



National Foreign Trade Council

Input to the United States Trade Representative consultation:

2027 National Trade Estimate (NTE) Comments

Comments Regarding Significant Foreign Trade Barriers for the 2027 National Trade Estimate Report

Docket No. USTR-2026-0498

October 29, 2026

Table of Contents:

Introduction	4
Cross-Cutting Issues	4
Country-by-Country Trade Barriers	6
Argentina	6
Australia	9
Azerbaijan	12
Bangladesh	13
Bolivia	14
Brazil	15
Cambodia	23
Canada	24
Chile	31
China	34
Colombia	39
Costa Rica	43
Dominican Republic	44
Ecuador	45
Egypt	46
El Salvador	47
Ethiopia	48
The European Union	48
Guatemala	72
Honduras	72
Iceland	73
India	73
Indonesia	85
Israel	96
Japan	96
Jordan	99
Kenya	100

Kuwait	108
Malaysia	108
Mexico	110
Nepal	121
New Zealand	122
Nigeria	122
Norway	124
Oman	124
Pakistan	125
Panama	127
Peru	128
The Philippines	130
Qatar	132
Russia	133
Saudi Arabia	134
South Africa	137
Switzerland	138
Taiwan	138
Tanzania	141
Thailand	141
Türkiye	144
Ukraine	149
United Arab Emirates	149
The United Kingdom	150
Vietnam	153

Introduction

These comments are submitted by the National Foreign Trade Council (NFTC) in response to the notice, *Request for Comments on Significant Foreign Trade Barriers for the 2027 National Trade Estimate Report* which was published in the Federal Register on September 14, 2026. Pursuant to the notice, the Office of the United States Trade Representative (USTR), through the Trade Policy Staff Committee (TPSC), publishes the National Trade Estimate Report on Foreign Trade Barriers (NTE Report) each year. USTR invites comments to assist it and the TPSC in identifying significant foreign barriers to, or distortions of, U.S. exports of goods and services and U.S. foreign direct investment for inclusion in the NTE Report.

NFTC is dedicated to making America more competitive in the global economy by ensuring the adoption of forward-looking tax and trade policies, by strengthening global rules and by opening foreign markets to U.S. products and services. Our strong support for these objectives, and our belief that their fulfillment is essential to our members' success in a globalized economy, have been unwavering for over a century. We, therefore, believe that it is critical to provide policymakers in the administration with our clear views about the role trade and tax policies play with respect to U.S. competitiveness in the global economy.

The National Foreign Trade Council is the premier business association advancing trade and tax policies that support access to the global marketplace. Founded in 1914, NFTC promotes an open, rules-based global economy on behalf of a diverse membership of U.S.-based businesses, who account for over \$6 trillion in revenue and employ nearly six million people in the United States.

Cross-Cutting Issues

Further to the country-specific comments on trade barriers below, we want to raise two cross-cutting issues that continue to create significant challenges for U.S. exporters:

Pharmaceutical Pricing Practices: Addressing unfairness in foreign pharmaceutical pricing practices is critical to supporting U.S. pharmaceutical exports and manufacturing jobs. As a global leader in medical innovation, the United States must ensure that international markets adequately value and pay their fair share for our groundbreaking medicines and vaccines. Across many international markets, government-controlled pricing and reimbursement systems systematically undervalue innovative medicines through non-transparent or discriminatory value assessments, the use of low-cost or outdated comparators, mandatory discounts and price reductions, revenue claw backs, and lengthy or unpredictable reimbursement processes. International reference-pricing policies can compound these distortions by importing artificially suppressed prices from other markets without accounting for differences in economic capacity, disease burden, standards of care, or the broader value medicines deliver to patients and society. By challenging pricing policies that undermine the value medical innovations bring to society, the United States can protect our manufacturing sector, sustain our innovation ecosystem, and maintain our competitive edge in the global biopharmaceutical market amid intensifying global competition from emerging life sciences players, such as China.

Customs Valuation for Intercompany Transfers: Customs valuation of intercompany transfers of technology equipment creates significant compliance burdens for U.S. companies. In particular, when goods are transferred between related parties (e.g., subsidiaries of the same ultimate corporate parent entity) without a sale, Customs authorities require complex valuation methodologies, applied inconsistently across countries (sometimes across imports to the same country) often necessitating the

provision of extensive documentation to prove arm's length values (even when values are the same or similar for hardware imports between unrelated parties). This issue is particularly difficult for transfers of broken or depreciated equipment between related companies. These issues create administrative burdens, potential disputes, and unwarranted audits and investigations. The complexity of valuation requirements, onerous documentation demands, and inconsistent application of valuation requirements across countries (and across imports into a single country) act as barriers to consistent and fair treatment of U.S. imports to other countries. This issue affects trade with: Indonesia, India, Brazil, Malaysia, Thailand, and Australia.

Harmonized System Classification Challenges: Inconsistent approaches to import classifications of technology hardware under the Harmonized Tariff Schedule (HTS) creates ongoing compliance challenges for U.S. companies. Classification disputes with Customs authorities over technology hardware categories often occur, even after previous agreements are reached (e.g., when new Customs officials are appointed). Since import classifications determine duty rates and special requirements, the inconsistent application creates uncertainty, leads to supply chain disruptions, and often results in additional administrative burden and costs (e.g., when addressing unwarranted audits, investigations, and legal challenges). The complexity of classifying integrated technology systems leads to inconsistent treatment across countries and acts as a barrier to consistent and fair treatment of U.S. imports to other countries. This issue affects U.S. trade with several countries, including: Indonesia, India, Brazil, Vietnam, Malaysia, Singapore, Thailand, and Australia. **WTO E-Commerce Moratorium:** The WTO e-commerce moratorium has played a critical role in establishing the seamless operation and growth of global digital trade. Despite its unfortunate lapse at the WTO Ministerial Conference 14 in March 2026, we have been pleased that the majority of nations have continued abiding by the practice of not imposing duties. A key contributing factor driving this outcome has been the United States' leadership in spearheading the voluntary plurilateral agreement to continue the moratorium, now joined by 25 members. In addition, the WTO E-Commerce Agreement includes a permanent moratorium as do several bilateral trade agreements, including the U.S. agreements on reciprocal trade. We strongly urge USTR to proactively monitor and vigorously challenge any trading partner that takes steps to impose customs duties on electronic transmissions, support a multilateral moratorium in the future, should consensus arise, and continue to build support for the plurilateral arrangement in the interim.

Access to AI Training Materials: Access to vast and diverse datasets, including publicly available information from the open web, is fundamental for building responsible, accurate, secure, and effective AI systems. This access is the lifeblood of AI progress. AI innovation fundamentally depends on the ability to learn from the widest possible variety of publicly available material. This allows the AI models to identify features, relationships, and patterns between and among data points. This extensive training on billions of data points helps the models learn, understand diverse perspectives, and guard against bias. To ensure AI's benefits are fully realized while addressing concerns about human creativity, establishing balanced copyright frameworks that do not restrict the fundamental learning process of AI models is crucial.

However, this essential ecosystem for AI innovation is threatened by a growing number of countries contemplating or adopting restrictive copyright policies that would serve as significant trade barriers. Nations such as Brazil are pursuing regulations that would severely limit or impose impractical licensing requirements on the use of copyrighted works for AI training. Even in the absence of formal legislative proposals, ongoing policy debates in Australia, Canada, and the UK are concerning. Within these discussions, stakeholders are challenging established copyright norms and raising fundamental questions about the use of local online content for AI training, which could have implications for AI model development, even when it occurs within the U.S. These approaches risk stifling innovation and disadvantaging developers who abide by international norms. We urge the U.S. government to protect AI innovation against the introduction or enactment of restrictive copyright frameworks in foreign markets,

which risks creating barriers to AI innovation, market access and deployment.

Country-by-Country Trade Barriers

Argentina

Import Policies

Express Shipments: Argentina operates two distinct express shipments regimes, each designed to accommodate different types of shipments with varying requirements and restrictions on weight, value, item count, and frequency of use. The coexistence of the two models and the count and value limitations create constant friction at customs clearance, increasing processing times and imposing disproportionate compliance burdens on U.S. companies. Under the Small Shipments Regime, individuals are limited to five duty-exempt shipments per calendar year, each capped at three units of the same commodity, a maximum weight of 50 kg, and a value not exceeding \$3,000 FOB. Shipments valued below \$400 FOB are exempt from customs duties and the statistical fee, though VAT (21%) still applies; shipments exceeding the five-shipment annual quota are subject to full customs duties (averaging 40%+) and VAT on the entire value, including the portion below \$400. This quota-based system creates significant operational challenges for U.S. companies, as they cannot access information to track quotas. The Customs and Trade Facilitation commitments contained in Annex III of the U.S.–Argentina Agreement on Reciprocal Trade and Investment (ARTI), signed on February 5, 2026, and amended on October 14, 2026, directly address these barriers. Article 1.22 commits Argentina to removing limitations on weight, value, item count, and frequency of use for simplified procedures applicable to express shipments, while Article 1.24 requires all border agencies to complete pre-arrival data processing to enable immediate release of low-risk shipments without diversion to bonded facilities. NFTC wants to ensure the Argentine Congress ratifies its ARTI, and in doing so takes all necessary policy actions to address these barriers through the implementation of changes to fully implement the express shipment provisions of the agreement.

Customs Treatment of Express Delivery Services: The absence of legal recognition for "International Express Service Providers" within Argentina's outdated Customs Code (Ley 22.415) constitutes a significant non-tariff barrier. Express operators are forced to clear time-sensitive shipments under incompatible legacy categories. This prevents the adoption of expedited clearance procedures used by regional peers, severely restricting supply chain modernization. This regulatory exclusion places U.S. companies at a distinct competitive disadvantage and restricts cross-border e-commerce growth. NFTC recommends that USTR press the Government of Argentina to formally integrate a dedicated Express Delivery Chapter within its ongoing Customs Code reform efforts. Ensuring local regulations align with modern international logistics standards is critical to facilitating seamless digital trade, removing unnecessary friction for U.S. exporters, and integrating Argentina into efficient global supply chains on par with its regional neighbors.

Implementation of Electronic Prearrival Clearance Commitments: Argentina has consistently failed to operationalize key trade facilitation commitments established under the bilateral Agreement on Reciprocal Trade and Investment. A primary concern for the U.S. logistics sector is the absence of a functional, integrated electronic prearrival clearance system. Current Argentine customs procedures mandate that inbound cargo must physically land and undergo ground processing before any formal clearance activities can commence. This negates the speed advantages inherent to express shipping, causes severe terminal congestion, and contradicts international best practices, undermining the core

objectives of the bilateral framework and delaying time-sensitive exports.

NFTC recommends that USTR utilize joint bilateral meetings to formally request a binding, transparent implementation timeline for electronic prearrival clearance capabilities. Establishing these automated processing pathways is indispensable for reducing transit times and lowering the administrative costs borne by American businesses. Fulfilling Argentina's bilateral trade facilitation obligations through modernized IT infrastructure is absolutely critical to ensuring that American exporters can compete effectively and efficiently within the expanding South American digital economy.

Barriers on Electric Equipment Imports: Argentina recently established new legislation on regulatory requirements for electric equipment. The new regulation was broadly advertised as positive, since international certificates are now accepted, as long as the importer is formally authorized by the international certificate holder, dismissing the need for local certification. However, the change did not incorporate the exceptions previously extended to companies importing the equipment for internal use. Subsequently, the change imposed new barriers to these importers, as the process to obtain the international certificate, identify the certificate holder, and obtain authorization is much more cumbersome than the previous possibility to present a sworn statement.

Technical Barriers to Trade

New Health Technology Assessment (HTA) Agency Potential as Market Access Barrier: In March 2025, the Argentine government announced the creation of the National Agency for the Evaluation of Health Technology Financing (ANEFiTS), which would operate under the Ministry of Health and conduct cost-effectiveness economic evaluations of all new technologies seeking registration in Argentina. The agency could determine that a product, even if approved by the FDA and marketed in the U.S. and worldwide, cannot apply for marketing authorization in Argentina because "its cost could be high for the system as a whole." This newly proposed HTA agency would establish an unprecedented non-tariff barrier to innovative medicines by allowing cost-effectiveness assessments to potentially block companies from seeking marketing authorization. USTR should urge that the scope and operational criteria used by ANEFiTs are aligned with international technical and transparency standards.

Government Procurement

Cloud Procurement Limitations: Argentina's public sector lacks a standardized framework for cloud service procurement, creating a market access barrier through lengthy, inefficient processes that deter cloud adoption and burden providers, particularly affecting U.S. technology companies serving public sector entities. The Secretaría de Innovación, Ciencia y Tecnología has been developing a public-sector cloud framework agreement (acuerdo marco) to standardize and streamline procurement from qualified providers, including international cloud service providers. Argentina should finalize this framework with flexible resource allocation and streamlined approval procedures to facilitate market access and efficient cloud adoption.

Intellectual Property Protection

Patentability of Pharmaceutica Inventions: The ARTI has already produced meaningful reforms. In March 2026, Argentina repealed the restrictive pharmaceutical patentability guidelines established by Joint Resolutions 118/2012, 546/2012, and 107/2012, and in June 2026, INPI repealed Resolution 283/2015 on biotechnological inventions. Patent applications are now to be examined case by case under the general standards of Patent Law 24,481. These are welcome steps. However, Joint Resolution 1/2026

also provides that holders of newly granted patents covering pharmaceutical products already marketed in Argentina by third parties may neither prevent continued marketing of those products nor seek compensation, which significantly limits the value of patents granted under the reformed framework. In addition, the 2015 amendments to INPI's patent examination guidelines that incorporated the 2012 criteria were not expressly addressed in the repeal. Argentina should ensure that patent rights granted under the new framework are fully enforceable, confirm that the 2012 criteria no longer apply in any form, and provide clear, predictable examination practices consistent with international standards.

Lack of Regulatory Data Protection (Pharmaceuticals): Argentina still lacks an adequate and effective system of regulatory data protection. Under Law 24,766 and Decree 150/92, follow-on products may obtain marketing approval by reference to the prior approval of an innovator's product in Argentina or in designated reference countries, effectively relying on clinical data generated by U.S. innovators without their consent. Under the bilateral agreement, Argentina committed to analyze the feasibility of a regulatory data protection regime consistent with Articles 20.45 and 20.48 of the USMCA. Argentina should complete this analysis promptly and transparently, with meaningful stakeholder input, and move to establish protection against the unfair commercial use of undisclosed test and other data that meets the USMCA standard referenced in the agreement.

Argentina also remains the only major economy that has not yet joined the Patent Cooperation Treaty (PCT). We understand that steps have been taken in the Argentine Congress to support PCT accession in accordance with the ARTI.NFTC urges USTR to work with Argentina to ensure that they formally join this foundational treaty to benefit American and Argentine innovators alike.

Services Barriers

Personal Data Transfer Restrictions: Argentina currently does not recognize the United States as an adequate jurisdiction for personal data transfers, creating a significant trade barrier for US companies. While data flows freely to EU member states, European Economic Area (EEA) countries, and jurisdictions with EU adequacy decisions, transfers to the US require additional safeguards through contractual clauses, reflecting Argentina's alignment with EU data protection standards and the absence of U.S. federal privacy legislation. This increases operational complexity, compliance costs, and implementation delays. The U.S.–Argentina Digital Trade and Innovation Agreement, signed February 5, 2026, contains a commitment to recognize the United States as an adequate destination; although it has not yet been ratified by Argentina's Congress, the government could nonetheless advance this recognition. A resolution would require modification of Disposition E60/2016 AAIP to include the United States as an adequate jurisdiction, or recognition of U.S. Data Privacy Framework (DPF) certified companies as meeting adequacy requirements.

Data Localization for Public-Sector Disaster Recovery (CNC Disposition 01/2026): On May 13, 2026, Argentina's Centro Nacional de Ciberseguridad (CNC) issued Disposition 01/2026, mandating that all National Public Sector entities maintain a backup/disaster-recovery data center within Argentine territory, located at least 1,500 km from the primary site and holding Tier 3 certification. These requirements have no precedent in OECD or G20 frameworks and cannot be met by internationally competitive U.S. cloud providers. The measure functions as a data localization mandate that forces entities away from modern cloud architectures toward inferior on-premises infrastructure and risks entrenching the state-owned operator (ARSAT) as the sole compliant provider. It was issued without public consultation and is in tension with Argentina's non-discrimination commitments under the ARTI. Argentina should adopt technology-neutral, outcome-based disaster-recovery requirements that recognize cloud multi-region resilience as compliant, and remove the in-country residency, fixed-distance, and

physical-building certification mandates.

Australia

Technical Barriers to Trade

Market Access (Pharmaceuticals): Australia undervalues new innovative medicines by setting prices based on older inferior medicines and generics and through biased health technology assessments that rely on low and outdated monetary thresholds per year of life gained from clinically proven treatments. Moreover, the Pharmaceutical Benefit Scheme (PBS) often restricts access to a small subset of the patient population for which the product was proven safe and effective and creates access delays through unnecessary data requirements and other administrative hurdles.

Data Center Frameworks and AI Standards: Australian state and federal governments have moved to impose new regulatory requirements on data center developers. In August 2026, New South Wales released a Data Centre Policy Framework. In September 2026, Victoria released a Sustainable Data Centre Action Plan, and the Australian Government released a consultation paper proposing mandatory national minimum standards for large data centers, under legislation expected in early 2027. The proposed standards include requirements to demonstrate meaningful community engagement, draw on local suppliers, and actively support workforce training, and separately propose conditions requiring entities undertaking frontier AI training in Australia to contribute to local research, innovation and capability, including by making compute available to Australian start-ups, researchers and small businesses on favorable terms. The development of these aspects should be monitored to ensure they do not operate as de facto local content requirements or impose disproportionate costs on U.S. cloud service providers, which account for the majority of data center investment in Australia.

Intellectual Property Protection

Inadequate patent notification arrangements: In the Australia-US Free Trade Agreement, Australia agreed to make necessary arrangements for notification to the patent owner if another party submits a medicine for marketing approval during the term of an existing patent, though action has not been taken to bring such an arrangement into existence. Instead of notifying the patent holder when a potentially infringing generic or biosimilar product commences the registration process, the patent holder only becomes aware of the potential infringement by carefully monitoring new additions to the Australian Register of Therapeutic Goods (ARTG). Immediately following the launch of the competitor's product, the reimbursed price of the originator product reduces by 25%. The patent holder is left with an emergency injunction as their only recourse to prevent launch while assessing the validity of their patent and litigation is pending, which is costly for parties and time consuming for the courts. The introduction of legislative reform requiring effective notification of generic and biosimilar applications submitted to the Therapeutic Goods Administration (TGA) to originator pharmaceutical companies and an effective mechanism for the early resolution of patent disputes before an infringing product is launched in Australia.

Insufficient regulatory data protection: Australia provides a 5-year period for regulatory data protection for both small molecule and biologic products which is substantially shorter than the regulatory data protection provided in many other countries for biologic products. This creates a disincentive to registration of products in Australia as originators can't be assured that their research will be protected. This is particularly challenging for biologics where unlike traditional chemical compounds, the generic version of the biologic is not exactly the same as the originator – this means patent protection alone is

insufficient. Australia should adopt a period of regulatory data protection that is in line with global best practice and provides adequate protection to products like biologics which are insufficiently protected by patents alone. Australia should also extend regulatory data protection for new indications, new formulations, new patient populations and new dosage forms would result in consistency with other markets.

Market-size damages: The Australian Government has sought “market-size” damages from patentees that have legitimately but ultimately unsuccessfully pursued patent infringement actions. These damages purportedly compensate the PBS for the effect of any delay in the PBS price reduction due to a preliminary injunction on generic launch which is ultimately lifted if the patentee is unsuccessful. These so-called “market-size damages” create significant uncertainty for pharmaceutical patent owners. It also undermines the rights of patent holders in Australia by introducing a strong disincentive to exercise their core right to enforce their IP protections and is inconsistent with Australia’s international commitments under the AUSFTA and the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

Services Barriers

Digital Duty of Care: In September 2026, the Australian Government released an exposure draft of an Online Safety ‘Digital Duty of Care’ Bill that would introduce a broad statutory obligation requiring providers of online services to ensure, so far as is reasonably practicable, a safe online environment. The duty would apply to social media platforms, search engines, hosting services, app distribution services and AI content generation tools, and would require providers to conduct annual risk assessments covering content, algorithmic recommendation systems and product design features. The regime would be enforced, with civil penalties of up to approximately AUD\$109 million (US\$78 million) for non-compliance. The Australian Government has indicated that AI companies, including providers of generative AI services, would be captured by the proposal. Legislation is expected to be introduced to Parliament in 2027. The scope of this legislation should be monitored to ensure the definition of regulated online services does not disproportionately capture U.S. technology companies or impose compliance obligations that function as barriers to market access.

Audiovisual Services: On November 25, 2025, Australia enacted the Communications Legislation Amendment (Australian Content Requirement for Subscription Video On Demand (Streaming) Services) Bill 2025. The law requires subscription video on demand (SVOD) services with more than 1 million Australian subscribers to invest at least 10 percent of their total program expenditure for Australia or 7.5 percent of their Australian revenue on new Australian drama, children’s, documentary, arts, or educational programs. To qualify as Australian, a production must meet the standard set out in the Australian Content Standards 2020 (ACCTS), which requires that certain key creatives and specified percentages of actors are Australian and that the program is produced and post-produced in Australia. The vast majority of the expenditure under the law will be by U.S. companies. An industry report estimated that, in the first five years, the law would require U.S. companies to spend \$1 billion (or \$200 million per year) on new eligible Australian content.¹ The law raises serious questions under the U.S.-Australia Free Trade Agreement.

Ex-ante Regime for Digital Services: In December 2024, AU Treasury launched its long-anticipated consultation on a new ex-ante regime for digital services. The proposed framework adopted aspects of

¹ <https://ccianet.org/wp-content/uploads/2025/12/Australias-VOD-%20Law-Poses-Key-Trade-Barriers-for-U.S.-Streaming-Services.pdf>

both the EU DMA and the UK DMCCA, which would allow the AU Government to designate digital platform services to broad obligations on matters such as self-preferencing and data use, as well as ‘service-specific obligations’. The initial proposal would trigger new compliance obligations around preventing self-preferencing, ensuring interoperability, and prohibiting manipulative design practices. The proposal identifies ‘priority services’ for designation as app marketplaces, ad-tech services and social media, although a wide range of digital services were flagged for future consideration, including general online marketplaces, virtual assistants and, potentially, cloud. Designation would also allow the ACCC to recommend service-specific (platform-specific) obligations. The scheme, if advanced, would raise similar trade-related concerns to the DMA, particularly if only US-headquartered companies meet the criteria for designation (which is possible given the initial sectors identified).

