 2025), available here.

[54] U.S. Customs and Border Protection, *CBP Collects $1 Billion Since End of De Minimis Loophole* (Dec. 17, 2025), available here.

[55] Bill Chappell, *This Rule Made Many Online Purchases Dirt Cheap for U.S. Consumers. Now It's Ending*, NPR (Aug. 28, 2005), available here.

[56] Mae Anderson, *Postal Traffic to US Still Down 70% Five Weeks After Duties Exemption on Low-Value Packages Ended*, AP News (Oct. 10, 2025), available here.

[57] The White House, *Fact Sheet: Following Trade Deal Announcements, President Donald J. Trump Modifies the Scope of the Reciprocal Tariffs with Respect to Certain Agricultural Products* (Nov. 14, 2025), available here.

[58] The White House, *Fact Sheet: The United States and European Union Reach Massive Trade Deal* (July 28, 2025), available here; Shayerah I. Akhtar, *U.S.-EU Tariffs and Trade Framework Agreement*, Congressional Research Service (Sept. 18, 2025), available here.

[59] Section 122 gives the President authority to impose temporary tariffs of 15% for 150 days to address balance-of-payment deficits. 19 U.S.C. § 2132. Section 301 permits the White House to impose tariffs on countries that the U.S. Trade Representative deems to be violating trade agreements or actively disadvantaging U.S. commerce. 19 U.S.C. §§ 2411–2420. Section 338 allows the President to impose tariffs on countries engaged in discriminatory trade practices against the United States. 19 U.S.C. § 1338.

[60] Exec. Order No. 14326 (July 31, 2025), available here.

[61] Paul, Weiss, *Trump Administration Heightens Enforcement Focus on Tariff Evasion and "Transshipment"* (Aug. 25, 2025), available here; U.S. Dep't of Justice, *Departments of Justice and Homeland Security Partnering on Cross-Agency Trade Fraud Task Force* (Aug. 29, 2025), available here.

[62] U.S. Dep't of Justice, *Market, Government, and Consumer Fraud Unit* (Sept. 9, 2025), available here.

[63] U.S. Dep't of Justice, *Departments of Justice and Homeland Security Partnering on Cross-Agency Trade Fraud Task Force* (Aug. 29, 2025), available here.

[64] Justin Wise, *DOJ Frauds Unit Tasked With Pursuing Evasion of Trump Tariffs (1)*, Bloomberg (July 10, 2025), available here; U.S. Dep't of Justice, *Market, Government, and Consumer Fraud Unit* (Sept. 9, 2025), available here.

[65] U.S. Dep't of Justice, Press Release, *Bay Area-Based Flooring Company and Its Owners to Pay $8.1 Million to Settle False Claims Allegations Related to Customs Duties Evasions* (Mar. 26, 2025), available here.

[66] Paul, Weiss, *Trump Administration Heightens Enforcement Focus on Tariff Evasion and "Transshipment"* (Aug. 25, 2025), available here.

[67] U.S. Dep't of Justice, Press Release, *Indonesian Jewelry Company, Co-Owner, and Two Other Employees Charged in Large-Scale Duty and Tax Evasion Scheme* (Nov. 17, 2025), available here.

[68] U.S. Dep't of Justice, Press Release, *Justice Department Resolves Criminal Trade Fraud Investigation with Plastic Resin Distributor; Former Executive Agrees to Plead Guilty*, (Dec. 18, 2025), available here; U.S. Dep't of Justice, *Ceratizit USA LLC Agrees to Pay $54.4M to Settle False Claims Act Allegations Relating to Evaded Customs Duties* (Dec. 18, 2025), available here.

[69] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments - 2025 Year in Review* (Jan. 21, 2026), available here.

[70] Paul, Weiss, *In First Major Escalation of Russian Sanctions During the Second Trump Administration, Treasury Announces New Sanctions on Major Russian Oil Companies and Urges Immediate Ceasefire* (Oct. 24, 2025), available here.

[71] Paul, Weiss, *OFAC Imposes $216 Million Penalty on Silicon Valley Venture Capital Firm for Russian Sanctions Violations* (June 30, 2025), available here.

[72] Paul, Weiss, *OFAC Reaches $11.5 Million Resolution With Private Equity Firm for Indirect Dealings With a Sanctioned Party* (Dec. 8, 2025), available here.