News Media-Related Digital Service Taxes: In August, 2026, the Australian government enacted the News Media Bargaining Incentive, requiring firms that earn more than A\$250m in annual Australian digital advertising revenue to enter into commercial deals with media organizations, or risk being hit with a 2.75% charge on that revenue. The new rules target digital companies, predominantly US firms, by applying only to platforms with over 5 million active social media users or 10 million active search users in Australia. While this has been described as an "incentive" rather than a "tax," the new rules apply regardless of whether a firm carries news as a service, and amounts to a targeted and highly discriminatory DST.

Content Regulation: Australia’s 2021 Online Safety Act empowers the Safety Commissioner to demand removal of “harmful” content, including adult cyber abuse. Under the Act, industry codes of conduct and standards for eight online sectors were developed to implement the requirements under the Act. Additionally, as of December 2025, Australian regulators have implemented a mandatory minimum age requirements of 16 for using certain social media platforms. Industry concerns with the overall regime include: strict investment requirements for content detection and removal; the ill-defined concept of “harm” leading to censorship of lawful content; and overbroad restrictions limiting creativity, valuable online experiences for minors, and freedom of expression and information.

Tranche 2 Privacy Act Reform: On August 31, 2026, the Australian government released a Consultation Paper² and an Exposure Draft³ of the Privacy Amendment (Personal Data Protection) Bill 2026, which proposed amendments to the Privacy Act 1988. The changes introduce a very broad concept of “trading” in personal information impacting third party behavioral ads relying on ad-tech: A new “trade in personal information” regime covers sharing personal data for money or in ways that support “direct marketing”, which includes many standard ad-tech flows. These trades are expected to require opt-in consent, which could materially affect how companies work with third-party ad-tech partners, unless the reforms more specifically targets ‘trade brokers’. The other significant change is an establishment of deletion rights for large platforms that could extend beyond members to business-to-business data. Large online platforms that meet this statutory definition would be required to delete personal data on request within a “reasonable period”, subject to limited exceptions.

Other Barriers

Taxation Ruling on Royalties – Character of Receipts in Respect of Software: On September 4, 2026, the Australian Tax Office (ATO) finalized its software royalty ruling (TR 2026/2) and released an expanded draft Practical Compliance Guideline (PCG 2026/D4). Like the previously proposed Draft

² https://consultations.ag.gov.au/rights-and-protections/privacy-reform/user_uploads/consultation_paper.pdf

³ https://consultations.ag.gov.au/rights-and-protections/privacy-reform/user_uploads/exposure-draft-bill-2026.pdf

Taxation Ruling TR2024/D1, TR 2026/2 treats certain outbound payments by in-country distributors of software as royalties subject to Australian withholding tax. This ruling is contrary to long-standing internationally accepted treaty interpretation, including paragraph 14.4 of the Commentary to Article 12 (Royalties) of the OECD Model Tax Convention. ATO's approach contemplated in the Draft Taxation Ruling was recognized in two letters from the US Treasury Department to the Australian Treasury Department, sent in August 2022 and April 2024, respectively, which highlighted that the approach violated well-settled norms, including the OECD Commentary, and threatened to "create a concerning imbalance in the benefits provided by the Australia-U.S. tax treaty." This approach by ATO is largely unchanged in the final ruling. Such a withholding tax would have similar anti-competitive and discriminatory effects as a digital services tax (DST) with respect to US software companies and others that sell software products and services (including cloud services) into the Australian market. USTR is urged to use all of the available tools in the toolbox to resolve this issue.

Country-by-Country Reporting: ATO's stringent public country-by-country reporting (CbCR) requires U.S. enterprises to give an annual Public CbCR to the Australian government. Public CbCR requires U.S. parents to disclose global revenues, profits and income taxes; the activities of the global group; and an entity's international related party dealings among other information. This is dissimilar from the EU regime which requires the information from the EU subsidiary, not the U.S. parent.

The law provides for a "blacklist," which requires that global reporting must be disaggregated for '[specified jurisdictions](#)', which includes American Samoa and the U.S. Virgin Islands. NFTC has significant concerns regarding this in terms of its privacy and competitive implications as well as its encroachment on U.S. sovereignty. When combined with other publicly available filings, such disclosures would compromise the privacy of individual U.S. business owners, business practices, and provide a roadmap for competitors and foreign adversaries to exploit. U.S. companies will bear a disproportionate burden from the extraterritorial reach of this mandate, as their worldwide operations, including sensitive information shielded under US law, will be publicly exposed through the Public CbCR on ATO's website.

Azerbaijan

Services Barriers

In November 2025, the Central Bank of the Republic of Azerbaijan (CBAR) introduced regulations revising the Regulation on Conducting Payment Operations and on Payment Instruments. The new regulations limit the use of tokenized e-commerce payment solutions for domestic online transactions. These restrictions are housed in Article 3.18 of the new regulations, which states that "Direct information exchange may be conducted between providers and payment system operators and payment system operators operating outside the country regarding transactions carried out within the country (except for domestic transactions in which the value of goods, works, or services is paid through electronic commerce), provided that such transactions cannot be executed without such an exchange."

CBAR did not publicly disclose nor allow for consultation on this provision before adopting these rules. Prior consultations into these proposed amendments did not include this language or similar restrictions on tokenized payment solutions for e-commerce.

Previously, Azerbaijan required non-tokenized domestic transactions to be processed through the local switch, but permitted tokenized transactions to utilize the infrastructure of international payment networks where the domestic switch did not support the necessary functionality. This framework enabled the

successful introduction of tokenized payment solutions such as Apple Pay and Google Pay into the Azerbaijani market, while the government continued to pursue its broader domestic processing objectives. The current restrictions represent a departure from Azerbaijan's established approach.

The domestic switch does not currently support the EMV tokenization protocols required for solutions such as Click to Pay. Click to Pay is an industry solution developed under the EMV Secure Remote Commerce (SRC) standard and supports services offered by several industry participants; therefore, this barrier negatively impacts the U.S. business community beyond Visa. Further, these restrictions directly benefit the Azerbaijani infrastructure operators, as the transactions get routed to a local switch as opposed to international networks, such as Visa and other similar solutions. Market participants have also been unable to proceed with planned deployments using alternative processing arrangements. As a result, Azerbaijani banks, merchants, payment service providers, and consumers are unable to access a secure digital commerce solution that is already being adopted in markets around the world. Not only does this barrier restrict U.S. EPS companies from operating in Azerbaijan by hindering this internationally accepted security standard, but these restrictions directly benefit the Azerbaijani infrastructure operators, as the transactions get routed to a local switch as opposed to international networks. By barring tokenized transactions, the regulations ensure that these transactions instead go through the local switch, which increases the payment volumes while contravening international standards. USG should engage Azerbaijan to ensure the government accords transparent, technology-neutral, and non-discriminatory regulatory treatment of U.S. electronic payment services companies (EPS) in Azerbaijan. U.S. EPS companies should be allowed to operate and process globally recognized tokenization-based payment solutions based on internationally-accepted standards. This includes secure e-commerce technologies that are not yet supported by local payment infrastructure in Azerbaijan. This should be permitted on a non-discriminatory basis, while maintaining appropriate regulatory oversight, consumer protection requirements, and domestic policy objectives.

Bangladesh

Import Policies

Illicit Trade: Illicit trade is becoming a more substantial challenge for U.S. companies operating in the region. One particular issue of concern is the increase in illicit trade crossing the border between India and Bangladesh. NFTC urges USTR to encourage intensive training, strategic deployment of resources, and greater partnership between Indian and Bangladeshi authorities. In addition, authorities should take greater action against websites selling illicit medicines and local distributors facilitating their spread.

Services Barriers

Data Localization Requirements: In October 2025, the Cabinet of the Interim Government of Bangladesh passed the Personal Data Protection Ordinance (PDPO) and the National Data Governance Ordinance (NDGO), with little industry consultation on the former and none on the latter. The [PDPO](#) contains concerning criminal liability and extraterritorial provisions, as well as data localization requirements for certain types of restricted data. Classified data (confidential and restricted) must be stored within Bangladesh's jurisdiction. Transfer of internal and confidential data abroad is allowed with consent or under specific contractual or interest-related conditions, and only to countries with suitable data protection technology and equipment. Most of the PDPO comes into effect immediately. However, Section 23 (Chief Data Officer) and Sections 31- 46 (Complaint Filing, Administrative Penalties, and Criminal Offences and Penalties) will only come into effect at a later date which is the earlier of: (1) the date specified by the Government through a gazette notification, and (2) 18 months from the date of

issuance of the PDPO.

Local Licensing Requirements: In November 2025, Bangladesh Bank (BB) Draft Payment System Operator (PSO) Regulation 2025 proposed bringing all payment ecosystem participants, including international card schemes (ICS), under a single PSO regime. Key risks for ICS include (amongst others) mandatory local incorporation, PSO licensing, domestic processing and storage of cardholder and transaction data.

In June 2026, BB published an updated PSO framework that introduced a carve-out for ICS. While the framework itself is no longer applicable to ICS, the carve-out included separate obligations for ICS. These requirements include licensing, local incorporation and data localization, amongst others, which could significantly impact ICS's cross-border operating model by requiring the establishment and maintenance of a locally incorporated entity, localization of certain data and operational functions, and potential duplication of infrastructure and compliance processes. These obligations would increase operational complexity and costs, reduce efficiencies derived from global network architecture, and create barriers to the seamless provision of international card scheme services in Bangladesh.

USTR should urge Bangladesh to ensure that regulatory requirements applicable to international payment networks are transparent, proportionate, and consistent with international practice, including by (1) exempting international card schemes from Bangladesh Bank licensing and local incorporation requirements; (2) permitting cross-border payment processing and data flows without localization mandates; (3) ensuring regulatory data requests are targeted, proportionate, and tied to a legitimate supervisory purpose; (4) recognizing global scheme rules governing dispute resolution, liability allocation, and participant obligations; and (5) removing notification requirements that could delay the deployment of security, fraud-prevention, and other value-added services.

Bolivia

Services Barriers

Data Localization Requirements: Bolivia maintains restrictive data localization requirements for the public sector through its Electronic Government Plan and its Open Software and Open Standards Implementation Plan (PISLEA 2025-2030), which remain in force. Public sector entities must store ‘non-public’ government data within Bolivian territory, effectively preventing international cloud providers from offering storage services to government institutions. While recent updates allow cloud services for ‘public’ data and certain operations (such as processing) on ‘non-public’ data, storage of ‘non-public’ data must remain local, and the absence of clear definitions of ‘public’ and ‘non-public’ data creates significant legal uncertainty. Bolivia should adopt internationally recognized data protection standards that permit cross-border data flows and apply risk-based approaches rather than blanket localization requirements.

Financial Sector Regulations: Bolivia’s Financial System Supervision Authority (ASFI) maintains one of the most restrictive cloud-adoption regimes in the region for financial institutions. Under its Information Security Management Regulations—updated in June 2026 by Circular ASFI 955/2026 (amending Circular ASFI/660/2020)—institutions must obtain a prior ‘no-objection’ before contracting cloud services, a requirement defined so broadly (covering personal data, financial or accounting information, or substitution of critical infrastructure) that it captures nearly all cloud contracts. Each service must also be backed by an implementation project approved by the Board of Directors, and the regulation imposes prescriptive mandatory contractual clauses, annual verifications, and a permanent on-

premises alternate processing center regardless of cloud adoption. Neighboring countries (Argentina, Brazil, Chile, Colombia, Peru, and Paraguay) require only notification. Bolivia should replace prior approval with a notification mechanism with clear timelines and checklists, accept internationally recognized certifications (e.g., ISO 27001, SOC) in lieu of per-contract documentation and on-site audits, and eliminate the mandatory on-premises alternate site where the provider offers native cross-zone redundancy.

Brazil

Import Policies

Prohibition on the Import of Refurbished Products: Brazil maintains import prohibitions on certain used ICT products. This policy is unfair, because refurbished products and components are “like new” products and should not be banned. U.S. companies are required to continue supporting customers with products that are under warranty, especially when such products have reached end-of-sale, and components are no longer available as new products.

Customs Classification Requirements for Express Shipments: Brazil continues to pursue customs initiatives that require increasingly granular tariff classification information for low-value, low risk express shipments. Recent discussions within Brazilian Customs contemplate requiring full 8-digit NCM classification at the shipment level for air express cargo. The proposal has been advanced with little to no formal consultation with affected stakeholders, outside of a transparent regulatory process, without an implementation grace period, and with extremely short lead times following only informal communications to industry. Such practices reduce regulatory certainty and limit meaningful private-sector engagement in the development of measures with significant commercial impact. If implemented, the requirement would impose substantial operational and compliance burdens on U.S. express carriers and exporters, increase costs, create delays in customs clearance, and undermine trade facilitation objectives. Given the high-volume and time-sensitive nature of express shipments, Brazil should instead pursue risk-based approaches and streamlined data requirements consistent with international express delivery practices and the WCO trade facilitation principles.

Technical Barriers to Trade

Incorporation Delays in Public Market (Medicines and Vaccines): Innovative medicines and vaccines face significant market access barriers in Brazil due to prolonged incorporation delays in the public market. Gaps between a positive incorporation decision and effective availability to patients. CONITEC, Brazil's health technology assessment body, evaluates the incorporation of new medicines and vaccines into the Unified Health System (SUS). This process and its associated timelines are regulated by legislation. If a medicine or vaccine is approved by CONITEC, it must be made available to patients within 180 days. However, data shows that 25% of the medications incorporated between 2019 and 2024 are still not available to the population. Out of the 143 medications approved by CONITEC, 36 are awaiting the completion of the procurement process. These implementation gaps create uncertainty for manufacturers and delay access to health technologies that have already received a positive incorporation decision.

Intellectual Property Protection

Misalignment with International IP Standards (Pharmaceuticals): Brazil does not currently provide a

statutory patent term adjustment mechanism to compensate for administrative delays in patent examination. In addition, the country does not offer a specific regulatory data protection regime for pharmaceutical products intended for human use, despite comparable protections being available for veterinary and agricultural products. The absence of these mechanisms may reduce legal certainty and predictability for the significant investments required to generate clinical and regulatory data and to support the development of innovative medicines. While Brazil has taken important steps in recent years to improve patent examination efficiency, continued efforts to strengthen the intellectual property environment could further support research, innovation, and timely access to new therapies for Brazilian patients.

Lack of regulatory data protection (RDP): Brazil does not provide RDP for biopharmaceutical products (despite applying RDP for veterinary, fertilizer, and agrochemical products).

Compulsory licensing: Members of Brazil's National Congress continue to pursue efforts to expand inappropriately compulsory licensing provisions in Brazil's Industrial Property Law. Some of these efforts included several unprecedented, vague, and broad provisions that go beyond what was envisioned under the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). These efforts fundamentally undermine the predictability and certainty necessary for U.S. innovators from all sectors to successfully invest in and accelerate the launch of new products in Brazil.

Services Barriers

Data Localization Requirements: Brazil's General Data Protection Law (LGPD), enacted in 2018 and fully effective from 2021, establishes specific conditions for international transfers of personal data. Unlike some jurisdictions, the LGPD does not permit international data transfers solely on the basis of a controller's legitimate interests and instead relies on the legal mechanisms expressly provided in the law. In 2024, the National Data Protection Authority (ANPD) issued Resolution No. 19/2024, establishing a framework for international data transfers, including standard contractual clauses, specific contractual clauses, binding corporate rules, and adequacy decisions. While this regulation increased legal certainty, stakeholders continue to monitor the implementation of the adequacy framework, as no foreign jurisdictions have yet been formally recognized by the ANPD as providing an adequate level of data protection.

AI Bill: The pending legislation (PL 2338/2023) would create substantial barriers for U.S. AI services by implementing broad regulations that fail to distinguish between high- and low-risk applications. The bill's lack of clear differentiation between AI developers and employers creates operational uncertainty for the entire AI value chain. Most significantly, it would require payment for Brazilian content used in AI model training and could effectively prevent U.S. companies from developing or deploying their generative AI features in Brazil.

Bill 2338/2023 (September 2026), authored by then-Senate President Rodrigo Pacheco, was approved by the Federal Senate in December 2024 and sent to the Chamber of Deputies. Per the Chamber's official process, the bill is under review by a Special Committee where it awaits the rapporteur's report; numerous related bills have been appended to it. Public hearings and regional seminars have taken place, but no committee or floor vote has occurred, and the bill remains unenacted as of September 2026. The rapporteur is expected to present the report following the elections in October. Separately, Brazil continues to build out AI-specific institutions and sector draft rules (e.g., AI data-center bills such as PL 3018/2024), which could compound compliance burdens on U.S. cloud and AI providers if the framework

is enacted.

Ex-Ante Competition Legislation: In September 2025, the Brazilian Government introduced competition legislation (Bill 4675/2025) modeled after the European Union's Digital Markets Act (DMA) and the United Kingdom's Digital Markets, Competition, and Consumers Act (DMCCA). The bill would apply to a small group of predominantly U.S. companies while sparing local incumbents and most Chinese competitors.

The proposed framework grants Brazil's Administrative Council for Economic Defense (CADE) broad powers to regulate digital services through a newly created Special Superintendence for Systemic Relevance, Free Competition and Consumer Protection in Digital Markets. This body would designate companies as "systemically relevant" and determine and apply special obligations to designated companies on a case-by-case basis. The bill provides CADE broad authority and open-ended criteria to designate companies, including a revenue threshold of R\$50 billion globally or R\$5 billion in Brazil, combined with qualitative characteristics including — but not limited to — operating multi-sided platforms and access to significant amounts of personal and business user data. The Finance Ministry has consistently stated that no more than 5–10 companies would be designated, and that these will include the DMA's "gatekeeper" companies — which are largely U.S. companies (e.g., Amazon, Apple, Meta, and Microsoft).

CADE would determine and apply special obligations following an administrative proceeding, which could include a ban on self-preferencing, mandated free data transfers and interoperability, and requirements to allow the installation and use of third-party applications without restriction. CADE is not required to demonstrate that its obligations are proportional to the problems identified. The bill requires only that CADE show its remedies are necessary to "protect and promote competition" — objectives so broad and undefined that they would allow CADE to justify virtually any intervention. Designation lasts for up to six years and applies to the entire company, while special obligations may be limited to a specific service or product. Failure to comply would result in penalties ranging from fines of up to 20% of gross revenue to company break-up.

This asymmetric regulatory treatment would cost U.S. companies hundreds of millions of dollars in compliance and potential fines that Brazilian and Chinese companies would not bear, undermining their ability to compete in Brazil, affecting U.S.-based jobs across the value chain, and diverting resources from U.S. research and development. Industry groups have estimated compliance costs of roughly R\$11 billion (approximately US\$2.2 billion) over ten years.

The bill was granted expedited under "urgency mode" authorities, which bypasses committee analysis and debate and allows it to be brought directly to the House floor for a vote at any time. The Government and the floor rapporteur have signaled they want the bill to pass by the end of 2026, despite the lack of consensus in Congress on competition legislation — notably, Bill 2768, a separate competition bill targeting digital services, passed the Chamber's Economic Development Committee in August 2026 and outlines a significantly different approach to addressing competition concerns in the digital space.

Network Usage Fees & Network Regulation: In 2026, Brazil continues to consider measures to apply ill-fitting or cumbersome regulations to value-added services, such as video-on-demand, streaming, social media, cloud, or other over-the-top services (OTTs). Brazil's Telecommunications Agency (ANATEL) is interested in imposing a network fee that a small group of U.S. content providers and technology companies would have to pay to large internet service providers to fund telecommunications infrastructure. This would disproportionately affect U.S. companies and essentially force them to

subsidize competitors while undermining the value of their existing infrastructure investments. ANATEL resumed discussions in March 2026 with a new Request for Comments to gather input from market participants, and its scope now appears broader— extending to digital infrastructure and traffic flows, including the role of Content Delivery Networks (CDNs), interconnection models, and traffic localization. ANATEL’s intent appears targeted at large international providers while potentially exempting smaller local competitors. This approach could set a concerning precedent for other markets and significantly impact U.S. companies' ability to invest in Brazilian digital infrastructure.

Digital Services Tax: Despite multilateral efforts to align international taxation rules, the Brazilian Congress continues to introduce bills aimed at creating unilateral Digital Services Taxes (DSTs) that would directly affect U.S. companies operating in the country. USTR has already found that similar measures, such as France’s DST, are actionable under Section 301. The implementation of these unilateral tax measures not only risks jeopardizing multilateral negotiations but also threatens U.S. businesses that fully comply with Brazil’s taxes and should receive equal treatment compared to local companies. The Brazilian Congress is currently considering seven DST bills, and on July 18, President Lula publicly expressed support for such initiatives to charge taxes from U.S. digital service providers. The seven DST proposals in Brazil’s Congress conflict with Brazil’s existing tax system, which already taxes profit remittances abroad, and contradict Brazil’s ongoing tax reform efforts that aim to tax both digital and physical products and services equally. An additional tax exclusively targeting the revenue of multinational companies, that in practice will end up burdening mostly U.S. companies, would effectively create double taxation and unfairly disadvantage American companies competing with local providers offering identical services to Brazilian customers. The disproportionate nature of these bills is evident in data from Brazil’s Federal Tax Authority from 2018 to 2022, which shows that digital services in Brazil generated average tax revenue of 16.4%, while non-digital private sector services contributed only 6.1% on average. The Brazilian government should focus its efforts and resources on achieving consensus through multilateral forums rather than implementing unilateral taxes that will discriminate against U.S. companies doing business in Brazil.

Copyright Taxes on Digital Platforms: Two significant legislative proposals in Brazil that could alter the copyright landscape for digital services and impose discriminatory taxes and obligations on U.S. technology companies:

- Bill 4968/24 (Senate, Dec 2024, Sen. Rodrigues) proposes a new remuneration right for copyright and related rights holders for content used by online platforms. A critical provision of this bill would mandate payment even in cases of unauthorized third-party uploads or where existing contractual agreements already permit the use of the work, introducing significant financial and operational risks for user-generated content platforms.
- Bill 2370/19 (Chamber of Deputies, Cong. Feghali) mirrors Bill 4968/24, aiming for broad copyright reform with uncapped liability and "must-carry" obligations for journalistic/artistic content, preventing platforms from avoiding payment by content removal.