[73] S. 1071, National Defense Authorization Act for Fiscal Year 2026 (Dec. 18, 2025), § 8369, available here.

[74] U.S. Dep't of Treasury, Press Release, *Treasury Targets Iran's Efforts to Domestically Manufacture Key Ballistic Missile Components* (May 14, 2025), available here.

[75] U.S. Dep't of Treasury, Press Release, *Treasury Targets Iranian Weapons Procurement Networks Supporting Ballistic Missile and Military Aircraft Programs* (Oct. 1, 2025), available here.

[76] U.S. Dep't of Treasury, Press Release, *Treasury Dismantles Key Elements of Iran's Energy Export Machine* (Oct. 9, 2025), available here.

[77] U.S. Dep't of Treasury, *Guidance for Shipping and Maritime Stakeholders on Detecting and Mitigating Iranian Oil Sanctions Evasion* (Apr. 16, 2025), available here.

[78] U.S. Dep't of Treasury, Press Release, *Treasury Dismantles Key Elements of Iran's Energy Export Machine* (Oct. 9, 2025), available here.

[79] U.S. Dep't of Justice, *Matthew R. Galeotti, Acting Assistant Attorney General of the Criminal Division, Delivers Remarks at Press Event Announcing Charges against Senior Leaders of the United Cartels* (Aug. 15, 2025), available here.

[80] *See*, *e.g.*, U.S. Dep't of State, *Designation of International Cartels* (Feb. 20, 2025), available here; U.S. Dep't of State, *Sanctioning High Ranking Members of Cártel del Noreste*, (May 21, 2025), available here; U.S. Dep't of State, *Designated Foreign Terrorist Organizations*, available here.

[81] U.S. Dep't of State, Press Statement, *Terrorist Designations of Muslim Brotherhood Chapters* (Jan. 13, 2026), available here; White House, *Designation of Certain Muslim Brotherhood Chapters as Foreign Terrorist Organizations and Specially Designated Global Terrorists* (Nov. 24, 2025), available here.

[82] 18 U.S.C. § 2333(a).

[83] *See* CNN, *Chiquita found liable for financing paramilitary group* (June 12, 2024), available here.

[84] 18 U.S.C. § 2339B(a)(1).

[85] Attorney General Pamela Bondi, *Memorandum Re: Total Elimination of Cartels and Transnational Criminal Organizations* (Feb. 5, 2025), available here.

[86] Paul, Weiss, *DOJ Announces New Corporate and White-Collar Enforcement Policies and Priorities*, at 1 (May 15, 2025), available here; Matthew R. Galeotti, *Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime*, at 4 (May 12, 2025), available here.

[87] Mike Vilensky, *US Prosecutor in NY Says 2025 Was 'Reset' for White-Collar Crime*, Bloomberg Law (Dec. 9, 2025), available here.

[88] Mark Mendelsohn et al., *How to Navigate Risks for Firms on Cartel-Related Activities*, Bloomberg Law (June 5, 2025), available here.

[89] U.S. Dep't of Justice, *Chiquita Brands International Pleads Guilty to Making Payments to a Designated Terrorist Organization And Agrees to Pay $25 Million Fine* (Mar. 19, 2007), available here.

[90] U.S. Dep't of Justice, *Lafarge Pleads Guilty to Conspiring to Provide Material Support to Foreign Terrorist Organizations* (Oct. 18, 2022), available here; Paul, Weiss, *DOJ Brings First Terrorism Material Support Charge Against a Corporation, Underlining the Importance of Compliance When Operating in High-Risk Countries and of Robust M&A Due Diligence*, at 1 (Oct. 22, 2022), available here.

[91] U.S. Dep't of Justice, *Father and Son Indicted for Providing Material Support to Mexican Cartel Engaged in Terrorism* (May 30, 2025), available here.

[92] El Pais, *Washington links the Jensen family to the CJNG leadership in charge of fuel theft* (Nov. 21, 2025), available here.

[93] U.S. Dep't of Justice, *Senior CJNG Member Indicted on Wire Fraud, Money Laundering, and Terrorism Charges for Operating Massive Timeshare Fraud Scheme* (Sept. 22, 2025), available here.

[94] U.S. Dep't of Justice, *Tren De Aragua Members and Leaders Indicted in Multi-Million Dollar ATM Jackpotting Scheme* (Dec. 18, 2025), available here.