Audiovisual Services: Brazil currently applies a Condecine tax on a per-title basis to films, pay-TV, and “other segments.” This tax does not apply to video on demand (VOD) services. However, there are several bills – most notably #8889/2017 and #2331/2022 – pending in the Brazilian Congress that would introduce a Condecine tax on streaming services through progressive revenue-based schedules — reaching 4% for video-on-demand and internet television services and 0.8% for audiovisual content-

sharing services, including U.S. social media services hosting user-generated content — with a 75% tax reduction for qualifying services whose offerings contain more than 50% Brazilian content. The bill also imposes other obligations on VOD services, including a phased catalogue quota for Brazilian works reaching 10% (or an alternative of 700 Brazilian works, half independent), prominence for local works, prominent placement of Brazilian broadcasters on connected TV interfaces, a requirement that providers above R\$500 million in annual gross revenue carry designated public-communication content without additional charge to users, a nine-week delay before theatrical releases may stream, and transparency obligations, while further denying specific quota exemptions to providers controlled by, affiliated with, or dependent on a foreign legal entity. These bills – most notably #8889/2017 and #2331/2022 – would disproportionately burden U.S. services, favoring domestic broadcasters with visibility and tax benefits, and act as a discriminatory digital trade barrier, impacting market access by American firms could undermine the viability of providers, chill investment, and reduce consumer choice.

Content Regulation: Brazil enacted the Digital Child and Adolescent Statute in September 2025, creating a comprehensive legal framework for minors' online safety. The law mandates robust age verification, parental controls, and strict rules for data processing and advertising targeting children. Services accessed by minors must prioritize their best interests, with privacy and safety by default. To expedite the law's enforcement, a [decree](#) was issued to accelerate the implementation timeline, reducing the compliance period from the originally planned one-year to just six months. Another presidential [decree](#) designated Brazil's National Data Protection Authority (ANPD) as the primary enforcement authority for the new law, tasked with ensuring adherence to new protective standards for minors in data processing and content moderation. Developments on this issue and guidelines/regulations issued by the ANPD need to be closely monitored, especially considering the ANPD's broad remit over multiple regulatory subject matters relating to digital services.

Liability for Third-Party Content: In June 2025, the Brazilian Supreme Court (STF) ruled that Article 19 of the Civil Rights Framework for the Internet (Marco Civil da Internet, Law 12.965/2014), which regulates internet application providers' liability for third-party content, is partially unconstitutional (Themes 533 and 987). The Court limited Article 19's application to specific cases, such as crimes against honor, and established exceptions for serious offenses like terrorism, incitement to suicide, hate speech, and anti-democratic activities. Additionally, the Court determined that liability is presumed when providers promote paid content or use chatbots or artificial-profile networks for unlawful purposes. Furthermore, internet application providers functioning as marketplaces are subject to civil liability under the Consumer Defense Code (Law 8,078/1990). Platforms must implement self-regulation measures, maintain transparency, and provide accessible service channels.

Providers are also required to establish a legal presence in Brazil. The decision applies prospectively and is binding on all courts in the country. In addition, in August 2025, ANATEL revised its Regulation on Conformity Assessment and Approval of Telecommunications Products. Marketplaces are now jointly liable with sellers for violations related to the offering of irregular telecommunications products. The measure formalizes joint liability for marketplaces and other digital platforms involved in the commercialization process - even if they only act in the dissemination and advertising - for offering telecommunications products that are not approved or do not comply with ANATEL's technical requirements. Separately, in July 2026 the Government issued executive Decrees No. 12,975/2026 and No. 12,976/2026 expanding platforms' duties to combat crimes and fraud; these decrees face suspension bids in Congress.

CIDE: The Contribution for Intervention in the Economic Domain (CIDE) is a 10% federal contribution on certain payments for royalties or technical services made by Brazilian entities to offshore recipients, in particular for a license or technical services that involve a transfer of technology into Brazil. *Law No.*

10,332/2001 significantly expanded the scope of the tax, allowing the government to charge CIDE even when no actual transfer of technology occurs. In 2025, the Brazilian Supreme Court ruled to confirm this scope extension. As a result, many business operations started being taxed, increasing the cost of international transactions and directly impacting the competitiveness of U.S. companies that provide technology or expertise.

Marketplace Liability: The recent adoption of the above mentioned ANATEL Resolution No. 780/2025 also introduces a framework that disproportionately burdens online marketplaces, particularly foreign-based platforms, by extending joint liability for product certification to digital intermediaries. This includes platforms that merely advertise or facilitate product listings without participating in the sale or logistics chain. U.S.-based marketplaces operating in Brazil now face heightened legal exposure for third-party sellers' compliance failures, including the obligation to verify ANATEL certification codes and ensure product conformity—tasks traditionally outside the platform's operational scope and technically difficult to implement at scale. These new provisions create significant legal uncertainty and risk and may not only restrict market access but also deter cross-border digital trade and innovation. The resolution therefore raises serious concerns regarding proportionality, operational feasibility, and alignment with global digital trade principles.

Electronic Payment Services: In the past few years, the Brazilian Central Bank's (BCB) role as a regulator and a competitor has created a conflict of interest that affects EPS' ability to compete effectively. The BCB's Competitiveness and Market Structure Department (Decem) oversees not only the development of policy that affects all payment schemes in the Brazilian market, but also the development and regulation of PIX, a real-time payment scheme (including its participation rules and licenses), which went live on November 16, 2020. Pix compete directly with U.S. payment firms. All Brazilian financial institutions with over 500,000 accounts were mandated to participate in the PIX scheme by November 2020. On June 15, 2020, U.S. payment networks partnered with WhatsApp and launched a new payments solution to enable WhatsApp users in Brazil to transfer money and pay businesses. However, the BCB immediately suspended the payments program by abruptly modifying the payments regulation (through BCB Circular 4031 dated June 23, 2020), without notice or opportunity for public comment. Since then, the Central Bank's conflict of interest between a regulator and a product manager has intensified. Given the over-regulated environment of Brazil's payments industry, the Central Bank controls time to market, and can determine sector economics. Additionally, the Central Bank has been increasingly delegating supervisory functions to industry players instead of undertaking these itself. USTR should urge Brazil to establish effective institutional separation between the BCB's regulatory and Pix-operating functions; publish transparent and equivalent rules for public and private payment systems; consult the private sector early on material changes; and ensure that participation, pricing, security, resilience, and access requirements do not disadvantage U.S. EPS suppliers.

USTR should also monitor implementation of BCB Resolution No. 522 and related centralized settlement obligations. Payment Scheme Owners are being required to monitor and enforce sub-acquirer compliance, creating potentially significant network liability and supervisory burdens. These obligations should be clear, proportionate, risk-based, and aligned with the authority and information actually available to scheme owners.

Agentic commerce is another area in which competitive neutrality may become increasingly important. Card-based payment systems currently have an initial advantage, as they already rely on mature infrastructure for tokenization, authorization, authentication, risk management, and processing, while Pix still requires further development to support comparable use cases at scale. As the BCB monitors the development of agentic payments, it should consider a technology-neutral and function-based approach that recognizes the distinct roles performed by agentic-commerce enablers, service providers, and

payment initiators. In particular, concepts designed for Open Finance should not be automatically extended to other payment ecosystems, such as card-based ecosystems, which were not included in Brazil's Open Finance framework. Any future rules, if developed, should enable innovation across payment methods while avoiding regulatory asymmetries or classifications that could distort competition among different payment models.

Express Delivery Services: The 2025 NTE states that: “ Brazilian Customs has established express delivery maximum per-shipment value limits of \$10,000 for exports and \$3,000 for imports,” when in fact the maximum per-shipment limit is \$1,000, placing U.S. operators in a yet more precarious position.

Data Act Policy: The Department of Innovation of the Ministry of Development, Industry, and Trade (MDIC) is considering policies and legislative proposals related to the "data economy" modeled after the European Union's Data Act, which would impose discriminatory obligations on U.S. companies regarding the use of non-personal data. Although a formal proposal has not been released, there will likely be a public consultation on the matter with questions about how Brazil should implement a similar Data Act in the country. There are concerns that this proposal could unfairly target U.S. companies through specific thresholds.

Status update (September 2026): No dedicated MDIC public consultation on a Brazilian "Data Act" or non-personal-data framework has been formally launched. The underlying trajectory nonetheless remains active and warrants monitoring for several reasons: (i) in January 2026 the European Commission adopted an adequacy decision for Brazil's data-protection framework, described as removing the "last regulatory barrier" to EU-Brazil data flows and reinforcing the EU-convergence dynamic that motivates an EU-style Data Act; (ii) Brazil's E-Digital digital-transformation strategy cycle (2022-2026) is concluding, creating a natural vehicle for a successor data-economy agenda; and (iii) the data-protection authority (ANPD) is actively developing a National Policy on Personal Data Protection and Privacy.

Services Barriers - Telecommunications

6 GHz Spectrum Reversal and Reallocation: In December, 2024, Brazil's telecommunication regulator, Anatel, abruptly announced that it would reverse its 2021 decision allocated the entire 6 GHz band for unlicensed services (Wi-Fi), choosing instead to repurpose the upper portion of the band for 5G. This reallocation was officially enacted on August 12, 2026, when Anatel issued a ruling (Ato nº 10.400) formally reducing the country's unlicensed 6 GHz allocation from 1,200 MHz to 500 MHz. As of October 2026, the spectrum auction itself has not yet occurred, but Anatel is actively holding public hearings to finalize the tender rules and obligations for the upcoming bidding. The regulator's actions disrupt consumers, enterprises, and small ISPs that had already invested in full-band Wi-Fi technologies from U.S. companies. Moreover, the initial reversal was made without giving stakeholders a formal opportunity for input, and the shift appears motivated by efforts to align with China's 5G spectrum priorities.

Investment Barriers

Data Center Obligations: ANATEL's Resolution No. 780/2025 (published August 1, 2025) introduces stringent requirements for data centers, including mandatory conformity assessments, enhanced operational resilience standards, and additional security and sustainability requirements. Despite lacking clear statutory authority, telecom regulator ANATEL approved these requirements without a robust public consultation or regulatory impact assessment. The resolution also extends joint liability to online marketplaces and digital platforms involved in telecommunications product commercialization, requiring

compliance verification and imposing penalties. This extremely broad interpretation captures platforms with no direct role in product handling, creating significant legal uncertainty.

ANATEL's Resolution No. 780/2025 could particularly burden U.S. cloud providers who have already made significant investments in the country. Of special concern is the transition period for existing facilities, which could require significant infrastructure modifications and investments, potentially affecting service continuity and market competitiveness. In December 2025, ANATEL launched Public Consultation No. 48/2025 on proposed rules for the conformity assessment of data centers integrated into telecommunications networks. In February 2026, ANATEL's Board suspended its enforceability, halting certification requirements pending further review, although remaining within ANATEL's stated regulatory scope, with further developments expected once the Board decides to resume discussion.

Recent ANATEL agenda (2026): ANATEL continues seeking to expand its remit to regulate digital services and environment, potentially including cloud services and data centers. Although ANATEL lacks an explicit legal mandate—its current authority is limited to telecom services—the regulator has been pursuing new regulations to expand its scope through broad interpretation of existing powers, including via cybersecurity regulation. ANATEL has again raised regulatory-risk concerns through a new public consultation on its 6GHz auction notice, open until October 23, 2026, which would require winning bidders to help deploy "Regional Neutral Nodes" and edge data centers in Brazil. It will be important to clarify whether this renewed effort to tie data-center obligations to spectrum awards reflects ANATEL's continued push to expand its reach into digital infrastructure and to classify data centers as regulated telecom services.

Taxes and Tariffs on Digital Infrastructure: Brazil's tax treatment of digital infrastructure has been a persistent concern for U.S. technology providers. Since late 2025, imported data-center equipment faced a compounded federal tax burden (reported at approximately 48.94%) — combining import duties, industrial product taxes (IPI), and social contributions (PIS/COFINS) — while a Chinese competitor benefited from favorable treatment through an Export Processing Zone (ZPE) arrangement, creating an uneven playing field for U.S. investors. This asymmetry disadvantaged U.S. companies that had already committed significant capital to the Brazilian market and risked distorting future investment decisions.

Recent development (September 2026): On September 15, 2026, President Lula signed Bill 278/2026 into law, establishing the Special Taxation Regime for Data Center Services ("ReData"), which suspends import duties, IPI, PIS/Pasep, and COFINS (including on imports) on ICT equipment and components intended for data centers for up to five years, converting to a permanent exemption once obligations are met. While ReData responds to the headline tax-burden concern for qualifying investments, it does not fully resolve the underlying issues and introduces new ones. First, the import-duty benefit applies only to products with no equivalent manufactured in Brazil, and the Manaus Free Trade Zone retains distinct treatment — so relief is conditional and uneven. Second, eligibility is tied to local-content and localization mandates that raise their own market-access concerns: participants must dedicate at least 10% of processing/storage capacity to the Brazilian market (which may not be exported or retained abroad), meet sustainability and water-efficiency criteria, source renewable/low-emission electricity, invest locally an amount equivalent to 2% of the value of products purchased using the benefits, and steer 40% of digital-economy investment to the North, Northeast, and Midwest regions. Program entry requires Ministry of Finance authorization, and non-compliance can trigger claw-back of suspended taxes with interest and penalties, or revocation of eligibility. U.S. stakeholders should therefore continue to monitor implementation — particularly the localization and local-content conditions and any residual asymmetry versus incentives previously extended to specific competitors — to ensure the regime does not simply substitute one form of discriminatory or trade-distorting treatment for another.

Cambodia

Services Barriers

Content Moderation: Cambodia continues to face censorship, internet filtering, and blocking, with independent outlets often targeted during sensitive political events like the 2023 [elections](#). A February 2021 sub-decree established the National Internet Gateway, creating a single point of entry for internet traffic. A 2024 notification requires companies to use a national domain name, raising concerns about potential abuse for content blocking and restricting foreign digital services, similar to China's "Great Firewall". Additionally, a draft Cybercrime bill from Cambodia's Interior Ministry could hold intermediaries liable for third-party content and mandate data localization. Expected to be finalized by late 2025, the bill reportedly allows the government to control operating systems and duplicate data if companies fail to address cybersecurity threats, and includes vague prohibitions on defamation, "insulting, derogatory or rude language," and "false information" harmful to public order and "traditional culture", with penalties including fines and imprisonment. It also permits internet traffic data collection for suspected criminals and criminalizes online content that "depicts any act or activity ... intended to stimulate sexual desire".

Data Localization Requirements: In addition to the draft Cybercrime Bill, data localization requirements are also found in the draft Cloud First Policy of Cambodia. The draft aims to accelerate digital transformation and public sector cloud adoption. However, the mandates regarding data localization (specifically for Confidential data) and stringent data sovereignty requirements, while designed to protect national interests, introduce significant complexities and potential limitations that could, in practice, hinder the widespread, efficient, and cost-effective adoption of cloud computing. The policy mandates that confidential data (which includes sensitive categories like Government Classified Information, Personal Identifiable Information, and Financial Data) must be stored or processed within the in-country infrastructure of an MPTC accredited CSP or the government cloud. By limiting the storage of critical data to local infrastructure, ministries and institutions (M&Is) are prevented from accessing the massive, cost-efficient Public Clouds offered by global providers, whose infrastructure may be located anywhere.

Personal Data Requirements: Further, Cambodia released a draft Law on Personal Data Protection (LPDP) on July 23, 2025, which is inspired by the EU's GDPR. The draft law introduces rules for data processing, establishes data subject rights like access and erasure, mandates appointing a Data Protection Officer for certain organizations, and includes administrative fines for violations. It applies to both domestic and foreign entities processing personal data of individuals in Cambodia, with a proposed 2-year implementation period after it is enacted. Several provisions in the LPDP deviate from international best practices and create an unpredictable and difficult compliance environment, presenting significant barriers for U.S. service providers seeking to serve the Cambodian market. Key concerns include:

- disproportionately high administrative fines of up to 10% of annual turnover, which far exceed global standards and is not clearly tied to turnover related to the specific violation, creating immense financial risk;
- operationally challenging and rigid compliance timelines, such as requiring "immediate" action upon consent withdrawal by privacy subjects, and a 72-hour data breach notification triggered merely by "becoming aware" of an incident, which is often impractical;
- a broad "right to erasure" that lacks a balancing test to protect freedom of expression and fails

to preclude a private right of action, which could lead to inconsistent enforcement and excessive litigation; and

- a high age of consent set at 16, which does not align with the widely accepted international standard of 13 and could limit teenagers' access to online services.

Services Barriers - Telecommunications

Local Testing Requirements (Telecommunications): The Telecommunications Regulator of Cambodia (“TRC”) is responsible for overseeing the “type approval” process for telecommunications equipment. Type approval is required to import telecommunications products and includes review of foreign standard test reports. The TRC imposes a variety of type approval and regulatory requirements, including enforcing country-of-origin requirements (e.g., separate certification needed for each country-of-origin for the same model of the product). In particular, the TRC requires suppliers to acquire test reports in the vendors’ name in

Cambodia for Small Form-factor Pluggable (“SFP”) modules that typically do not require certification in other countries. Reports from Original Equipment Manufacturers (“OEMs”) or Original Design Manufacturers (“ODMs”) are not accepted by the TRC. Additionally, type approval is required for line-cards (also not required in other countries). The current regulations are highly burdensome for U.S. suppliers because it is impractical to obtain certificates and type approval for line cards that cannot function independently. Lastly, the TRC also prohibits import of refurbished products.

The TRC’s overly stringent enforcement of its type-approval guidelines is an unfair market access barrier that is out-of-step with practices in other countries’ regulations and disrupts business operations and customer support in Cambodia. Furthermore, Cambodia made significant expansions to the scope of type approval without consultation or provision of transition periods.

Canada

Import Policies

CBSA Assessment and Revenue Management project: The Canadian Border Services Agency (CBSA) continues to pursue several concerning changes to customs procedures and practices that may conflict with Canada’s customs and trade facilitation obligations in the USMCA and the World Trade Organization’s Trade Facilitation Agreement. The CBSA Assessment and Revenue Management project, better known as CARM, is a multiyear initiative to change the Canadian importation process. The CARM system became the official system of record for assessing and collecting duties/taxes on imported commercial goods on October 21, 2024. Persistent issues with CARM’s implementation, including system backlogs, compliance burdens, and procedural disruptions, have raised concerns among U.S. traders and logistics providers. These challenges risk undermining trade fluidity and supply chain reliability between the United States and Canada. NFTC’s concerns in this section of the NTE around CARM persist. NFTC urges continued flexibility in CARM, including the extension of transitory measures and to make additional permanent changes to CARM to alleviate the backlogs and disruptions caused by the CARM program.

Customs Act: Amendments to Canada’s *Customs Act* introduced through the 2024 Budget Implementation Bill (*Bill C-19*) impose new obligations and potential liabilities on express carriers

delivering goods into Canada. These provisions substantially alter the risk framework for small and medium-sized enterprises (SMEs) engaged in cross-border e-commerce. Under the revised rules, carriers continue to be held liable for additional taxes, duties, penalties, and related costs for up to four years after importation, even in cases where they act solely as intermediaries, requiring them to recover such costs from shippers after the fact. Such measures undermine trade facilitation goals under the USMCA and disproportionately affect smaller firms seeking to access the Canadian market.

Customs System Reliability and Contingency Procedures: Unplanned CBSA system outages continue to interrupt the electronic release of express and commercial shipments at Canadian ports of entry. Because express shipments are released electronically ahead of arrival, even brief outages create backlogs, missed delivery commitments and storage costs for U.S. exporters. Canada has no published, binding backup plan for clearing low-risk shipments during an outage. NFTC recommends that USTR urge Canada to adopt service-level standards for customs systems and a transparent backup plan. That plan should keep express release working during outages, consistent with Canada's trade facilitation commitments under the USMCA.

Intermediary Liability Under Forced Labor Import Measures: NFTC supports efforts to keep goods made with forced labor out of North American and global supply chains. However, Canada's proposed forced labor import legislation cannot place enforcement liability on express carriers and customs brokers. Canada should align its approach with the U.S. Uyghur Forced Labor Prevention Act and establish a USMCA-consistent process for identifying and releasing detained goods.

Technical Barriers to Trade

Innovative medicine and pharmaceutical market access: Canada continues to underinvest in new medicines relative to its peers, spending only 0.32% of GDP on medicines launched in the past decade, compared to 0.78% in the United States. This creates substantial market access barriers for U.S. Industry recommends:

- **Net Price Policy Reform:** Enhanced federal financial resourcing should be provided to provinces to address the structural undervaluation of innovative medicines and therapies and existing access barriers:
 - **pCPA:** The pan-Canadian Pharmaceutical Alliance (pCPA) must evolve beyond cost-containment to a mandate that recognizes the value of innovation and aligns pricing with globally competitive benchmarks.
 - **CDA:** Canada's Drug Agency (CDA) requires fundamental reform to better assess the full patient, health system and societal value of new medicines and therapies. As an immediate step, it is vital the CDA discontinue the practice of issuing price reduction recommendations (based on outdated metrics), which often call for unrealistic reductions of 70-90%, resulting in price points that are at or below generic-equivalent levels.
- **PMPRB:** The government should reduce red tape by sunseting the Patented Medicine Prices Review Board (PMPRB), which was established nearly 40 years ago and whose mandate has not kept pace with the realities of pharmaceutical pricing and patient access in Canada today. At a minimum, the restoration of the United States and Switzerland as PMPRB comparator countries using the Highest International Price (HIP) benchmark is imperative.

- **No Localization:** Ensure that increased funding for these reforms avoids localization policies that disadvantage or create unfair obligations for U.S. companies operating in Canada (e.g. *Buy Canadian*).
- **Market Access Delays (Pharmaceuticals):** In Canada, it takes approximately two years following regulatory approval for a medicine to reach patients insured on public drug plans. This is due to lengthy sequential administrative processes and federal-provincial pricing negotiations through the pan-Canadian Pharmaceutical Alliance (pCPA) before individual jurisdictional funding agreements. In an ideal world, patients would not have to wait to access innovative medicines while officials and manufacturers discuss *behind-the-scenes* financial and administrative details. Canada should significantly reduce the additional bureaucratic delays following national regulatory approval to access public drug plan formularies managed by each province or territory.

Government Procurement

WTO Government Procurement Agreement Listing: Canada is a member of the WTO Government Procurement Agreement (“GPA”), which binds Members, including the United States and Canada, to reciprocal market access in government procurement. Shared Services Canada (“SSC”), a government agency that was formed in August of 2011, has not been listed in Canada’s Appendix I Annexes of the WTO GPA. SCC is the Canadian government’s largest procurer of information technology (“IT”) products and services, as it brings together the IT resources from 42 departments.

Buy Canada Procurement Policy: As a result of trade tensions and sovereignty threats, the Canadian Government has introduced “Buy Canada” or “Canada First” procurement policies – including digital sovereignty strategies at the federal and provincial level.

- **Cloud:** The Canadian government issued a Sovereign Cloud Request for Information, with objective to discard non-domestic hyperscalers from procurement opportunities, and focus on working with local providers over leading American cloud providers. This will impact foreign direct investors’ ability to expand their services into procurement (particularly areas such as national security, defense, and healthcare), as well as regulated industries like financial services. For large strategic procurements ($\geq \$5M$), Canadian suppliers and Canadian content receive bid evaluation advantages, which can tilt outcomes toward Canadian^[OBJ]-based or Canadian^[OBJ]-controlled solutions in sectors like digital infrastructure and services.
- **Sub-national:** Several Canadian provinces have also enacted or informally adopted measures that de-prioritize or negatively affect American suppliers in tenders ranging from medical devices to IM/IT, often favoring domestic suppliers in violation of national treatment commitments.
- **Vaccine and pharmaceuticals:** Buy Canadian is a new federal procurement framework that gives suppliers with Canadian manufacturing or production activity preferential pricing and evaluation treatment. In vaccine tenders, this could provide up to a 20% price advantage to suppliers with a Canadian production footprint linked to the product subject of a tender, despite globally integrated vaccine supply chains. Since December 2025, the policy has also provided a 10% automatic price discount for Canadian bidders and required 20% of bid evaluations to reflect Canadian value-added content. These measures are inconsistent with Canada’s obligations under the WTO Government Procurement Agreement, additional WTO obligations (e.g., GATT, TRIMs, TBT and SPS) and related USMCA/CUSMA provisions. Canada is currently the only WTO GPA signatory applying local-content requirements of this kind to vaccine procurement,

prompting concerns from several major trading partners at the WTO GPA Committee. Buy Canadian creates material trade-compliance, market-access, and public health risks when applied to innovative medicines and vaccines.

- Canada's focus on localization has also emerged in pharmaceutical and life sciences processes that should turn on scientific judgment rather than manufacturing location. Recent developments include:
 - updated National Advisory Committee on Immunization (NACI) guidance seeking information on "current or planned domestic manufacturing" in vaccine dossiers;⁴
 - a proposed Health Canada priority review process favoring generic drug submissions involving domestic manufacturing;⁵ and
 - recommendations of the Pharmaceutical and Life Sciences Sector Task Force to factor domestic value creation into procurement and investment decisions.⁶

Intellectual Property Protection

Copyright Act: Canada's Copyright Act lacks explicit provisions for AI-generated works, and the Copyright Act doesn't include a specific exception for text and data mining. While limited exceptions like fair dealing may apply, the absence of clear guidelines could restrict AI development.

Inadequate Patent Term Adjustment (PTA): The USMCA requires Canada to provide PTA for unreasonable delays during the prosecution and issuance of any patent. However, Canada has created a PTA framework which includes inequitable barriers that constructively undermine the treaty provision, and which will prevent American patent holders from obtaining compensation for unreasonable delays. The process to apply for PTA is burdensome, costly, and creates significant market uncertainty. Canadian patent holders do not face these burdens or lack of adequate adjustment in the United States. NFTC encourages USTR to urge the Canadian government to provide up to 5 years of patent term restoration that runs consecutively with patent term adjustment instead of concurrently.

Inadequate Patent Enforcement: USMCA Article 20.44 obligates Canada to (1) provide notice if a generic or biosimilar company relies on the safety and efficacy data of a "previously approved" innovator's product and (2) to provide adequate time and sufficient opportunity for the innovator to seek appropriate remedies before the marketing of the allegedly infringing product. Canada's system currently provides instead that a generic or biosimilar company can rely on previously approved products if they are not yet marketed. In such cases, there is no notice or opportunity to obtain timely and appropriate remedies by the innovator. We urge USTR to work with Canadian counterparts to fully implement USMCA obligations relating to patent enforcement such that notification and an opportunity to pursue

⁴ Manufacturer Vaccine Dossier Submission Process and Outline NACI Secretariat, Centre for Immunization Programs, PHAC (May 2026).

⁵ Health Canada seeks feedback on a proposed pilot approach to prioritize certain generic drug submissions involving domestic manufacturing within the regulatory review queue: Notice (July 15, 2026) <https://www.canada.ca/en/health-canada/programs/consultation-proposed-pilot-approach-prioritize-certain-generic-drug-submissions-involving-domestic-manufacturing-within-review-queue/notice.html>.

⁶ Pharmaceutical and Life Sciences Sector Task Force: Report to the ministers of health and industry (July 24, 2026) <https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/announcements/pharmaceutical-life-sciences-sector-task-force/report-ministers-health-industry.html>.

appropriate remedies in a timely manner are provided so long as the generic or biosimilar is referencing the previously approved product, consistent with the text of Article. 20.44, regardless of whether the innovator product is marketed.

Services Barriers

Online Streaming Act (C-11): In April 2023, the Canadian Government passed Bill C-11 Act to amend the Broadcasting Act,. The law and related rules promulgated by Canada’s regulator can compel U.S. platforms to promote Canadian over U.S. content and force U.S. companies to make financial payments into funds that only Canadians can access and invest in content they cannot own. On June 4, 2024, the Canadian Radio-television and Telecommunications Commission (CRTC) announced that streaming services meeting certain thresholds (e.g., annual revenues of C\$25 million or more in Canada) and not affiliated with a Canadian broadcaster will have to contribute 5% of their Canadian revenue starting in the 2024-25 broadcast year. In November 2025, the CRTC issued a new, restrictive definition of Canadian content that will magnify the negative impact of future measures on U.S. companies and the U.S. film and TV production industry. Following this, the CRTC on May 21, 2026, adopted a further audiovisual expenditure framework raising the requirement to 15% (inclusive of the existing 5% base contribution) for covered unaffiliated online broadcasting groups — well below the up-to-30% investment obligation previously anticipated. The government has since announced a reconsideration of this approach: on June 3, 2026 it announced new policy directions and a review of the CRTC’s recent decisions, and a July 17, 2026 Department of Justice court letter indicated the government intends to eliminate the original 5% base contribution, leaving the CRTC’s adopted framework in limbo pending formal policy instructions. While the government subsequently announced it would issue a policy direction reforming these decisions, the reversal still needs to be implemented and there are still concerns that it will not remove all the discriminatory aspects of the law, and as of October 2026, no such policy direction has been published. NFTC encourages USTR to treat Canada’s *Online Streaming Act* (C-11) as a deliberate and discriminatory measure against U.S. networks and streaming services and the U.S. film and tv production industry.

Québec Bill 109: Quebec’s Bill 109 became law in December 2025, with the stated purpose to promote discoverability of and access to original French-language cultural content in the digital environment. The law grants broad authority to the Québec Cabinet to enact regulations that will impose new registration requirements, reporting requirements and French content quotas, accessibility and discoverability requirements on digital services and manufacturers of TVs and connected devices. It also creates a new administrative unit within the Ministère de la Culture et des Communications under the name “Bureau de la découvrabilité des contenus culturels” (the BDCC) and gives the BDCC broad powers to enforce the bill. The law is in the process of being implemented and is expected to move ahead even with a new party forming government following the October 5th provincial election.

Data Localization: The Province of Québec adopted privacy legislation, known as Bill 64, in September 2021 that would make data transfers extremely difficult. The law only permits public and private sector entities (with limited exceptions) to transmit personal data outside of the province to jurisdictions with a level of protection equivalent to Québec’s privacy law. The U.S. International Trade Commission identified the law as a barrier to digital trade in its “Year in Trade 2021” report published in August 2022.

Bill C-36 (the Protecting Privacy and Consumer Data Act) was introduced in June 2026, changing Canada’s federal privacy law to require express, opt-in consent for the collection, use or disclosure of personal information subject to limited exceptions. Under the new law, express, opt-in consent will be required for any data processing that aims to influence decisions or behaviors regardless of the actual

impact on a person. This imposes the same requirements for personalized content recommendations or ads as for data to be used for profiling in employment services - two very different risk tiers. Additionally, the bill's definition of personal information includes inferred data. This development would have the most impact on AI model training which often rely on data inference, which would mean that any inference would need an additional legal basis for data processing - just adding more compliance burden. USTR is urged to proactively engage the Canadian government to advocate for a legislative framework that is interoperable with global standards and promotes a fair and open digital marketplace.

Additionally, Shared Services Canada (SSC) issued a request for information (from August 13, 2025 through September 30, 2025) to inform the development of a sovereign procurement stream for Infrastructure-as-a-Service and Platform-as-a-Service. This framework would require all government data to be processed and stored in Canada, and providers, including parent companies, to be free from foreign laws allowing external government access. SSC cites a National Security Exception to bypass trade obligations. Canada's proposal excludes U.S. cloud providers based on ownership, not security, raising significant concerns that U.S. providers will be unfairly prejudiced in bidding for public sector contracts, making this a discriminatory trade barrier.

News Media-Related Digital Service Taxes: Additionally, Canada's Bill C-18 (the Online News Act) enacted in June 2023, empowers the Canadian Radio-Television and Telecommunications Commission (CRTC) to mandate payments from large "digital news intermediaries" to news publishers for content reproduction. Inspired by Australia's News Media Bargaining Code law, C-18 targets specific U.S. companies (namely Meta and Google), as evidenced by Canadian lawmakers' statements in Parliament and the Parliamentary Budget Office estimates, which projected C\$329.2 million annually would be paid to news publishers under the assumption that only Google and Meta would be implicated under the legislation, with 75% of that amount going to large broadcasters. Implementing regulations require platforms to pay at least 4% of their global revenue (adjusted for Canada's GDP ratio) for exemption. This has led to one of the target U.S. companies securing a five-year exemption after agreeing to an annual C\$100 million payment to Canadian news organizations, while the other U.S. company ceased news linking in Canada. The law harms the user's access to the open Internet and threatens security and safety. It also conflicts with Canada's international trade obligations, including under the U.S.-Mexico-Canada Free Trade Agreement (USMCA) Articles 14.4 (Investment) and 15.3 (Cross-border Services) regarding National Treatment; USMCA Articles 14.5 (Investment) and 15.4 (Cross-border Services) regarding Most-Favored Nation Treatment; USMCA Article 14.10 regarding Performance Requirements; USMCA Article 19.4 regarding Non-Discriminatory Treatment of Digital Products and WTO intellectual property agreements. Prime Minister Mark Carney acknowledged the law's shortcomings in August 2025, suggesting that the government could seek to amend or repeal the law in view of its disruptive impact on the dissemination of news and information online.

Artificial Intelligence: In June 2022, the Government of Canada tabled the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27, the Digital Charter Implementation Act, 2022. Bill C-27 has now lapsed but AI elements are expected to be re-introduced. AIDA proposed significant new powers for the government to regulate 'high-impact' AI systems, but included overly broad definitions of 'high-impact' systems that could capture low-risk use cases. AIDA's unclear "person responsible" definition further complicates matters, potentially requiring the revelation of proprietary information. The lack of clarity poses risks for innovators and online service providers, especially with the government's intent to reintroduce AI elements, possibly including content moderation under "high-impact", as articulated in an October 2023 letter from then Minister of Innovation, Science and Industry, François-Philippe Champagne. The proposal also included monetary penalties of up to 3% of global revenues and introduced a first of its kind criminal enforcement provision for non-compliance. This regulatory approach poses significant risks to U.S. companies and the U.S.-led risk-based approach to AI governance.

and will create a massive compliance burden on leading U.S. AI researchers and developers and threaten interoperability across North America.

Separately, the Competition Bureau's 2024 consultation on its discussion paper on AI and competition will need to be monitored. The paper is part of the Bureau's broader inquiry on how competition is developing in AI markets, the potential for regulation to protect and promote competition in AI markets, and potential measures to address competitive harms arising from AI. Industry advises monitoring this process to ensure that any regulatory oversight on competition and AI is balanced, flexible, and nationality-neutral. The generative AI market is diverse, with no current signs of competitive harm from AI input access; and existing competition laws are sufficient to address future issues, including the potential for algorithmic collusion.

Content Moderation: In 2021, Canada proposed a framework to address harmful online content, including 24-hour takedown requirements, monitoring, filtering, and site-blocking, raising concerns about censorship and overbroad definitions. On February 26, 2025, the Online Harms Act was introduced, imposing strict obligations on social media platforms, including 24-hour removal deadlines for child exploitation and non-consensual intimate content. This bill would establish a powerful Digital Safety Commission with authority to issue codes, impose fines (up to 6% of global revenue), conduct inspections, and potentially mandate company funding, raising concerns about encryption due to possible scanning requirements. The Conservative Party also proposed an alternative bill (C-412, *Protection of Minors in the Digital Age Act*) to impose "duty of care" obligations, parental controls, private rights of action for "serious harm," and prohibit certain interface designs,[#] risking over-enforcement and frivolous lawsuits. Although these proposals expired, the Liberal government announced in June 2025 its intention to revive and expand the effort to address AI developments.

Additionally, the Office of the Privacy Commissioner of Canada (OPC) recently concluded its exploratory consultation on age assurance, which ran from June to September 2024, and is now proceeding to draft formal guidance for online service providers. While the consultation is officially complete, this process is advancing in concert with pending federal legislation, specifically Bill S-209, which seeks to mandate age verification for access to certain online content and is currently being considered in committee in the Senate. The Privacy Commissioner has endorsed this Bill, signaling a coordinated regulatory and legislative push toward mandatory, high-friction age assurance systems. For U.S. industry, this trajectory raises significant concerns that constitute a potential non-tariff barrier to trade, including: substantial operational costs and technical burdens of implementing Canada-specific systems, which disproportionately impact small and medium-sized enterprises; the creation of legal and financial liability from collecting and storing highly sensitive datasets that link verified identities to private online behavior; and regulatory uncertainty driven by a lack of clear technical standards, data protection safeguards.

Lawful Access Act (Bill C-22): Canada's government introduced Bill C-22 on March 12, 2026; it passed the House of Commons on June 18, 2026, and now awaits Senate consideration. The bill would expand mechanisms for obtaining subscriber and transmission information and establish a Supporting Authorized Access to Information Act governing service-provider capabilities and assistance, including technical requirements and information-retention obligations that could create substantial implementation costs and security concerns for U.S. communications and cloud providers. The House-passed text includes safeguards that materially narrow these powers: judicial authorization for subscriber-information production orders, a restriction on compelled decryption unless the provider supplied the encryption and holds the means to decrypt, and a bar on requirements that would create a systemic vulnerability — though that last goal sits in tension with the bill's targeted-access provisions. USTR should monitor the Senate process and any implementing regulations, scrutinizing whether the technical-capability

obligations undermine secure services or impose disproportionate costs on foreign suppliers.

Chile

Technical Barriers to Trade

Non-Harmonized Digital Rules: Chile's digital regulations serve as a significant technical barrier to trade and present challenges for foreign technology companies operating in the market. Most notably, the country requires cybersecurity incidents to be reported within 3 hours, compared to the international standard of 72 hours. This regulatory divergence functions as a non-tariff barrier, requiring foreign companies to create costly Chile-specific compliance systems. The financial impact is substantial — according to the "AI Unlocking Ambitions" study commissioned by AWS, companies must dedicate 19% of their investment capital just to meet local regulatory requirements. The situation is further complicated by Chile's fragmented institutional framework, where overlapping jurisdictions and conflicting requirements create additional barriers for international companies without local expertise. This regulatory landscape, lacking a central coordinating body, has led to inconsistent policies across agencies that could hinder the development of a coherent national digital strategy.

Reforms to Express Delivery VAT Collection: Chile recently implemented a modernized compliance framework that modifies the de minimis treatment for low-value imported goods. By shifting value-added tax collection away from the physical border for shipments falling under a specific threshold, this new mechanism successfully reduces administrative friction and streamlines the entry process for U.S. e-commerce exports arriving in the country. While the secondary regulations originally created operational concerns by separating goods below the \$500 threshold from those above it, the final implementation reflects a constructive regulatory achievement. Defining this mechanism required a lengthy and highly complex coordination process between the Internal Revenue Service (SII) and Chilean Customs. Ultimately, this interagency collaboration produced a positive result that enhances the efficiency of the express delivery regime. NFTC commends Chile for this modernization effort and encourages continued collaboration to further facilitate expedited customs procedures and eliminate unnecessary delays.

Customs Information Technology Infrastructure and Stability: Chilean Customs relies on highly outdated information systems that experience frequent blackouts and unexpected outages, disrupting automated clearance channels and forcing incredibly slow manual reviews. Furthermore, physical inspections lack automated risk-management criteria, relying heavily on subjective officer interpretations. This infrastructure instability negates the benefits of expedited shipping and causes severe supply chain disruptions for American exporters. NFTC recommends that USTR consistently urge Chile to invest in modernizing automated customs tools. Furthermore, USTR should press Chilean Customs to establish a transparent, binding contingency plan that guarantees express lanes remain functional during software crashes, reducing subjective clearance delays.

Notarization Requirements for Sanitary Health Approvals: Certain imported products require authorization from the Regional Ministerial Secretariats of Health (SEREMI) before they can be cleared by Customs. Health authorities in Chile currently require express operators to present notarized powers of attorney to obtain these approvals on behalf of consignees, based on the interpretation of Law 19.880 governing administrative procedures. This requirement creates administrative burdens that are difficult to reconcile with express logistics operations, particularly for shipments destined to individual consumers. In addition, the requirement is applied differently to customs brokers, creating uneven regulatory treatment.

Customs Disposal Procedures for Abandoned Cargo: Customs authorizations required to legally dispose of abandoned cargo in Chile can take several years, leaving goods permanently trapped in the bonded warehouses of express operators. This bureaucratic paralysis forces logistics providers to act as indefinite storage facilities, consuming critical capacity, driving up overhead costs, and creating severe health and safety hazards. To resolve this bottleneck, NFTC strongly recommends that USTR urge Chilean Customs to implement a streamlined, time-bound administrative mechanism for the rapid authorization of cargo disposal, preserving the warehouse capacity necessary for fluid bilateral trade.

Customs Fines and Authorized Economic Operator: Chile Customs continues to levy disproportionate, punitive fines on minor, non-fraudulent clerical and data entry errors, unnecessarily raising compliance costs for U.S. express operators. Treating simple administrative mistakes on high-volume manifests as punishable offenses contradicts trade facilitation principles and deters supply chain investment. Concurrently, Chile's Authorized Economic Operator program fails to deliver tangible trade facilitation benefits, denying certified partners expedited clearance or reduced inspection rates. NFTC recommends that USTR raise these issues to establish a mandatory administrative safe harbor for minor clerical errors. Furthermore, USTR should press Chile to reform its AEO program to guarantee meaningful, measurable facilitation benefits, bringing the program into alignment with established international customs norms and properly incentivizing corporate compliance.

Intellectual Property Protection

Patent Linkage: Despite being a clear obligation under the U.S.–Chile Free Trade Agreement, Chile has yet to implement a formal patent linkage system, leading to IP infringements on both the public and private market. These linkage issues stem from the disconnect between the authorization granted by the local medicines regulatory agency (ISP) and the patent rights granted by the National Intellectual Property Office (INAPI), where this absence of mandatory consultation allows unauthorized products to enter the private market and even the public procurement system. This gap in enforcement results in multiple costs for American pharmaceutical companies in the form of increased legal and operational costs, regulatory uncertainty, and distorted competition. Chile should implement a robust patent linkage system that includes a) legal framework mandating the ISP consult the patent registry before granting sanitary registration b) administrative interface between INAPI and ISP to flag potential conflicts and c) effective and balanced procedural rules and due process mechanisms for notification and appeals.

Inadequate regulatory data protection (RDP): Chile does not provide adequate protection for undisclosed test data, leading to possible unfair commercial use and unauthorized disclosure by third parties. This RDP system contains weaknesses ranging from inappropriate procedural barriers to seek and receive RDP to ambiguous carveouts precluding RDP for certain pharmaceutical innovations (e.g., new uses, formulations, compositions, dosage forms, etc.). Specifically, Chilean regulators inappropriately require innovators to request RDP for specifically identified data and deny RDP in the event subsets of clinical trial data were voluntarily disclosed publicly. Chile should align its regulatory data protection standards with global norms to prevent unfair treatment of American innovation.

Services Barriers

Electronic Payment Services:

U.S. Electronic Payment Service (EPS) suppliers face critical regulatory challenges in Chile due to General Instruction No. 5 (“ICG No. 5”) issued by the Chilean Competition Tribunal (TDLC) and upheld by the Supreme Court. These measures impose structural limitations on U.S. EPS' ability to update their

rules, standards, and scheme fees without prior agreement from licensees or approval from the National Economic Prosecutor's Office (FNE). In particular, Instruction 4.6.e mandates that any change to the payment system rules undergo a negotiation or review process that can extend for months.

This framework severely restricts operational flexibility and poses a material risk to its ability to respond in a timely manner to technological advancements, evolving regulatory requirements, and emerging security threats. The delay and uncertainty introduced by these obligations undermine the capacity to maintain a secure, competitive, and innovative payments environment.

Moreover, the requirement to provide 60 to 90 days' advance notice for adjustments to scheme fees and merchant risk categorization further impedes U.S. EPS suppliers' ability to adapt dynamically to market conditions. While intended to foster competition, these constraints create a rigid regulatory environment that threatens to slow innovation and investment in Chile's digital payments ecosystem.

Chile should also ensure that implementation of ICG No. 5 permits expedited changes needed for security, fraud prevention, legal compliance, and global technical standards; includes defined review criteria and deadlines; and does not discriminate against U.S. EPS suppliers. As Chile reviews its payments regulatory framework, it should assess whether the regime is supporting competition, innovation, investment, security, financial inclusion, and long-term sustainability. USTR should encourage meaningful consultation with U.S. stakeholders and regulatory impact assessments for material payment measures, including an evaluation of cumulative and overlapping obligations across authorities. Better coordinated and predictable regulation would preserve legitimate public-policy objectives while enabling U.S. suppliers to compete fairly and bring secure global payment innovations to Chilean consumers and merchants.

Chile also has an opportunity to preserve competitive neutrality as account-to-account, instant-payment, and person-to-merchant solutions continue to develop. Because the regulatory framework for these services is still evolving, Chile should ensure that comparable payment activities are ultimately governed by equivalent, risk-based standards for security, compliance, liability, consumer protection, tax transparency, and regulatory oversight. A consistent framework across payment rails would support innovation while preserving formalization and trust and avoiding future competitive distortions affecting U.S. card networks.

This is a trade and investment concern—not solely a domestic competition-policy matter. Fragmented and unpredictable regulation raises the cost of supplying U.S. digital payment, data-processing, cybersecurity, fraud-prevention, and network-management services into Chile; delays the introduction of globally standardized innovations; impairs the scalability of U.S. business models; and reduces incentives for further U.S. investment. It may also disadvantage U.S. suppliers relative to domestic or emerging payment solutions that do not bear equivalent regulatory burdens.