[95] U.S. Dep't of State, *Designation of International Cartels* (Feb. 20, 2025), available here.

[96] *See* 18 U.S.C. § 2333; *Twitter, Inc.* v. *Taamneh*, 598 U.S. 471 (2023); *In re Chiquita Brands Int'l, Inc. Alien Tort Statute and Shareholder Derivative Litigation*, 0:08-md-01916-MARRA (S.D. Fla. June 10, 2024), at *5.

[97] U.S. Dep't of Justice, *Chiquita Brands International Pleads Guilty to Making Payments to a Designated Terrorist Organization And Agrees to Pay $25 Million Fine* (Mar. 19, 2007), available here.

[98] Office of Foreign Assets Control, OFAC Alert, *International Cartels Designated as Foreign Terrorist Organizations and Specially Designated Global Terrorists* (Mar. 18, 2025), available here.

[99] Financial Crimes Enforcement Network, FinCEN Alert, *FinCEN Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels* (May 1, 2025), available here.

[100] Financial Crimes Enforcement Network, *FinCEN Announces Data-Driven Border Operation to Address Potential Money Laundering* (Dec. 22, 2025), available here.

[101] FCC, *Fact Sheet: FCC Updates Covered List to Include Foreign UAS and UAS Critical Components on Going Forward Basis* (Dec. 22, 2025), available here.

[102] FCC, *FCC Announces Landmark Enforcement of Team Telecom Commitments* (Jan. 8, 2026), available here.

[103] U.S. Dep't of Justice, *Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries* (Apr. 11, 2025), available here.

[104] Paul, Weiss, *2025 Year in Review: Cybersecurity and Data Protection* (Jan. 7, 2026), available here.

[105] FCC, *Chairman Carr Establishes New Council on National Security Within Agency* (Mar. 13, 2025), available here.

[106] FCC, *Chairman Carr Highlights Wins Delivered in 2025* (Dec. 23, 2025), available here.

[107] 47 C.F.R. 1.50002(b); 47 U.S.C. §§ 1601–1609.

[108] 47 U.S.C. § 302a(b).

[109] FCC, Second Report and Order and Second Further Notice of Proposed Rulemaking, (Oct. 29, 2025), FCC 25-71, ¶ 18.

[110] *Id.* at ¶ 57.

[111] *Id.* at *2.

[112] FCC, Public Notice, Public Safety and Homeland Security Bureau Announces Addition of Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced Abroad, and Equipment and Services Listed in Section 1709 of the FY2025 NDAA, to FCC Covered List (Dec. 22, 2025), DA 25-1086, at *1.

[113] FCC, Public Notice, Public Safety and Homeland Security Bureau Announces Exemption of Certain Uncrewed Aircraft Systems (UAS) and UAS Critical Components from FCC Covered List (Jan. 7, 2026), DA-26-22, at *2.

[114] Farah Stockman, *Trump Administration Declares Foreign-Made Drones a Security Threat*, NEW YORK TIMES (Dec. 22, 2025), available here.

[115] The White House, *Unleashing American Drone Dominance* (June 6, 2025), available here.

[116] FCC, *FCC Acts to Accelerate Submarine Cable Buildout & Security* (Aug. 7, 2025), available here.

[117] FCC, *FCC Takes Action on "Bad Labs" Apparently Controlled by China* (Sept. 8, 2025), available here.

[118] FCC, *FCC Approves New Safeguards Against Untrustworthy Gear* (Oct. 28, 2025), available here.

[119] FCC, *FCC Announces Landmark Enforcement of Team Telecom Commitments* (Jan. 8, 2026), available here.

[120] S. 1071, National Defense Authorization Act for Fiscal Year 2026 (Dec. 18, 2025), available here.

[121] *Id.* § 851(a)(1). A separate provision of the 2026 NDAA contains a similar, overlapping prohibition preventing elements of the intelligence community from contracting with certain similarly defined biotechnology companies of concern. *See id.* § 6703.

[122] *Id.* §§ 851(a)(2)(A)–(B).

[123] *Id.* § 851(f)(2).

[124] *Id.* § 851(f)(1).

[125] *Id.* § 851(e).

[126] *Id.* § 851(l).

[127] *Id.* § 851(d)(1).

[128] *Id.* § 851(h).

[129] *Id.* § 851(f)(1).

[130] *Id.* § 851(c)(1) and (2).