Requirement for Local Presence to Digital Services Platforms: The Child Safety bill under discussion in Congress and supported by the Executive creates obligations that apply to every provider of digital platforms that offers services to users in Chile, regardless of its place of incorporation, domicile, or establishment (Article 2). This approach is overly broad, as it effectively subjects every service provided from the U.S. to Chile to the full scope of Chilean regulation. Furthermore, Article 19 of the Bill requires foreign providers to designate a legal representative domiciled in Chile within ninety calendar days of the publication of the law, under penalty of a serious infringement that, if repeated, may lead to the suspension of the service. This provision may be inconsistent with Article 11.5 of Chapter Eleven (Cross-Border Trade in Services) of the Chile–United States Free Trade Agreement, in force since January 1,

2004, which prohibits requiring a service supplier of the other Party "to establish or maintain a representative office or any form of enterprise, or to be resident, in its territory as a condition for the cross-border supply of a service." By making a representative presence in Chile a condition for cross-border supply, Article 19 effectively creates a local presence requirement that constitutes a trade barrier under the FTA.

Cloud Outsourcing Regulations for Financial Institutions: The Chilean financial regulator (CMF) has rules related to the general IT outsourcing of services (RAN 20-7) that allow cloud adoption in country and abroad but require financial institutions to have local data centers for contingency purposes, when processing relevant data / critical workloads abroad. The 2017 version of the regulation issued by the CMF did not allow for an exception to requirements on local infrastructure for contingency purposes. Following a public consultation process in 2019, the CMF agreed to create an exception for the requirement. However, the regulator authorized a narrow exception exclusively for banks that maintain adequate operational risk management per CMF's assessment. Many financial institutions in Chile cannot benefit from the exception, as they do not meet CMF's requirements on "adequate" operational risk management. This has become a blocker for the advance of data hosting services in Chile, as it effectively funnels financial institutions to local infrastructure offerings. The CMF has since opened a second consultation in May 2026 on broader RAN reforms — introducing a "fourth party" definition that cascades compliance obligations to subcontractors, imposing prescriptive exit strategies, and retaining in-country contingency requirements, collectively discouraging cloud adoption.

Data Protection: Additionally, Chile approved a new Personal Data Protection Law in 2024, inspired by the EU's General Data Protection Regulation (GDPR). The law is set to enter into force in December 2026. A significant issue is that the law's implementation is heavily dependent on the issuance of numerous secondary regulations by a new Data Protection Agency, which will only become operational concurrently with the law itself. This creates substantial legal and operational uncertainty for U.S. companies. Critical mechanisms for enabling international data transfers—such as standard contractual clauses, binding corporate rules, and adequacy decisions—have not yet been developed. The absence of this essential regulatory framework makes it impossible for businesses to prepare for compliance, potentially disrupting transatlantic data flows that are vital for the digital economy. It is essential that Chile ensure all critical secondary regulations are finalized and published months in advance of the law's entry into force, or alternatively, that the transition period is extended to provide businesses with adequate time to adapt.

Potential Barriers in New Cybersecurity Framework Law: Chile recently approved a new Cybersecurity Framework Law (in effect as of March 1, 2025), modeled after the EU's Networks and Information Security Directive 2 (NIS 2). While the objective of enhancing cybersecurity is laudable, its implementation could create significant trade barriers if not properly designed. It is critical that the law and its subsequent regulations, and Chile's overall cybersecurity framework, promote regulatory interoperability with internationally recognized standards, such as the NIST Cybersecurity Framework and ISO standards. This would prevent the creation of unique, country-specific requirements that would be burdensome for U.S. firms. Furthermore, the framework must not impose bureaucratic hurdles that hinder compliance for companies without a physical or legal presence in Chile. For example, requiring a *Clave Única* (Chile's state-issued digital ID) for registration or compliance would effectively exclude foreign companies whose implementation and cybersecurity teams are located outside of Chile. The law must be implemented in a manner that recognizes the global nature of cybersecurity operations and the Digital Economy.

China

Import Policies

Clearance Policy and Procedures for International Transshipment Goods: There is a lack of a cohesive clearance policy and associated procedures for international parcels transiting (not entering) the Chinese market. This hinders efficient cargo flow and increases business cost. Express carriers have long requested innovative and streamlined clearance procedures from China Customs. A pilot project with robust private sector consultation and input is recommended.

Intellectual Property Protection

Data Requirements for NMPA Clinical Trial Applications: NMPA has in recent years required an unusually detailed review of manufacturing and control process for biologic CTA filing at the Center for Drug Evaluation (CDE) and sample testing requirements of vaccine material at NIFDC at the CTA stage, which requires biopharmaceutical companies to reveal proprietary information about manufacturing steps and test methods and additional data beyond what is required on the face of the CTA application materials. This is not consistent with international practice and is particularly concerning for innovative biologic and vaccine products. The additional information and testing requirements delay the clinical trials and raise concerns about potential disclosure of confidential information (including manufacturing and commercial information) at early clinical phase.

Patent Term Extension Conditions (Pharmaceuticals): China introduced the PTE to the revised Patent Law in 2021, and the detailed guidelines took effect on January 20, 2024. The new Implementation Rules establish specific basic conditions for PTE eligibility, which weaken the value of PTE and its ability to encourage innovative medicines to enter China and benefit the Chinese patients. In a significantly positive development, China's 2026 Regulatory Data Protection (RDP) measures provide six years of protection for innovative medicines, including those first approved outside China. However, certain improved medicines are limited to four years if they do not meet China's restrictive "new drug" definition. In addition, PTE remains restricted to "innovative drugs" and certain "improved new drugs". According to the definition in Registration Classification of Drugs, this refers to drugs that have not been approved in other countries before submitting applications in China, following the 'new-to-the-world' standard. Also, the protection scope during the extended patent term is confined to the approved new drug, specifically limited to the relevant technical solution for the approved indication. Finally, the narrow scope of PTE protection may have unintended consequences, which may potentially impact the scope of protection of innovative products.

Patent Linkage (Pharmaceuticals): In 2021, the new law and various measures were released to implement the patent linkage system in China. While aspects of an effective early dispute resolution system are reflected in these measures, the system still has deficiencies. For example, there is no procedure that provides for patent certification modification or opposition. Moreover, ANDA filers can circumvent patents that are listed on the PL platform by using a different dosage form. This patent linkage system must be improved in a manner that advances innovation: 1) ANDA filers should make certifications with respect to relevant patents they know or should have known listed in the PL system even if these patents are technically listed for a different product having the same API (e.g., a product with different dosage form). 2) ANDA filers should be afforded an opportunity to amend/correct their statements.

Delayed Review of Patent Applications (Pharmaceuticals): An unreasonable delay at the patent office (CNIPA) has resulted in China's National Medical Products Administration (NMPA) approval of generic versions of products that have a patent pending.

Services Barriers

Electronic Payment Services: When China joined the WTO in 2001, it committed to allowing non-Chinese EPS companies to compete and do business in its domestic market on equal terms with Chinese companies, including by processing renminbi-denominated transactions in China. While other EPS suppliers were eventually able to secure licenses, PBOC has been delaying action on the licensing application submitted by another U.S. supplier, Visa. On October 10, 2026, Visa received approval of its "Application to Prepare" from PBOC, which allows Visa to begin formal preparations to establish a domestic bankcard clearing institution in China. We urge USTR to closely monitor the formal application process and we encourage continued prioritization to ensure all leading EPS suppliers are authorized and fully licensed to operate in the market.

Restrictions on Cloud Computing: Even though U.S. cloud service providers ("CSPs") have stimulated innovation and application of cloud services around the world, China's regulators impose market access restrictions for foreign companies, which require Value-Added Telecoms ("VAT") licenses. China has launched "pilot" programs to open its cloud market in Beijing, Shanghai, Shenzhen and Hainan "free trade zones," but CSPs still need to fulfil the previous localization requirement.

Market Access for Cloud Services: China implements a licensing system for telecommunications business operations. Only companies established in China, after obtaining a telecom business license, can engage in telecom business activities. Foreign companies' participation in the value-added telecommunication (VAT) sector is highly restrictive. Based on *Telecommunications Regulations of the People's Republic of China*, *Classification Catalogue of Telecommunications Services*, and *Special Administrative Measures for Foreign Investment Access (Negative List) (2021 Version)*, foreign companies are still denied access to the business sectors critical to cloud services nationwide, namely B11 Internet data center (IDC) business, and B12 content distribution network (CDN) service. Although the Ministry of Industry and Information Technology announced the expansion of the opening-up of VAT sector on a pilot basis in April 2024, the opening-up is only limited to four designated areas (Beijing, Shanghai, Shenzhen and Hainan "free trade zones"), posing commercial and technical difficulties for cloud service providers with interconnected data centers both inside and outside those areas.

In addition, China imposes sector-specific requirements for cloud services in industries such as financial services and smart vehicles, in effect prohibiting the usage of public cloud services. These unfair restrictions are exacerbated by other market access restrictions: connectivity requirements, restrictions on the ability to engage in cross-border data transfers, and requirements to localize computing infrastructure. Many international financial institutions and vehicle manufacturers are unable to use public cloud services globally for enhancing operational resilience and efficiency, and achieving consistent internal standards (e.g., risk management functions).

Critical Information Infrastructure. The CII Security Protection Regulation, effective from September 1, 2021, mandates enhanced protection of CII. This regulation promotes the procurement of "secure and trustworthy" network products and services, potentially resulting in unequal treatment between domestic and foreign companies' products. Companies identified as CII operators face additional obligations under Chinese security legislation, including mandatory certification, assessment, and cybersecurity reviews. In a similar vein, the concept of "important data" was introduced in Article 37 of the Cybersecurity Law (CSL) in 2017. In recent years, a series of guidelines have been continuously issued to guide data processors in data classification and identification of important data, imposing an increasing compliance burden on companies that own important data. Moreover, the ambiguous definitions and opaque recognition criteria for CII and important data, coupled with the expanding application by industry

regulators, have created high compliance burdens and potential entry barriers for foreign companies seeking access to certain industries or customers.

Cybersecurity Review: The *Cybersecurity Review Measures (CSRM)* were revised on January 4, 2022, making it mandatory for CII operators procuring network products and services, and online platform operators conducting data handling activities that influence or may influence national security, to proactively apply for a cybersecurity review. The review is an opaque process, presumably assessing a host of factors, including the security, openness, transparency, and diversity of sources of products and services; the reliability of supply channels, as well as the risk of supply disruptions due to political, diplomatic, and trade factors. For example, the Cyberspace Administration of China (CAC) launched and failed a cybersecurity review of Micron in early 2023, resulting in a demand for CII operators to stop purchasing its products. With vague criteria and broad scope, China's cybersecurity review regime could be abused and used to discriminate against foreign technology providers, thus creating entry barriers for many MNCs.

Secure and Controllable ICT Policies: The Chinese government has implemented secure and controllable ICT policies through various laws and regulations, including the *Cybersecurity Review*, the *Critical Information Infrastructure Protection Measures*, and the *Cryptography Law*. These policies have been reinforced under the banner of technological self-reliance and security since the 14th *Five Year Plan* in 2021. In practice, these policies have been widely used, creating obstacles for foreign ICT products to get into sectors ranging from government, CII operators, and even State-Owned Enterprises (SOE). In past years, the concept of SOE Cloud and State Cloud in China has further exemplified the policy.

Encryption Requirements: China's 2019 Cryptography Law includes restrictive requirements for commercial encryption products that "involve national security, the national economy and public interest" which must undergo a security assessment, including critical information infrastructure. This has resulted in unnecessary restrictions on foreign ICT products and services. Recent regulations have added to concerns that China's encryption requirements are being used to discriminate against American companies. For example, China amended the Commercial Cryptography Administrative Regulations in April 2023. The amended regulations fail to support interoperable international standards and use internationally standardized encryption algorithms. Furthermore, the regulations reflect an extensive import license/export control scheme and impose requirements applicable only to CII and party and government organs to networks above Multi-Level Protection Scheme ("MLPS") level three.

Furthermore, on October 7, 2023, the State Cryptography Administration ("SCA") published the Administrative Measures for Security Assessment of Commercial Cryptography Applications (Measures), which came into effect on November 1, 2023. The measures proposed the concept of Important Network and Information Systems without providing definitions. Unless these important ambiguities are favorably resolved, these regulations will impose unfairly high compliance costs and create entry barriers for American companies that rely on internationally accepted encryption algorithms.

Digital Trade Barriers / Data Localization and Cross-border Data Flow: China imposes complex restrictions on the storage, movement, and access to data across borders, making it very difficult and costly for foreign companies to manage their global operations. In 2021, China released *Personal Information Protection Law (PIPL)* and *Data Security Law (DSL)*, which, along with the CSL implemented in 2017, established an overarching regulatory framework on data. The framework sets out three pathways for the cross-border data flow, namely security assessments, protection certification and standard contracts.

On security assessment, CAC's *Measures on Data Exit Security Assessment*, effective from September 1, 2022, stipulate the requirements for cross-border transfer of important data and personal information by CII operators and other companies that reach certain thresholds of data. The Measures put forward specific requirements for data exit security assessment, stipulating that data processors shall conduct a data exit risk self-evaluation before applying for data exit security assessment. Alongside the Measures, the regulations and standards on protection certification and standard contracts of personal data cross-border flow were also promulgated, forming a cross-border personal data flow management mechanism.

Noting that the existing data transfer framework is impeding economic growth and impractical for domestic and foreign businesses operating in the global economy, on March 22, 2024, CAC promulgated new provisions on promoting and regulating cross-border data flows, which would limit instances in which the aforementioned cross-border personal data flow mechanism would apply or a data exit security assessment would be necessary. In particular, the new provisions allow that personal data transfers due to human resource management and contractual transactions, such as cross-border e-commerce, cross-border payments, plane ticket purchases and hotel bookings, and visa applications be exempted under the cross-border personal data flow management mechanism. While the new provisions do not further elaborate on the scope of "important data", they stipulate that data processors are not required to apply for a data exit security assessment if they have not been notified by the relevant authorities, or if the data has not been publicly declared as important data. Pilot Free Trade Zones within Beijing, Tianjin, Shanghai and Hainan may also develop their own negative list of data for which the cross-border personal data flow mechanism would not apply. Beijing, Tianjin and Shanghai authorities have started to publish such negative lists.

While the People's Bank of China, the National Financial Regulatory Administration, the China Securities Regulatory Commission, the State Administration of Foreign Exchange, CAC, and the National Data Administration jointly issued the *Compliance Guidelines on Promoting and Regulating Cross-border Data Flow in the Financial Sector* in April 2025, the guidelines were only shared with selected financial institutions, making it difficult for the industry and other related stakeholders such as technology services providers to work out viable compliance measures with the regulators

Market Access for Aviation: The Civil Aviation Administration of China (CAAC) has implemented various policies and directives that pair specific top-tier hubs with one or two dominant state-backed carriers which discriminates against foreign flagged air carriers. Preferential slots allocation (which include securing prime peak-hour landing and departure times and terminal space) and other benefits are disproportionately granted to "champion" airlines. We continue to request that USTR advocate for more flexibility and predictability in CAAC's cargo slots allocation regime so cargo airlines can respond more nimbly given the international trade environment dynamics, which are distinct from passenger airline needs.

Anticompetitive Practices

Domestic Substitution: In recent years, China has enacted a range of industrial policies aimed at promoting its own technological self-sufficiency to reduce the dependence on American technology. In particular, China's "secure and controllable" measures put American companies at a severe disadvantage against Chinese firms. For over ten years, China has required its public sector and state-owned enterprises to purchase so-called "secure and controllable" Chinese products; it has also imposed domestic research and development ("R&D") requirements and considers the location in which R&D was conducted as a cybersecurity risk factor. These "secure and controllable" standards are not transparent, and are not accessible to American companies.

Colombia

Import Policies

Invoicing: Colombia allows traders to submit electronic copies of invoices; however, a physical copy must still be attached to the shipment. While the Colombian Government has reported ongoing efforts to upgrade its customs digital systems, progress has been limited, and no definitive timeline has been confirmed.

Advanced Customs Declaration Requirements for Imports: Colombia's customs service is implementing changes under Decree 659 of 2024, requiring advanced customs declarations for all non-express shipments. DIAN demands the full dataset for an import or transit declaration at least 48 hours in advance of arrival across all modes of transportation. These long lead times far exceed U.S. requirements, threatening to significantly delay imports while shipments sit at the port until the lead time passes. Notably, there are currently no exceptions for perishable goods, and failing to file full information sufficiently in advance triggers heavy fines.

NFTC strongly recommends that USTR actively urge the Colombian government to align its customs procedures with established international standards. Implementing a maximum four-hour prearrival reporting window for air cargo, aligned with the WCO SAFE Framework, would bridge the gap between customs security and commercial realities. NFTC urges USTR to advocate for immediate exemptions for perishable goods and the removal of disproportionate penalties, ensuring that U.S. exports do not face artificial delays and punitive measures at Colombian ports.

Proposed Elimination of De Minimis Exemption: Colombia is advancing legislative actions which seek to eliminate the de minimis VAT exemption by reducing it to zero dollars for low-value import shipments and generate additional data requirements. Eliminating this exemption would force thousands of small packages into formal clearance channels, overwhelming strained customs resources and destroying the economic viability of bilateral retail transactions for American small businesses. NFTC recommends that USTR aggressively engage the Colombian Ministry of Finance to preserve the de minimis threshold and facilitative import measures as a foundational trade facilitation baseline, protecting the competitiveness of U.S. exports.

Customs Sanctions and Merchandise Forfeiture Regime: Colombia's new customs sanctions and merchandise-seizure regime, enacted under Law 2586 of 2026, establishes severe, disproportionate sanctions for postal and express shipment intermediaries. The law imposes punitive fines of approximately \$13,000 per transaction for minor offenses and permits the physical seizure of goods for simple discrepancies in declared shipment descriptions. This regime places an unreasonable premium on strict documentation accuracy over trade facilitation, treating minor clerical errors as fraudulent activities and introducing massive legal liabilities for U.S. e-commerce operators. NFTC recommends that USTR urge the Colombian government to ensure proportional enforcement. It is critical that Colombia enforces a penalty framework that respects international trade facilitation standards and provides a reasonable safe harbor for non-fraudulent administrative errors.

Application of Single-Use Plastics Import Tax: Colombia implemented a single-use plastic packaging tax that legally burdens importers, but customs authority DIAN improperly shifted this responsibility onto express delivery operators. This mandate creates an impossible compliance standard, as transport intermediaries lack the visibility and proprietary data to determine the exact plastic content within sealed third-party shipments. Forcing carriers to sign sworn estimates creates a high risk of fraudulent

documentation penalties. NFTC strongly recommends that USTR request an administrative resolution from the Colombian government explicitly exempting express delivery carriers from this tax, ensuring environmental rules correctly target actual producers and importers.

Technical Barriers to Trade

The National Food and Drug Surveillance Institute (INVIMA) delays: In recent years, the pharmaceutical industry has experienced worsening delays in regulatory approval times, resulting in significant market access barriers. In November 2023, the Administrative Court of Cundinamarca issued an emergency measure in response to the growing shortage of drugs in Colombia due to the delays in regulatory approvals. The Court mandated a contingency plan, developed jointly by INVIMA and the Ministry of Health, detailing necessary actions to reduce the shortage of drugs in Colombia, including accelerating regulatory approvals. This order was revoked by the Consejo de Estado, eliminating the obligation for INVIMA and the Ministry to proceed with these plans. In December 2024, the Administrative Court of Cundinamarca again mandated the continuation of an urgent response plan to address ongoing medicine and supply shortages.

Substandard biologics regulation: On September 18, 2014, Colombia issued Decree 1782, which establishes marketing approval evaluation requirements for all biologic medicines. As part of the Decree, Colombia created an unprecedented “abbreviated” pathway for the registration of non-comparable products, which is inconsistent with WHO guidelines and accepted standards in the United States and other countries, and which could result in the approval of medicines that are not safe and/or effective. Industry urged the Colombian Government to remove this third pathway from the Decree but was unsuccessful.

Restrictive Definition of Broadband: Colombia's Communications Regulation Commission (CRC), through Resolution CRC 8307 of 2026, has modified the country's broadband definition to set minimum thresholds of 300 Mbps download / 150 Mbps upload for broadband and 1,000 Mbps download / 500 Mbps upload for ultra broadband. While the intent to update the existing 25/5 Mbps standard was broadly supported by industry stakeholders, the new thresholds far exceed evidence-based international benchmarks. By comparison, the U.S. Federal Communications Commission updated its fixed broadband benchmark to 100/20 Mbps in March 2024. The FCC had also established a long-term aspirational goal of 1,000/500 Mbps for ultra broadband; however, in July 2025, the FCC under Chairman Brendan Carr issued a Notice of Inquiry to reconsider that standard, finding that a 1,000/500 Mbps goal "may be unreasonably prejudicial to technologies such as satellite and fixed wireless that presently do not support such speeds." In August 2026, the FCC formally abolished the gigabit speed goal in its Section 706 broadband deployment report, adopting a technology-neutral framework that does not set an ultra broadband benchmark that would disadvantage non-fiber platforms. The CRC's own functional analysis similarly points to approximately 100 Mbps as the relevant threshold for current consumer use in Colombia, yet the CRC has moved in the opposite direction of the FCC by codifying an ultra broadband standard that the United States has expressly rejected.

The CRC's new thresholds are problematic because they effectively exclude non-fiber technologies — including satellite and fixed wireless platforms — from qualifying as broadband, thereby undermining the very digital inclusion objectives the proceeding sought to advance. Setting speed floors that only fiber networks can meet discourages investment in the diverse mix of technologies needed to close Colombia's digital divide, particularly in rural and underserved areas where terrestrial fiber deployment is not economically viable. The FCC's decision to eliminate its own gigabit aspirational goal underscores the growing international consensus that broadband definitions must remain technology-neutral to encourage

deployment across all platforms. Accordingly, the CRC should modify Resolution 8307 to adopt a broadband standard of 100/20 Mbps and an ultra broadband standard that does not foreclose participation by satellite and wireless providers, ensuring that regulatory definitions promote — rather than impede — investment across all platforms and geographies.

Government Procurement

Restrictive Cloud Services Procurement: Colombia's new Public Cloud Framework Agreement (AMP V) has been in operation since March 5, 2026 and creates security and market-access risks for U.S. cloud providers. First, AMP V does not require internationally recognized security certifications such as FedRAMP or equivalent. This allowed PRC-headquartered Alibaba Cloud and Huawei Cloud to enter the catalog for the first time and compete to host Colombian government workloads. Second, Clause 37 ("Data and Information Repatriation and Digital Sovereignty") requires buyer entities and providers to assess whether the provider has cloud infrastructure in Colombia. Where this is viable, systems and data must be repatriated to Colombian territory, with the costs chargeable to the buyer entity. The clause rewards where infrastructure is located rather than how secure it is. Because trusted-supplier standards are also absent, it risks moving sensitive government data onto PRC-controlled local infrastructure that is subject to China's 2017 National Intelligence Law, which would undermine bilateral security cooperation. In parallel, Presidential Directive 06 of 2025, which remains in force, allows national entities to contract the majority state-owned Internexa S.A. directly as a "public innovation laboratory," bypassing competitive procurement. These measures potentially infringe the U.S.–Colombia Trade Promotion Agreement (USCTPA) non-discrimination commitments in government procurement and cross-border trade in services. Colombia should remove Clause 37, require internationally recognized security certifications (FedRAMP, ISO/IEC 27001/27017/27018, SOC 2 Type II or equivalent) as eligibility criteria, and revoke Directive 06.

Intellectual Property Protection

Compulsory licensing (Pharmaceuticals): The threat of unmitigated compulsory licensing in Colombia is a continued risk for the innovative biopharmaceutical industry. In April 2024, the Colombian Government issued a compulsory license (CL) on an antiretroviral medicine on vague and ambiguous grounds. Since that action, the Ministry of Health (MoH) has publicly signaled its desire to use the threat of CLs as a price “negotiation” tool despite other and more effective options that would not compromise incentives for innovation.

Regulatory data protection (RDP) failures: Colombia fails to respect existing legislation that would otherwise provide RDP upon approval of novel pharmaceutical products.

Restrictive patentability criteria: Contrary to its obligations under the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Colombia does not grant patents for second uses.

Effective patent enforcement: Despite having a specialized court under the auspices of the Superintendence of Industry and Commerce (SIC) designed to address IP infringement matters, Colombia needs to implement effective early resolution mechanisms that provide for the timely resolution of patent disputes before marketing approval is granted to infringing follow-on products during the patent term through increased collaboration between INVIMA and SIC.

Services Barriers

Taxation of the Digital Economy: Colombia faces a significant fiscal gap, formally requested IMF support in September 2026, and is widely expected to pursue a new tax reform. In the past, tax reforms have targeted digital services in ways that unfairly affect U.S. companies. Tax Reform Bill 004 of 2026, filed by the outgoing administration, proposed several measures to tax the digital economy. These included an increase in the Significant Economic Presence (SEP) rate from 3% to 5%; a tax on the gross revenue of non-resident digital suppliers (Article 57 of Law 2277 of 2022); the elimination of the VAT exclusion for web hosting and cloud computing services; and the elimination of the current benefits for U.S. cross-border e-commerce shipments. The current administration rejected that bill, but these three measures could return in the new reform. Colombia should avoid any new tax measures that target U.S. digital companies.

Restrictive Network Usage and Digital Service Regulations: Colombia's proposed "Internet Solidarity" bill, introduced in August 2025, creates a new trade barrier through excessive regulation of digital services, despite the Communications Regulatory Commission's (CRC) earlier finding against implementing "Fair Share" contributions. The legislation establishes a new "Digital Intermediary Service Providers" category that subjects U.S. cloud providers to burdensome registration requirements, mandatory authority cooperation, and content moderation obligations. The bill's broad scope and six-month implementation timeline for regulations create significant operational uncertainty for U.S. technology companies. Of particular concern is the combination of expanded CRC authority to demand provider information while establishing internet access as a fundamental right, potentially enabling future implementation of network fees or similar financial obligations that could disadvantage U.S. providers in the Colombian market.

Electronic Payment Services (Tax): The tax regulation establishes income, VAT and other municipal withholding taxes applicable to credential payments. However, this regulation has not evolved with the financial industry and has not been applied to identical payments made by newer payments systems such as digital wallets, QR code payments, e-commerce payment buttons, the public real-time payment system (Bre-B), which is now operating, and other payment methods such as cash. This discourages the adoption of card acceptance among merchants. Withholdings sum up to ~5% of transaction amount: Income: 1.5%, VAT: 2.85%, Municipal Tax: ~0.4%. The reduction in cash flow for merchants derived from accepting credential payments constitutes a significant barrier to the general adoption of credential payments acceptance. These tax asymmetries create unjustified advantages for companies participating with other payment methods (cash, QR, transfers) and prevent the fully successful deployment of US credential companies in the country's payment ecosystem.

Intermediary Liability: Colombia has not met its 2006 U.S.-Colombia Free Trade Agreement (FTA) obligations regarding Internet service provider protections. A 2018 revision to its copyright law omitted online intermediary protections, leaving intermediaries that export services to Colombia vulnerable to civil liability. The law also lacks standard exceptions like text and data mining. A new AI bill (Bill 043/2025) further compounds concerns, imposing a "permission-first" regime requiring express consent from rights holders for AI training. This approach would create insurmountable barriers to AI development and deployment, increasing legal uncertainty for online services in Colombia.

Investment Barriers

Cost containment measures focused solely on the biopharmaceutical industry: Government measures to improve the sustainability of the Colombian health system have focused solely on the biopharmaceutical industry and have not addressed broader issues within the pharmaceutical supply chain or other health care sectors. For example, in 2020, the Colombian Government issued regulations to limit

expenditures on medicines not included in the publicly funded Health Benefit Plan (HBP) based on historical levels that would effectively restrict new innovative medicines from entering the country. These measures have been criticized for their technical shortcomings by virtually all sectors of the health system and academia.

New drug price regulation methodology: A draft circular was published by MOH in September 2023, outlining a new method for pricing new medicines. In addition to international reference pricing (IRP), it established a value-based pricing model based on clinical value assessments undertaken by the *Instituto de Evaluación Tecnológica en Salud* (IETS). In March 2024, the National Drug Pricing Commission (NDPC) issued Circular 18 of 2024 adjusting the methodology for regulations in place since 2013. This Circular allows for more restrictive IRP by expanding the number of reference countries from 17 to 19 and cherry-picking countries to include those that are less supportive of innovation. In addition, if a drug is declared by the government to be of public interest, then the price will be set to the lowest price in the reference basket of countries.

The Superintendency of Commerce issued Resolution 35379: This resolution authorized the intervened HMOs to jointly coordinate purchasing processes for high-cost medications (invoking an exception to competition regulations) with the goal of leveraging collective bargaining power to secure price reductions and curb escalating pharmaceutical expenditures. However, the implementation of these measures has triggered significant legal and regulatory uncertainty. The resolution compels companies to sell directly to HMOs—entities whose financial standing remains precarious—while obliging the industry to absorb the costs of dispensing and delivering medications, all under a regime of prices significantly below established regulatory thresholds.

Costa Rica

Technical Barriers to Trade

Market Access Delays (Pharmaceuticals): It can take up to 18 months for pharmaceutical products to progress from approval to registration due to human resource issues. While mechanisms exist to expedite the review of high-standard medicines, they lack the efficiency to manage the volume of requests and reduce response times—resulting in significant delays. To address inefficiencies in current regulatory mechanisms, it is crucial to establish systems that prioritize medicines targeting unmet medical needs and those already authorized by high-standard regulatory agencies.

Customs Procedures and Trade Facilitation Barriers: Despite CAFTA-DR Article 5.7 commitments, Costa Rica has failed to implement digital systems for pre-arrival manifest processing, preventing advance risk assessments. Furthermore, Customs strictly requires formal Spanish translations for all non-Spanish commercial invoices. This adds no risk-control value, driving up administrative costs and causing unnecessary clearance delays. Invoices issued in English should be exempt from translation, provided key fields like value, currency, Incoterms, and clear descriptions of the goods are present on the documentation.

Additionally, Costa Rica included a *de minimis* framework in its new customs law in 2023, establishing a threshold of 100 Central American Pesos (USD 100 FOB) that exempts duties while assessing a 13 percent value-added tax. However, the government has yet to implement the specific regulations allowing its application. This inaction leaves low-value U.S. e-commerce exports subject to disproportionate fees and delays. NFTC recommends that USTR initiate CAFTA-DR compliance reviews to compel IT modernization, secure the acceptance of English-language invoices, and press for the immediate

operationalization of the stalled de minimis threshold.

Services Barriers

Extraterritorial application of local regulation (EPS): Costa Rica is exerting extraterritorial authority over U.S. Electronic Payment Services providers (EPS) and U.S. banks through a Central Bank of Costa Rica's (BCCR) regulation of inbound cross-border payments. In March 2020, the Congress of Costa Rica enacted Law 9831 granting the Central Bank of Costa Rica (BCCR) authority to set price control measures to the card payments system, including a wide range of electronic service providers with operations in Costa Rica. In November 2022, the BCCR updated its regulation and capped among others, the international Interchange Reimbursement Fee (XB IRF), and the international Merchant Discount Rate (XB MDR). This measure restricts U.S. commerce of digital services by setting a cap on the fees that U.S. banks can charge for transactions conducted in Costa Rica using debit or credit credentials issued in the U.S. As a result, this regulation affects commercial agreements between U.S. EPSs and U.S. banks, even though these agreements are governed by U.S. law.

The BCCR's regulation of inbound cross-border payments favors Costa Rican entities to the detriment of U.S. banks and EPS suppliers. The regulation disproportionately affects U.S. banks as the 60% of inbound cross-border transactions in Costa Rica are with payment credentials issued by U.S. banks.

NFTC recommends that USTR urge Costa Rica to withdraw the extraterritorial provisions established by the BCCR that affect the business operations of U.S. financial institutions regarding cross-border card payment transactions. Specifically, we recommend the removal of Article 44 and any references to cross-border transactions since they fall under the jurisdiction of countries other than Costa Rica.

Tax Asymmetry: While tax withholdings on card payments continue to create an uneven playing field for U.S. EPS, a proposal from the Costa Rican Ministry of Finance to address this issue has stalled. The plan, which would extend tax withholdings to include the Central Bank's mobile payments platform, Sinpe Móvil, has faced strong opposition from the Central Bank, political actors, and the general public, reducing its viability.

We urge USTR to emphasize to Costa Rica the critical need for an equitable payments ecosystem, highlighting the direct negative impact of the current fiscal asymmetry on U.S. EPS and proposing a definitive solution: either impose the withholding tax across all payment methods or eliminate it entirely.

Dominican Republic

Services Barriers

Extension of Telecommunications Regulation to Cloud and Digital Services (Draft General Law on Telecommunications, Digital Infrastructure and Connectivity): The Dominican Republic is considering a draft General Law on Telecommunications, Digital Infrastructure and Connectivity that would extend sectoral telecommunications obligations to cloud computing, data centers, content delivery networks, and other information-society services through an undefined concept of "functional linkage." This premise is technically and legally flawed: cloud providers supply computing, storage, and analytics building blocks used across all sectors; they do not transmit signals over public networks, use public spectrum, or provide a public telecommunications service, and their relationship with telecommunications operators is a customer-supplier relationship. Because the "functional linkage" trigger sets no threshold of

control, indispensability, or territorial impact, the regulated perimeter can expand by later regulation or case by case, sweeping in facilities and providers that perform no telecommunications function and could even be labeled "critical telecommunications infrastructure" (Arts. 1–3, 4.1, 5). These obligations are technically unworkable under the cloud shared-responsibility model, in which providers secure the infrastructure "of" the cloud while customers control security "in" the cloud and providers have no visibility into customer workloads. The resulting uncertainty would deter investment and slow digital adoption. The Dominican Republic should confine the law to the conveyance of signals over public networks and the scarce resources that support them, and add an explicit, unconditional exclusion for computing, storage, hosting, database, analytics, artificial-intelligence, content-delivery, and managed-DNS services as information-society services outside its scope.

Ecuador

Import Policies

Customs Clearance Procedures and Inspection Bottlenecks: Ecuador import processes include highly duplicative procedures that severely undermine supply chain efficiency. Express companies must apply physical, Ecuador-specific labels to packages containing information already provided via electronic air waybills, where a single error detains entire consolidated shipments. Local customs authorities impose recurring, rigid fines per transmission for minor manifest discrepancies and simple piece count mismatches. Furthermore, operators are forced to weigh each package three separate times, increasing operational costs. Under the Agreement on Reciprocal Trade (ART) with the United States, Ecuador explicitly agreed to remove requirements for individual Master Airway Bill labeling, eliminate reweighing protocols, and implement periodic payment systems. However, these commitments remain completely unfulfilled. These punitive practices cause critical clearance delays, severe service failures, and drastic increases in operational costs, preventing U.S. exporters from reliably reaching the Ecuadorian market.

NFTC recommends that USTR engage Ecuadorian authorities to immediately codify the mandatory regulations agreed upon under the ART, specifically eliminating duplicative labeling and reweighing for trusted operators. USTR should press Ecuador to establish a risk-based, selective screening process rather than blanket X-ray inspections and eliminate disproportionate fines for minor manifest discrepancies. Finally, USTR must formally request that Customs allocates sufficient resources to accommodate the clearance of the growing U.S. express export volumes, restoring predictability and efficiency to the bilateral supply chain.

Imposition of Tax on Express Shipments: Ecuador's Category B courier regime imposes non-tariff barriers hindering U.S. exports through restrictive weight and frequency limits, alongside a mandatory \$20 per-shipment fee. This fee artificially raises costs, discouraging small-scale digital trade. Exacerbating these burdens, Ecuador recently issued Bulletin 75, arbitrarily reinterpreting the Organic Code of Production, Commerce, and Investments to abruptly eliminate the tax exemption for Category B express shipments. Authorities now collect a 0.5 percent FODINFA (Children's Development Fund) tax on these imports, increasing transaction costs and disrupting established regional clearance practices. NFTC recommends that USTR urge Ecuador to eliminate the \$20 fee, ease Category B limits, and formally amend customs regulations to permanently exempt fast-track courier imports from the FODINFA surcharge, preserving market access.

Government Procurement

Mandatory Cloud Procurement Through State-Owned Telecommunications Companies: Ecuador requires public sector entities to procure cloud computing services through government-owned telecommunications companies, principally the National Telecommunications Corporation (CNT), rather than contracting directly with cloud service providers. The requirement derives from Ministerial Agreement No. 141 (MINTEL, 2011), which was expanded in 2019 to cover cloud and other digital services for all public entities; after a brief exclusion of cloud services in 2023, MINTEL reinstated the mandate. Although forced data localization was eliminated through the Fintech Law reform of the Ingenios Code—allowing government data to be stored outside Ecuador—the obligation to contract cloud through CNT when serving the State remains in force. The mandatory intermediary increases costs, slows service delivery, and creates anti-competitive effects, since all U.S. providers must route sales through the same state-owned entity. Ecuador should allow public entities to procure cloud directly from qualified providers on a technology-neutral basis, through a transparent framework that does not mandate intermediation by state-owned telecommunications companies.

Services Barriers

Restrictive Artificial Intelligence Regulations: Ecuador's proposed artificial intelligence regulations, introduced by the Data Protection Authority (SPDP), represent a significant trade barrier that threatens U.S. companies' market access and operational capabilities. The "Regulation for the Guarantee of Personal Data Protection Rights in the Use of Artificial Intelligence" creates multiple compliance challenges through jurisdictional overreach, as it conflicts with Ecuador's Digital Transformation Law (LOTDA) which designates MINTEL as the AI governance authority. The regulation imposes discriminatory operational burdens on foreign technology providers through mandatory human supervision requirements, complex traceability standards, and expansive audit rights. Of particular concern are the blanket prohibitions on crucial AI applications, including real-time biometric identification systems and synthetic content generation, which effectively bar U.S. companies from deploying innovative technologies in the Ecuadorian market. These restrictions, coupled with excessive compliance costs, create disproportionate barriers for U.S. businesses, especially affecting technology startups and SMEs. The proposed framework contradicts Ecuador's international commitments to facilitate digital trade and promote technological innovation, while establishing unnecessary obstacles that particularly impact U.S. companies' ability to compete effectively in Ecuador's digital economy.

Electronic Payment Services: Current tax regulation establishes income and VAT withholdings applicable to credential payments which discourage the adoption of card acceptance among merchants. Simplified tax regimen "RIMPE" establishes an exemption from these withholdings only for taxpayers (individuals and legal persons) with an annual income ranging from USD 1 to USD 20,000, but any other taxpayer is subject to withholdings up to ~13% of transaction amount. The reduction in cash flow for merchants derived from accepting credential payments constitutes a significant barrier to the general adoption of credential payments acceptance and prevents the fully successful deployment of US credential companies in the country's payment ecosystem.

Egypt

Services Barriers

Electronic Payment Services: Central Bank of Egypt (CBE) ambitions to promote domestic payment infrastructure (scheme) and push for co-badge with international payment networks is forcing such networks to adjust their business models in accordance with the government's political ambitions to enhance domestic payment infrastructure rather than independent / market-led commercial ambitions.

The Central Bank of Egypt had introduced FX-management measures during the 2022-2023 foreign currency crisis, including cross-border debit card restrictions. Cross-border use of debit and prepaid cards remains restricted despite improving macroeconomic and FX conditions. The restrictions limit consumer choice, digital commerce, and international transactions. USTR should urge Egypt for a gradual, controlled reactivation supported by spending limits, real-time monitoring and targeted risk controls.

Data Localization Requirements: The Personal Data Protection Law, which aims to regulate data collection, processing, and storage, is awaiting the release of its Executive Regulations (ERs). These ERs, initially anticipated in early 2025, will provide businesses with specific compliance guidelines and introduce a one-year transition period after issuance. The delay in their release, reportedly due to recent political and crisis management priorities, has left businesses in a state of uncertainty.

Content Regulation: In 2018, Egypt enacted a law requiring all social media users with more than 5,000 followers to obtain a license from the Supreme Council for Media Regulation (SCMR). Additionally, in May 2020, Decree No. 26 of 2020 established a detailed licensing regime for media and press outlets, including online platforms. This regulation requires platforms to remove harmful content within 24 hours and obligates international companies to establish a local representative office to provide legal liability and act as a point of contact for content-related matters. Licensing fees for international platforms are set at EGP 3,000,000, and there are no explicit safe harbor protections for foreign companies, which may increase compliance complexity.

In June 2024, the SCMR reiterated its licensing requirements, issuing notifications to all digital and satellite platforms operating in Egypt to comply with relevant regulations under Law No. 180 of 2018, Prime Ministerial Decree No. 418 of 2020, and SCMR Decision No. 29 of 2020. Platforms were given a 90-day grace period to regularize their status, with potential consequences for non-compliance, including financial penalties, service blocking, or license revocation. The enforcement of these requirements is supported by the National Telecommunications Regulatory Authority (NTRA) and the Central Bank of Egypt (CBE), which can restrict payments and access to non-compliant platforms.

While the SCMR has primarily focused on over-the-top (OTT) platforms such as regional streaming services, international platforms face additional requirements to meet compliance standards. Social media platforms, although not the current primary focus, also fall under the same regulations. While Decree No. 92 of 2020 introduced an accreditation model for social media platforms, offering a less demanding alternative to licensing, the accreditation model is not widely emphasized by the SCMR, and platforms are often guided toward pursuing full licensing. This can introduce additional operational and financial requirements, particularly for international entities navigating Egypt's regulatory environment.

El Salvador

Government Procurement

Lack of regulatory framework for MEAs: A significant barrier to accessing innovative medicines is the absence of regulatory frameworks that facilitate negotiations through managed entry agreements (MEAs) within public procurement systems. Without a structured framework for managed entry agreements, healthcare systems face challenges in incorporating innovative treatments into their formularies—ultimately limiting patient access to cutting-edge therapies. Implementing clear and structured regulatory frameworks that facilitate managed entry agreements can enable effective negotiation of prices and terms for innovative medicines. Additionally, adopting value-based pricing models helps ensure that the cost of innovative medicines reflects their clinical benefits, while making them more accessible to patients.

Intellectual Property Protection

Inadequate regulatory data protection (Pharmaceuticals): El Salvador does not provide adequate protection for undisclosed test data or other data generated to obtain marketing approval for pharmaceutical products, leading to possible unfair commercial use and unauthorized disclosure by third parties. El Salvador should align its regulatory data protection standards with global norms to prevent unfair treatment of American innovation and meet its IP obligations under CAFTA–DR.

Ethiopia

Services Barriers

Electronic Payment Services: In 2023 the National Bank of Ethiopia opened up the digital payment market to issue payment instruments and operate payment systems licenses to foreign operators. Kenya-based Safaricom has obtained a license to issue payment instruments with a reportedly high investment protection fee (USD 150M). A high investment protection fee to allow international payment networks to obtain a license to operate payment systems may be a barrier to allowing more international companies the opportunity to operate in the market and generate economic growth.

The European Union

Import policies

Fragmented Extended Producer Responsibility Requirements: U.S. small businesses selling goods into the EU face extended producer responsibility (EPR) obligations that vary across Member States and product categories, including separate registration, reporting and compliance requirements. A particular concern is the requirement in some regimes for producers established outside the EU to appoint a locally established authorized representative in every EU Member State. The EU has proposed simplifying authorized representative requirements for producers established within the EU, while largely preserving Member States’ ability to require them for third-country producers. This may leave U.S. SMEs facing significant fixed compliance costs even when selling only small volumes cross-border. The forthcoming broader reform of EU EPR rules under the Circular Economy Act will therefore be important for addressing fragmentation, proportionality, and the accessibility of compliance mechanisms for small foreign sellers.

Customs Reform and Low-Value E-Commerce Charges. Since July 1, 2026, the EU applies a flat €3 customs duty per line item to goods in consignments valued below €150, charged according to the categories of goods contained in the parcel. The new Union Customs Code also introduces an EU-wide handling fee of €2 per line item for all e-commerce shipments and a new “importer for distance sales” framework, under which either the seller or the platform facilitating the sale may assume the importer role depending on the arrangements between them. These changes create particular challenges for U.S. SMEs selling low-value, second-hand, vintage, collectible or unique goods, for which information such as manufacturing origin or detailed product classification may be difficult to obtain. Industry is also seeking clarity regarding the handling fee, implementation of the importer model in a way that remains aligned with limited intermediary liability under the DSA, and the transition to the EU Customs Data Hub.

Digital Product Passport. The EU is progressively introducing Digital Product Passport (DPP) requirements under the Ecodesign for Sustainable Products Regulation. The DPP Registry became

operational in July 2026, with requirements applying first to certain batteries in 2027 and subsequently expanding to additional product groups. U.S. stakeholders have already raised concerns regarding implementation timelines and access to commercially sensitive information. Second-hand and legacy products present additional challenges because sellers may not have access to information held by the original manufacturer or to an existing DPP, particularly for products manufactured before the relevant requirements apply. Depending on how product-specific rules are designed, requirements to provide or verify complete DPP information could therefore create barriers to legitimate cross-border trade in used and refurbished goods.

European Product Act. The European Commission is preparing a European Product Act to update EU product compliance and market surveillance rules. Early Commission drafting raises particular concerns for U.S. sellers of second-hand and refurbished goods, which could continue to be treated similarly to newly manufactured products entering the EU despite sellers often lacking access to original technical documentation or the manufacturer. The approach could also make marketplace distribution dependent on manufacturer-controlled credentials, potentially allowing manufacturers to restrict downstream or secondary-market circulation. Proposed systematic pre-listing verification requirements could create additional barriers for U.S. SMEs using marketplaces to reach EU consumers and risk undermining the intermediary limited-liability framework established by the Digital Services Act. In addition, the draft envisages a new EU market surveillance fee on products imported from third countries, with differentiated treatment depending on how goods enter the EU, adding a further cost specifically to cross-border trade. The future framework should provide proportionate compliance pathways for imported used goods, preserve downstream distribution and avoid imposing discriminatory or unnecessary costs on legitimate U.S. exports.

Authorized Representative and Responsible Economic Operator Requirements. Since the 2019 Market Surveillance Regulation, EU product rules have increasingly required products sold from third countries to have an economic operator established in the EU. The General Product Safety Regulation subsequently extended this model to a much broader range of consumer products, and the European Product Act (see above) now risks expanding or reinforcing it further. For U.S. SMEs selling directly to EU consumers, particularly sellers of second-hand, refurbished, collectible or low-volume goods, the need to appoint an authorized representative or otherwise secure an EU-based responsible operator can create significant fixed costs and administrative barriers disproportionate to their level of trade. The EU should avoid further expanding these requirements without proportionate alternatives for legitimate third-country sellers and products for which the original manufacturer or another EU economic operator is unavailable.

Carbon Border Adjustment Mechanism (CBAM): The Carbon Border Adjustment Mechanism (“CBAM”) imposes a requirement on businesses to report on embedded emissions of imports. In EU’s CBAM also added a carbon price on imports in emission-intensive sectors (cement, iron, steel, aluminum, fertilizers and electricity) whose production/related emissions are not subject to the equivalent costs or regulation in the producer’s country. Importers are now required to purchase and surrender “CBAM Certificates” based on the average price of allowances under the EU’s Emissions Trading System (ETS).

Even for small imports, CBAM imposes a significant compliance burden. The first year of reporting created uncertainty as U.S. suppliers were forced to grapple with a lack of clear guidance, available tools, and time and resources invested in compliance. Over time, CBAM implementation will further raise costs for importers in Europe since free Emissions Trading Scheme (ETS) allowances will be gradually phased out. However, the full impact of this transition will largely be felt post-2030. Under a July 2026 European Commission proposal to reform the EU ETS, the phase-out of free allowances for CBAM sectors would be extended until 2038. Starting in 2031, retaining these free allowances will become conditional on companies investing an equivalent sum into verified decarbonization projects

within Europe.

The EU adopted a package of reforms in 2025. Under the revised scope, the EUR 150 de minimis exemption per consignment is replaced with an annual mass-based threshold of 50 tons of CBAM goods per importer. This exempts a range of businesses, especially SMEs. In addition, the first sale of CBAM certificates has been postponed to February 2027. These steps were welcome. The European Council adopted an approach that would significantly expand CBAM's scope starting in 2028. In doing so, the Council broadened the scope by adding over 200 more product codes with high iron, steel or aluminum content, including household refrigerators, heat pumps, boilers, turbines, and vehicle parts. This will lead to a major increase in the number of goods brought into the EU for which importers must acquire CBAM certificates. Contrary to the simplification proposal, it would materially increase the administrative and financial burden for importers in scope.

CBAM discriminates against products from countries like the United States that do not have equivalent carbon emissions pricing schemes in place.

EU Customs Rules: The EU adopted a major reform of its Union Customs Code (UCC) in September 2026. The revised UCC includes potentially positive changes for U.S. businesses, including the establishment of an EU Customs Authority and the development of an EU Customs Data Hub, a single digital portal for importers and exporters to interact with national EU customs authorities. As part of the broader reform, the EU eliminated its EUR 150 de minimis duty exemption on July 1, 2026. It will also introduce an EU “handling fee” for low-value consignments (essentially e-commerce) from November 2026.

Some of these changes were intended to take effect by 2028 when the EU Customs Data Hub is expected to be launched (initially only for e-commerce) to ease compliance. Political pressure caused by a surge in low-value-commerce imports, mainly from China, has led to some measures being implemented earlier. As of July 2026, the EU has introduced a “temporary regime” until 2028 under which imported goods in distance sales (B2C) with an intrinsic value below €150 are subject to a fixed €3 duty per item. In addition, declarants will be obliged to provide “product identifiers” (PIDs) for each good imported in distance sales from November 1, 2026. These are alphanumeric codes assigned to a specific model, batch, or article by the manufacturer and/or the merchant.

Not only are these requirements administratively burdensome, but the PID is an entirely new data element that is not currently required by any other customs administration in the world. Exporters therefore have no comparable prior obligation to draw on, and building the systems, data flows and internal processes needed to capture and transmit this information reliably will take considerable time, particularly for smaller B2C merchants and marketplaces who do not have the compliance infrastructure of major manufacturers. The EU has rushed implementation and given businesses a lead time of barely six months to comply.

Absent a transition mechanism, there is a material risk that PID data will not be available consistently and at scale from the application date, exposing importers and customs representatives such as express carriers to clearance delays, border bottlenecks and potential fines in Europe for reasons entirely outside their control. Some EU customs authorities, such as Ireland, have already informed the industry that import declarations will be rejected if PIDs are missing.

National Fee on Low-Value Shipments: In 2026 a number of EU countries advanced efforts for a €2 administrative fee on each non-EU shipment declared goods shipment of €150 or less. It applies

to business-to-consumer, business-to-business and person-to-person shipments, including those already registered under the EU's import VAT scheme (IOSS). Depending on the country, sporadic implementation efforts are now underway with some planning for implementation in the midst of Christmas peak shipping starting December 1, 2026. These country specific fees would stack on top of the EU's €3 duty per item and the planned EU handling fee. Repeated last-minute changes to the start date also force carriers to reprogram billing and clearance systems with only days' notice. NFTC recommends that USTR urge the EU to stop Member States from adding national fees on top of EU-wide charges for low-value shipments, and press countries to align with the launch of the EU customs hub.

France – payments sovereignty: Political debate on payments sovereignty in France has become more institutionalized. The French National Assembly's Inquiry Committee on France's digital dependencies and systemic vulnerabilities, initiated by the Ecologist and Social Group and chaired and reported by MP Cyrielle Chatelain, examined France's reliance on non-European providers across cloud, AI, digital infrastructure and payments. Its final report followed hearings with more than 100 stakeholders and included 18 recommendations and 29 policy proposals. The payments chapter presents domestic scheme Carte Bancaire (CB), pan-EU solutions (Wero) and the Eurosystem CBDC project (Digital euro) as assets supporting French and European strategic autonomy but does not recommend restrictions on international card schemes. However, given the stated goals of this Committee, USG should monitor developments to ensure this initiative does not lead to preferential treatment for domestic and pan-EU schemes over US competitors.

Technical Barriers to Trade

EU Corporate Sustainability Due Diligence Directive and Sustainability Omnibus Package: The EU's 2023 Corporate Sustainability Due Diligence Directive (CS3D) threatens to impose substantial and disproportionate compliance costs on U.S. businesses, particularly due to its extraterritorial scope. For many U.S. companies operating in the EU, the CS3D will impose sustainability-related due diligence requirements on their U.S. parent companies and any of their subsidiaries, impacting relations with suppliers anywhere in the world, regardless of the existence of a relevant EU nexus.

The 'Omnibus I Directive', which entered into force in March 2026, introduces amendments to the CS3D to reduce the administrative burden. These changes represent a step in the right direction, including: (1) focusing due diligence on direct suppliers and business partners; (2) only requiring companies in scope to request information from business partners with fewer than 5,000 employees when it cannot reasonably be obtained another way; (3) capping financial penalties at 3% of worldwide turnover (previously minimum 5% and potentially uncapped); (3) pushing back monitoring requirements from every 12 months to every five years; (4) eliminating mandatory EU-wide civil liability; and (5) delaying the application of the law to 2029 and the first reporting deadline to 2030. In addition, CS3D will apply to non-EU companies generating EUR 1.5 billion in annual turnover in the EU instead of EUR 450 million.

Nevertheless, some of the key issues for U.S. businesses remain unaddressed, including: (1) the law's unprecedented extraterritorial reach, which impacts supplier relationships across all subsidiaries, regardless of location and EU nexus; (2) requirements to adopt prescriptive due diligence systems across global operations, which will lead to costly and time-consuming risk management exercises; (3) burdensome supply chain obligations; (4) significant financial penalties; and (5) fragmented litigation risks, as national civil liability systems create significant legal exposure for U.S. businesses across 27 EU Member States, and finally (6) the complex and significant administrative burden.

EU Deforestation Regulation: The EU’s Regulation on deforestation-free products (“EUDR”) creates a due diligence process for companies regarding the import of deforestation-risk products such as palm oil, timber, cocoa, coffee, leather, wood, pulp and furniture, among others. U.S. companies market collaboration suites that include wood furniture and other pulp/wood fiber products.

Pursuant to the EUDR, businesses must provide a statement demonstrating compliance with all relevant local laws in each exporting country along with full traceability of the goods throughout their supply chains. The regulation also provides for periodic reviews that would expand the regulation’s scope to cover new products and ecosystems. Information requirements include geolocation data to the exact plot of land where the covered material was produced and documentation demonstrating that there has been no deforestation or degradation of forest in the relevant area since December 2020.

EUDR is unfair because it imposes significant compliance costs and creates conflicting legal requirements due to its extraterritorial application (*i.e.*, imposing compliance obligations on suppliers in third countries) and will have unforeseen consequences on supply chains. The EUDR also makes sourcing raw material more challenging due to current and potential third country suppliers’ inability and lack of capacity to comply with the regulation. While the EU has postponed the entry into force of the EUDR until December 31, 2026, and made some minor changes to the scope, a substantial review of the rules or a carve-out for low-risk countries is critical.

Pharmaceutical Market Access Barriers:

- **France:** France combines price cuts, rebates, revenue taxation, a potential clawback and pharmaceutical-specific taxes to drive net prices on innovative medicines to be among the lowest in Europe. When setting prices, France asserts that 60% of new innovative medicines provide no added benefit over current treatments. Older inferior medicines and generics are often used as price benchmarks, and increasingly excessive rebates are required by the statutory health insurance system. New innovative medicines supposedly awarded “price stability” are still subject to excessive rebates that can push net prices far below the agreed-to price floors. Revenue taxation and pharmaceutical-specific taxes further reduce spending on already devalued medicines with calls for additional reductions.
- **Germany:** Germany rejects clinical trial evidence to assert, when setting prices, that [55%](#) of new innovative medicines provide no added benefit over current treatments. The Federal Joint Committee (G-BA) selects comparators for these required benefit assessments, often using older inferior medicines and generics as price benchmarks (in 74% of assessments). New innovative medicines are often priced 10% lower than older patent protected medicines deemed to offer the same benefit and new medicines deemed to offer a minor added benefit are often not priced higher than older medicines offering less benefit. An additional 20% rebate is imposed on all patent-protected medicines used in combination therapies. Germany has also maintained a [price freeze](#) for all medicines reimbursed by statutory health insurance since 2010. Germany’s 2026 Statutory Health Insurance Contribution Rate Stabilization Act passed in July further increases Germany’s devaluation of innovative medicines by, among other steps, increasing the rebate on innovative medicines from 7 percent to 15.5 percent, imposing an additional 9 percent rebate on innovative vaccines and expanding and extending the 2009 price freeze through 2030. Germany’s pricing policies are currently the subject of a Section 301 investigation, and we urge USTR to negotiate a bilateral agreement that secures meaningful reforms to Germany’s pricing and reimbursement system and ensures that Germany pays its fair share for biopharmaceutical innovation.

- **Italy:** Italy imposes revenue clawbacks, driven by underfunded hospital budgets, that have rapidly become unsustainable for biopharmaceutical manufacturers. In 2024, manufacturers were required to pay back approximately €2B of €17B in hospital medicine revenues ([AIFA](#)). The Italian Medicines Agency (AIFA) deems only a third of new innovative medicines as “fully innovative,” which means many new medicines are not exempted from revenue clawbacks nor placed immediately on regional formularies. Pricing and reimbursement processes at the national level already delay patient access to new medicines, which is exacerbated by further unnecessary delays and uncertainty in listing products on regional formularies.
- **Spain:** Spain sets prices of new innovative medicines by using older inferior medicines and generics in Spain and other countries as price benchmarks. The Spanish government selects the comparators from a broad group of treatments and then chooses from the drugs with the lowest prices as the comparator. When recommending coverage of new medicines, the Inter-Ministerial Commission on Medicine Prices (CIPM) examines a broad group of existing treatments and then selects the medicine with the lowest price as the comparator. Regional authorities often require additional assessments, rebates and price cuts that further undervalue new innovative medicines and further restrict and delay patient access. In addition, Spain requires mandatory discounts of 7.5% for all innovative medicines and a revenue clawback of 2% on all retail pharmacy sales to further reduce spending on already devalued medicines.

Government Procurement

Plans for European Preference in EU Public Procurement and Funding Instruments: The new European Commission has advanced European preference criteria in EU public procurement and funding procedures, which create significant risk for U.S. market access and fair access to tenders, including U.S. businesses with operations or sales in Europe. Under the reform proposals, the Commission has proposed European preference criteria for strategic sectors. Similarly, the recent Defense EDIP/SAFE proposals and the Clean Industrial Deal reference EU content requirements as one of the criteria and a mandate for funding. We expect the upcoming Industrial Decarbonisation Act (IDA) and Cloud and AI Development Act (CADA) to include similar requirements. The strategic sectors under scope are yet to be defined but could include clean energy technologies, along with critical technologies that are deemed important for Europe’s industrial and economic security, such as AI, quantum, and advanced semiconductors.

These proposals have broader implications for U.S. companies operating in Europe and will affect other areas. For example, the EU’s proposed Clean Corporate Vehicles Regulation would only allow EU public sector bodies to provide financial incentives for corporate acquisitions of cars and vans if they are low- or zero-carbon and “Made in EU” from 2028 onwards. Such requirements would limit choice and drive-up costs for U.S. businesses with sizeable vehicle fleets in Europe.

The EU’s proposed European preference risks introducing a discriminatory approach that acts contrary to the EU’s international trade obligations, notably where it would fail to incorporate the principle of non-discrimination and requires that treatment accorded to the goods and services of other GPA Parties shall be no less favorable than the treatment accorded to domestic goods and services. Subject to how they are drafted and enacted, European preference criteria and EU content requirements may risk limiting U.S. businesses’ ability to access parts of the EU government procurement market, impacting a wide range of industrial sectors including defense, clean tech and critical digital technologies. In addition, the EU is also progressively adding localization requirements in new Research and Innovation projects (e.g., under Horizon Europe), notably those related to 6G and secure connectivity projects,

excluding U.S. companies from the initiatives.

Public Procurement Act: In September 2026, the EC published a proposal for a new Public Procurement Act (PPA). The proposal seeks to harmonize public procurement rules across the EU, and includes a ‘European preference’ principle, giving contracting authorities the ability to exclude non-European bidders. While the PPA acknowledges the EU’s commitments under the WTO Government Procurement Agreement (GPA), and grants companies from GPA countries “equal treatment”, there are many exceptions to this rule. For example, the EC can withdraw market access for GPA partners if they fail to maintain reciprocal market access, or if the EC identifies loosely-defined economic security risks (e.g., risks of excessive dependencies). The PPA proposal also ends price as the primary award factor, establishing a ‘Best Price-Quality Ratio’ standard (BPQR). Quality criteria, such as environmental and social standards, security and resilience, must carry a weight of at least 30% (or 50% for labor-intensive contracts). Collectively, the reciprocity, economic security and quality criteria offer contracting authorities several pathways to exclude U.S. bidders from tenders that they would normally be eligible for under the GPA.

Croatia - Public Sector Cloud Procurement Barriers: Croatia’s 2025 State Information Infrastructure Act requires government bodies and public institutions to use the Shared Services Centre (CDU) for hosting government data, subject to certain government-approved exemptions. The Act provides for publication of a CDU service catalog and for the government to specify CDU service providers, but does not set out a process for additional commercial cloud providers to join CDU supply arrangements. In August 2026, the government authorized agreements with several local IT providers – APIS IT, FINA, CARNET, and AKD – as CDU service providers. This framework limits covered bodies’ ability to procure services directly from commercial cloud providers and can constrain qualified U.S. providers’ access to these public sector workloads.

Greece - Energy Efficiency Requirements in Procurement: Under Greece’s Recovery and Resilience Facility (RRF), the Ministry of Finance requires that all data centers used in funded digital projects be listed as participants in the European Code of Conduct on Data Centre Energy Efficiency (EU CoC). While the EU CoC is a voluntary initiative, Greece has made it a mandatory eligibility condition for RRF projects. Because U.S. CSPs’ data centers are not on this registry, they are automatically disqualified from RRF-related tenders, despite meeting equivalent or higher international standards (EN 50600, ISO). This exclusionary procurement practice restricts U.S. participation in Greece’s largest EU-funded digital modernization projects.

Ireland - Public Procurement Barriers: Despite Ireland being home to extensive U.S. cloud infrastructure, its public sector remains a laggard when it comes to cloud adoption. A principal reason for this is the refusal of its authorities to establish a cloud procurement framework that would enable the purchase of services from U.S. CSPs. Under intense pressure from industry, the Irish procurement authority sought to establish such a framework in 2024. That process, however, ended in failure, with the procurement authority insisting on unworkable terms and conditions that no U.S. CSP could meet. A leaked internal Government briefing note cited the extraterritorial application of the U.S. CLOUD Act — which it likened to the Chinese Cybersecurity Law — as a red-line issue. It also suggested that “U.S. political turmoil” gave rise to excessive risk, thereby precluding the use of U.S. cloud services by the Irish public sector.

Malta - Public Sector Cloud Procurement Requirements: Malta’s Cloud Services Policy (GMICT P 0124), effective from September 2024, gives primary preference to cloud services supplied by the government through its designated agent. A system owner selecting another service must justify that

choice in writing, and contracting authorities may mandate use of the government service in tenders.

Netherlands - Cloud Procurement Barriers: The Netherlands' government-wide cloud policy (*Herziening rijksbreed cloudbeleid*), adopted by the Council of Ministers in July 2026, functions as a de facto discriminatory barrier against U.S. cloud providers. While framed as risk management rather than an outright ban, the policy systematically steers the Dutch public sector's highest-value workloads toward EU-headquartered suppliers through a jurisdiction-based test rather than a data-location test. Its core provision advises critical and essential entities — energy, water, banking and payments, telecoms and digital infrastructure, major transport, healthcare and systemic parts of central government — against using, for their primary processes, any supplier that falls “in part” under a non-EU/EEA jurisdiction. This wording is drafted to capture U.S.-parented providers even where all data is stored and processed within the EU, casting doubt over whether U.S. firms can serve these workloads at all — regardless of the substantial local investment, EU data residency and sovereign offerings they provide. The policy is reinforced by a default exclusion of public cloud for government email and document management (overridable only on a demanding three-part test with ministerial sign-off), a cybersecurity screen that can exclude suppliers from countries deemed to run “an active cyber programme against Dutch interests”, and a layer of per-deployment risk assessments, exit-plan obligations and central notification requirements that materially raise the cost and lengthen the sales cycle of every significant U.S. cloud deployment. Taken together, these measures discriminate on the basis of corporate nationality rather than any objective security or performance standard, disadvantage U.S. providers relative to EU-based competitors in procurement, and are consistent with a broader European trend toward using jurisdiction — not data location — as the deciding criterion for market access.

Poland - Local Content Requirements for Public Procurement: The Ministry of State Assets issued non-binding guidelines requiring contracting authorities to score bidders on local content, including Polish workforce share, local subcontractors, and in-country tax contributions. While these provisions do not carry the force of statute, they function as soft law that effectively disadvantages foreign companies in public tenders — particularly those whose supply chains and service delivery models do not rely sufficiently on local suppliers.

Intellectual Property Protection

EU General Pharmaceutical Legislation and Bolar Provisions: In March 2026, the European Union finalized revisions to the GPL that weaken intellectual property protections for innovative medicines by conditioning portions of regulatory data protection (RDP) on product launch, clinical trial, and market access requirements and by significantly expanding the Bolar exemption beyond its traditional non-commercial scope. The revised Bolar provisions would permit activities such as health technology assessments, reimbursement applications, and participation in procurement tenders during the patent term, undermining effective patent enforcement and reducing incentives for pharmaceutical innovation. These exceptions do not appear consistent with the obligations of the EU under the TRIPS Agreement and, moreover, renders more difficult, if not impossible in some cases, timely pursuit of routine patent enforcement. These measures appear inconsistent with international IP norms, create discriminatory localization incentives, and risk setting a precedent that could encourage other countries to adopt similar approaches.

Services Barriers

Digital Markets Act (DMA) Implementation: The DMA, adopted in 2022, is an ex ante competition regulation that designated six U.S. companies and one Chinese firm as “Gatekeepers”. Gatekeepers are

subject to strict restrictions on the use of data, obligations on data portability and access, and requirements on interoperability. Gatekeepers are also prohibited from engaging in a range of business practices often considered pro-competitive, forcing them to de-integrate offerings from different areas of their portfolio that were previously organized into a single, easy-to-use product. As a result, U.S. companies have had to redirect substantial internal resources away from product development and innovation to instead focus on regulatory compliance.

Some of these product changes have significantly degraded the quality of services and generated complaints from European consumers. Compliance costs for each of the five U.S. “gatekeepers” are estimated to average around \$200 million annually, totaling up to \$1 billion annually, and require extensive engineering hours, vastly exceeding the EU's initial per-gatekeeper cost of EUR 1.4 million (\$1.64 million). The European Commission completed its first mandatory review of the DMA on April 28, 2026, concluding the regulation remains fit for purpose and declining to propose meaningful reform, though some policymakers and competition authorities continue to push for expanding its scope to new services (e.g., GenAI, cloud).

The Commission is preparing to extend the DMA to cloud by designating two U.S. cloud service providers as gatekeepers despite them not meeting the quantitative thresholds. Meanwhile, it’s using the DMA to pursue discriminatory fines, prepare new investigations under novel interpretations, and constantly shift compliance requirements – all against America’s most innovative companies. In addition, we continue to see the politicized use of the Gatekeeper label in unrelated legislation as a further way to target the designated companies.

Data Act: The Data Act regulates access to and transfer of data generated by connected products and related services in the EU. The Regulation entered into force in January 2024, and its main provisions started to apply in September 2025. The Regulation mandates sharing of commercial data and the transfer of trade secrets under certain conditions. It also creates new discriminatory barriers that limit data sharing with companies designated as 'Gatekeepers' under the DMA.

For cloud providers, the Data Act imposes price caps for multi-cloud use, whereby the exchange of data between different providers may only be charged at cost. Data transfers when a customer switches to an alternative cloud providers must be free of charge. While cloud providers may recoup data transfer costs that are directly linked with such transfers (incremental costs), the Data Act disregards that the costs incurred by each provider for the fixed assets related to data transfers and interconnection vary significantly. Some U.S. providers invest heavily in developing custom networking hardware and software, scaling out their fiber network globally, and interconnecting in many locations with many providers. Such a strategy requires years of sustained, high-cost investment, whereas other strategies that rely on using intermediary third-party networks for interconnection might involve minimal investment. In sum, the Data Act risks penalizing those who have made significant long-term investments in advanced network infrastructure, with U.S. cloud providers being the most harmed.

Content Moderation / Digital Services Act: The Digital Services Act (DSA) creates new rules alongside existing safe harbors for the handling of illegal third-party content on hosting and intermediary services in the EU, such as video-sharing services, social networks, and online marketplaces. In addition, the DSA creates a new classification of companies called Very Large Online Platforms (VLOPs) - a grouping that disproportionately targets U.S. companies, based on a presumption that services with more than 45 million active users present “systemic risk”, irrespective of any specific risk assessment. The DSA imposes obligations such as: notice & takedown systems for hosting services; ‘know your business customer’; strict transparency and reporting obligations; risk assessments, yearly audits; obligations to disclose the main parameters used in their recommendation systems; data access; and requirements to

appoint a compliance officer. Fines can reach up to 6% of annual turnover.

On April 24, 2023, the European Commission designated the first very large online platforms and search engines. Indeed, out of the 20 services designated, the majority ended up being U.S. firms. The DSA was weaponized to incorporate regulations on a variety of other topics not initially germane to the stated goal of online safety. For example, the inclusion of restrictions on personalized targeted advertising undermines the horizontal normative purpose of the DSA proposal and harms European companies along with U.S. firms. Throughout implementation, the European Commission continues to use the DSA to further regulate online services beyond the scope of the legislation. We see ongoing politicized use of the VLOP designation in unrelated legislation as a further way to target the designated companies.

Network and Information Security 2 (NIS2) Directive Transposition/Implementation: While the NIS2 Directive aims to create a harmonized cybersecurity framework across the EU, the transposition process grants Member States significant leeway in interpreting and implementing its provisions.

This flexibility has led to a fragmented landscape of national requirements, as highlighted by the early transposition efforts of Croatia, Hungary, and Belgium, and the various draft proposals. Areas exhibiting variations in national interpretations include, among other things, scope, reporting, audits, and certifications. The Hungarian transposition,⁷ for instance, adds some (sub)sectors to the original NIS2 sectors while the draft Czech Republic transposition demonstrates divergence in its definition of “important” and “essential” entities, potentially leading to discrepancies in which organizations fall under the scope of the regulation.⁸ Diverging reporting obligations can be seen in the Croatian draft transposition and the audit and certification requirements vary across the countries having already transposed NIS2.⁹

These discrepancies pose significant challenges for organizations operating across multiple EU Member States. They face navigating a complex web of diverging requirements, potentially increasing compliance costs, and creating an uneven cybersecurity landscape within the EU. Such divergence creates significant hurdles for pan-European providers, who now face:

- **Disproportionate Burden:** Navigating a complex web of national requirements strains resources and stifles innovation. The need to comply with multiple, potentially overlapping regulations divert time and resources away from core business operations and cybersecurity enhancements.
- **Reduced Competitiveness:** Increased compliance costs and complexity, without a corresponding improvement in security decision-making, put pan-European providers at a competitive disadvantage compared to entities operating solely within less regulated Member States.
- **Barrier to the Single Market:** Divergent requirements create unnecessary obstacles for companies operating across borders, hindering the free flow of services and potentially fragmenting the Digital Single Market. This runs counter to the principles of a unified digital space within the EU.
- **Reduced Effectiveness of NIS2:** The administrative burden associated with compliance can overshadow the directive’s core objective which is enhancing cybersecurity. Instead of focusing on proactive measures and long-term strategies to counter emerging threats, organizations

⁷ <https://njt.hu/jogszabaly/en/2023-23-00-00>

⁸ <https://www.psp.cz/sqw/text/orig2.sqw?idd=244061>

⁹ https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html

become bogged down in navigating and adhering to a complex regulatory maze.

The issues above have also caused complexity and regulatory burdens for U.S. air carriers, both passenger and cargo. NIS2 does not clearly specify which European jurisdiction(s) non-EU air carriers must consider for NIS2 compliance. The proposed “Cybersecurity Package” from January 2026 includes targeted amendments to NIS2, including the clarification that non-EU carriers fall under the jurisdiction of the Member State of their “main establishment” in the EU. If adopted, it would simplify future engagements to a single EU Member State and allow for the U.S. Government to determine the feasibility of a bilateral recognition agreement.

To fully realize the potential of NIS2 and achieve a truly robust cybersecurity landscape within the EU, addressing this fragmentation is crucial. Member States must strive for greater harmonization of national requirements, ensuring consistency and interoperability across borders and encouraging the adoption of existing, widely recognized, international standards in order to streamline compliance and reduce unnecessary duplication of efforts. The European Union Agency for Cybersecurity (ENISA) has already highlighted the benefits of such an approach in its guidance on the European Electronic Communications Code (EECC), advocating for the use of established international standards to reduce compliance burdens on providers operating across multiple EU countries.

Cybersecurity Act: In January 2026, the EC published a proposal for a revised Cybersecurity Act (CSA2). The proposal would allow the EC to designate specific countries as ‘high-risk’ but lacks clear criteria and timelines for the designation process, giving the EC broad powers and discretion. In addition, the proposal would also allow the EC to designate ‘high-risk’ vendors and lists ‘supplier dependency’ as grounds for designating suppliers of key ICT assets as ‘high-risk’. A ‘high-risk’ designation would prohibit a supplier from obtaining European cybersecurity certificates, participating in public procurement and contributing to technical standardization. A vendor with state-of-the-art encryption, flawless audit records and zero technical vulnerabilities could therefore be banned from certification and public tenders simply because its products are widely adopted and deemed a ‘dependency’. Further, provisions to strengthen the role of ENISA, the EU cybersecurity agency, could lead to it becoming a parallel standardization body, scaling back reliance on international and European standards. The CSA2 proposal also seeks to replace the standing Stakeholder Cybersecurity Certification Group (SCCG) with an annual ‘European Cybersecurity Certification Assembly’. Moving from a standing expert group to an annual assembly significantly dilutes industry’s ability to provide detailed, structural technical input during the design and maintenance of cybersecurity schemes.

EU Cybersecurity Certification Scheme for Cloud Services (EUCS): The European Commission has developed several policies seeking to restrict market access for U.S. cloud service providers (CSPs), particularly through the use of ‘sovereignty requirements’ (i.e., restrictions on foreign-owned and/or foreign-headquartered companies). The EU Cybersecurity Certification Scheme for Cloud Services (EUCS) was proposed in 2020 to harmonize the cybersecurity certification process for cloud services in the EU, but became contentious due to the introduction of sovereignty requirements, which would have prevented U.S. CSPs from serving customers in the public sector and certain regulated industries. These requirements were removed from the draft in March 2024, but adoption was suspended because of continued disagreement between EU countries. The European Council, European Parliament, and European Commission continue to focus on the revision of the EU Cybersecurity Act (CSA2); this legislation provides the legal basis for the EUCS and other certification schemes. USTR should take note of successful sovereignty-advancing changes made to the CSA and how this shapes the precedent for future pushes.

Cloud and AI Development Act (CADA): Since 2020, the EC has developed several policies seeking to restrict market access for U.S. cloud providers. The EU Cybersecurity Certification Scheme for Cloud Services (EUCS), proposed by the EC in 2021, sought to introduce ‘sovereignty requirements’ that would have significantly limited the ability of U.S. cloud providers to operate in the EU. These requirements were eventually abandoned in 2024 due to strong pushback from industry, EU Member States, and trade partners.

In June 2026, following the failure to adopt EUCS, the EC published a proposal for a new Cloud and AI Development Act (CADA). The proposal seeks to restrict U.S. cloud and AI providers from serving the EU public sector by introducing a mandatory sovereignty framework with four tiers – Union Assurance Levels (UAL) 1 through 4 – that evaluates providers on the basis of ownership and nationality, rather than technical and operational controls. Under the current proposal, U.S. providers would be excluded from the highest sovereignty tiers (UALs 3-4) by default, face extensive structural obligations to meet the minimum level required for sensitive public sector use (UAL-2) – including obligations to demonstrate immunity from U.S. law – and be subject to onerous data localization requirements across all public sector use-cases. In addition, the EC would be able to extend these requirements to organizations outside the public sector (e.g., energy, healthcare, financial services) through secondary legislation, with no meaningful legislative scrutiny.

The treatment of U.S. providers under CADA contrasts with other initiatives being developed by the EC. For example, under the proposed Industrial Accelerator Act and Public Procurement Act, foreign suppliers are automatically deemed equivalent to domestic suppliers if they are headquartered in a country that is a signatory of the WTO Government Procurement Agreement (GPA) – including the U.S. – and the EC can only revoke this equivalence in specific circumstances. Under CADA, on the other hand, foreign providers are excluded from the highest sovereignty tiers by default. In other words, whereas the Industrial Accelerator Act and the Public Procurement Act aim to respect the EU’s trade commitments by presuming eligibility for partners with whom the EU has binding trade agreements, CADA treats all foreign providers as ineligible by default.

While the EC pursues initiatives to exclude U.S. cloud providers from a substantial share of the EU market, European IT providers continue to enjoy unfettered access to the U.S. market. The U.S.’s federal certification scheme for government IT procurement, FedRAMP, does not discriminate against EU companies, and leading European IT providers are able to supply the U.S. Government. In addition, several EU companies have obtained a Facility Security Clearance (FCL) in the U.S., enabling them to handle classified information.

Finally, while CADA is applicable to public procurement of cloud and AI services, it contains a clause that empowers the European Commission to extend certain requirements (risk assessments) to private sector entities “operating in sectors of high criticality”, such as energy, transport and financial services. This would be a wholly unwarranted interference in private companies’ ability to choose their suppliers, which should be based on commercial considerations.

Digital Networks Act (DNA): In January 2026, the European Commission proposed a new Digital Networks Act that includes problematic new provisions for U.S. technology and content providers. Amongst the risks, the framework may scope cloud infrastructure — including private networks connecting data centers, and subsea cables — into the EU’s telecom regulatory framework, subjecting U.S. cloud providers to onerous obligations that duplicate existing cybersecurity requirements under NIS2. Separately, the DNA’s ‘voluntary’ conciliation mechanism for IP interconnection disputes, and the inclusion of Content Delivery Networks (CDNs) within its scope, risks introducing backdoor network

fees, giving telecom operators unilateral power to trigger regulatory proceedings and extract payments across the digital value chain. These risks have escalated sharply during the legislative process. Despite the EU's commitment in the EU-U.S. trade deal not to introduce or maintain network fees, the Commission did not entirely abandon the concept of network fees in its DNA proposal. Instead, due to continued lobbying from European telcos, they have introduced two new provisions that could ultimately enable European telcos to secure additional payments from U.S. providers.

The first problematic provision is the creation of a new “Facility for Voluntary Conciliation”. This provision would allow parties involved in an IP interconnection dispute – e.g. a large European telco, on the one hand, and an American content and application provider (CAP) or content delivery network (CDN), on the other – to trigger a new “conciliation” process under the oversight of European regulators. These regulators must then issue formal opinions and recommendations on the case. While such outputs would be non-binding, the DNA states that this process is intended to allow European telcos to address the “disproportionate or unsustainable investment needs” generated by the traffic of U.S. technology and content providers. As such, the proposed “voluntary” conciliation mechanism could result in a proliferation of disputes against U.S. CAPs and CDN providers across EU Member States in pursuit of desirable regulatory precedents and could ultimately lead to *de facto* network fees. This momentum is extending to the national level. Spain and France are receptive, and Italy's regulator (AGCOM) has already moved to bring CDNs under its general authorization regime. Several Member States are also leveraging security and resilience arguments to expand regulatory oversight of U.S. infrastructure and to position European operators as sovereign alternatives to U.S. cloud providers. Moreover, lawmakers in the European Parliament are considering amending the proposal to make this a mandatory dispute resolution mechanism that would allow European telcos to pursue payments more directly.

The second problematic provision is the expansion of the scope of the “*General Authorisation regime*”, an existing legal regime under the European Electronic Communications Code (EECC) that allows EU Member States to require public telcos to register before they can offer services in their jurisdiction. The DNA would expand the scope of this regime to a huge number of private networks used to provide “information society services available to the public”. This would capture U.S. CAPs and CDN providers (along with other private infrastructure used to deliver internet content that the general public can access). In addition to creating unwarranted regulatory and administrative burdens for U.S. CAPs and CDN providers, this change could also create a route to backdoor network fees by potentially bringing them into the scope of the dispute resolution mechanism for interconnection. If this was the case, European telcos would be able to use the mechanism to pursue payments from U.S. technology and content providers (thereby establishing *de facto* network fees).

Separately, the DNA proposes wholesale reforms to satellite licensing and spectrum management in the EU, shifting key competences from national to EU-level authorization and registration processes. By layering these EU-level requirements onto existing national frameworks — and operating in tandem with the EU Space Act and the proposed 2 GHz MSS Regulation, the latter of which introduces an EU-level authorization regime explicitly grounded in “sovereignty” considerations — these measures create procedural asymmetries that fall disproportionately on large non-EU (predominantly U.S.) satellite constellations seeking market access.

EU AI Act: The EU AI Act establishes a horizontal risk-based framework to regulate AI systems in the EU. The regulation entered into force in August 2024, triggering the gradual phase-in of its provisions over a 36-month period. It is now being supplemented with implementing rules and standards to operationalize its requirements for general-purpose AI, low-risk AI and high-risk AI. Despite some alignment with OECD work, the lack of clarity in key definitions in the AI Act undermines the effectiveness of this law and could hinder AI adoption in Europe by both EU and U.S. companies.

Problematic definitions include AI systems, general-purpose AI models, and the classification of high-risk and prohibited AI. The broad definition of "high-risk" applications, along with burdensome compliance requirements and steep fines, imposes new compliance burdens on U.S. companies operating in the EU, and could dampen innovations and create legal uncertainty and new obstacles for products and services that are already subject to a multitude of regulatory mandates. Compliance requirements for "high risk AI" are administratively cumbersome and may not be technically possible for firms to adhere to with certainty, given obligations such as requiring human oversight. The problem is compounded by the ambiguous allocation of responsibilities within the AI value chain. Furthermore, the vague wording of certain prohibited systems creates legal uncertainty and risks banning low-risk applications.

CEN and CENELEC, the European standardization bodies, have launched a dedicated technical committee (JTC 21) to develop harmonized standards that will support the implementation of the AI Act, including a framework for AI trustworthiness and standards for AI risk management and quality assurance. However, current estimates indicate harmonized standards will not be ready until mid-2026, which creates timing challenges given the regulatory requirements for high-risk AI will begin applying in August 2026. Industry is therefore requesting a delay in the application of these requirements, which the European Commission seems open to including in targeted legislative amendments, expected in the upcoming Digital Omnibus. It remains unclear whether the standards developed in JTC 21 will be fully consistent with existing ISO standards (e.g., ISO 42001). Divergent standards would require businesses to adapt, at least in parts, to EU-specific requirements.

In addition, the AI Act also requires providers of general-purpose AI models to disclose a "sufficiently detailed" summary of their model training data. The Commission has developed a template for these disclosures, which was finalized in July 2025. Industry stakeholders have raised concerns about the technical feasibility and commercial sensitivity of granular training data disclosure requirements, particularly regarding the protection of trade secrets. It remains to be seen whether the Commission will allow companies not to disclose trade secrets in the template. It also remains unclear whether, and how, the Commission will enforce the AI Act's suggestion of applying EU copyright law to any general-purpose AI model, regardless of where its training was conducted. This would conflict with copyright territoriality principles. Finally, any adjustments to the copyright *acquis* should avoid duplication, contradiction, or requirements that are unworkable for companies operating across the EU and global markets.

EU Data Act Article 32 on International Governmental Access and Transfer: The EU Data Act establishes rules and "safeguards" for foreign governmental bodies' access requests to non-personal data stored in the EU. Specifically, Article 32 of the EU Data Act (2023/2854) provides that data processing services "shall take all adequate technical, organizational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State".

Article 32 of the Data Act makes U.S. companies responsible for potential conflicts in law relating to governmental access to data. At a minimum, this *de facto* item requires companies to conduct and publish evaluations of U.S. and other non-EU laws equivalent to the Transfer Impact Assessments (TIA) under the General Data Protection Regulation (GDPR) for non-personal data, which is disproportionate to the risk presented. GDPR TIAs are already very complex for U.S. companies providing data processing services for *personal* data. In a maximalist scenario, it could force U.S. companies to localize non personal data infrastructure and operations to provide the requisite guarantees. This measure is specifically targeted at and discriminates against U.S. companies due to EU concerns around U.S. governmental authorities' requests for information.

Digital Fairness Act: The European Commission is assessing potential gaps in EU consumer protection rules as part of its future Digital Fairness Act (DFA). A broad, horizontal approach could impose similar requirements across very different digital services and business models, without sufficiently accounting for differences in underlying consumer risks. For online marketplaces, new requirements could also overlap with existing obligations under the Digital Services Act (DSA), GPSR, and EU consumer law, adding regulatory complexity and uncertainty for U.S. businesses. Overly broad restrictions on personalization, advertising, or interface design could impede product discovery and make it more difficult for SMEs and individual sellers to reach interested buyers.

AVMS-D: The EU's Audiovisual Media Services Directive (AVMSD), last refined in 2018, sets rules for content quotas, advertising, and the promotion of European works on both traditional broadcasters and digital platforms. In May 2025, the EU Council signaled a revision to adapt the directive to video-sharing platforms and social media, with emphasis on content prominence, protection of minors, and European content visibility. For U.S. businesses, the AVMSD creates operational and compliance burdens, restricts flexibility in content offerings, and may limit market access for streaming and digital media services (See the member state sections below for more details).).

Financial Information for Data Access Regulation: The European Parliament and the Council of the EU are seeking to exclude companies designated as 'Gatekeepers' under the DMA from the draft FIDA Regulation, making them ineligible for the financial data sharing scheme. The policy options prominent in the FIDA discussions are: (1) full exclusion (based on Germany's non-paper), where the definition of 'data user' would be modified to explicitly exclude 'Gatekeepers' from the full regime; and (2) partial exclusion (based on the Commission's non-paper), preventing 'Gatekeepers' from processing, combining and cross-using customer data under FIDA, and requiring 'Gatekeepers' to obtain authorization to operate as a FISP (Financial Information Service Provider).

EU Digital Simplification Omnibus: The European Commission's Digital Omnibus package, introduced in November 2025, proposes to require that data subjects be able to give or withdraw consent and object to data processing through automated, machine-readable signals set at the browser or operating system level, with all controllers required to honor those signals. While the intention to reduce cookie banner fatigue is understandable, the mechanism chosen risks creating a structural competitive distortion by concentrating effective control over the consent layer in the hands of a small number of browser and operating system providers, some of whom operate significant advertising businesses of their own. Rather than simplifying the consent landscape for users, this approach transfers decision-making power from the user-controlled relationship to a technical intermediary with its own commercial interests, which is opposed to the GDPR's foundational requirement that consent be freely given to an identified controller for identified purposes. The Digital Omnibus also seeks to specify how often services can ask users for consent after they have rejected it. This significantly reduces the freedom of companies to communicate with their own users and, ultimately, to innovate. The Digital Omnibus also proposes to introduce a specific provision on AI training under the GDPR explicitly recognizing legitimate interest as a legal basis for processing personal data in AI model development while adding an unconditional right to object that goes beyond the existing GDPR framework. This is unnecessary and counterproductive as the GDPR already provides a comprehensive and technology-neutral legal basis framework that is fully capable of governing AI training. Creating a parallel, AI-specific regime risks adding compliance complexity without meaningfully strengthening data subject protections.

EU Space Law: The EU Space Act (EUSA) proposal would introduce stringent requirements for satellite constellations, in some cases discriminating against non-EU operators. Critical provisions include:

1. Constellation size classification: The EUSA establishes three categories of operators, which are subject to different requirements. The category subject to stricter requirements, ‘giga-constellations’ (≥ 1000 satellites), targets two U.S. constellations.
2. Technical requirements: The proposal creates uncertainty by deferring crucial technical specifications to future Implementing Acts (IAs). However, the draft already shows that the Commission is intending to introduce novel standards lacking scientific basis and deviating from international norms, including on orbital congestion, orbit selection and intra-constellation risk.
3. Collision avoidance services: EU operators must use EU Space Surveillance and Tracking (EU SST), while non-EU operators are excluded and must rely on alternative services that meet certain requirements. Several of those requirements are not met by the U.S. Space-Track system and are not aligned with best practices, creating operational challenges for non-EU operators.
4. Registration process discrimination: Non-EU operators face undefined registration timelines, while EU operators benefit from a 12-month process. The governance framework, involving a Compliance Board at the EU Agency for the Space Program (made up of delegates from Member States), raises concerns about potential delays and conflicts of interest (e.g., the French Government has recently invested €1bn+ in Eutelsat OneWeb, a competitor to U.S. constellations).
5. Implementation timeline: The EUSA will apply to spacecraft launched after January 2030, with a 2-year exemption for satellites completing critical design review in the prior year. With final adoption of the full legislative package expected in 2028/2029, this creates tight compliance windows for next-generation constellations.

Inspection rights: The European Commission seeks authority to inspect non-EU facilities, raising concerns about business secret disclosure and potential conflicts with U.S. regulations, particularly ITAR requirements.

News Media-Related Digital Service Taxes: The European Media Freedom Act (EMFA) was enacted on April 17, 2024, with a dual goal of supporting media freedom and diversity and protecting journalists. In particular, the EMFA introduces a special treatment of media content on very large online platforms. While the adopted text claims that this special treatment would not contradict the horizontal rules established in the Digital Services Act, the implementation will be challenging as the EMFA create additional complexity in interaction with other digital regulations.

More concerningly, the creation of a press publisher’s right under Article 15 of the Copyright Directive creates problems with respect to online services providers needing to pay news organizations for hosting news content, including links. In contrast to U.S. law and current commercial practices, Article 15 may effectively require search engines, news aggregators, applications, and platforms to enter into commercial licenses before including snippets of content in search results, news listings, and other formats. As EU states continue to implement the rules in the Copyright Directive into their national laws, some governments are re-interpreting key provisions to the detriment of users, publishers and platforms alike, and creating new barriers and challenges for U.S. companies when complying with national rules:

- One example of this trend can be found in Croatia. While the European Commission, and former

Commissioner Breton specified that “*Member States are not allowed to implement Article 15 . . . through a mechanism of mandatory collective management*”, the Croatian draft law includes a provision which would make it mandatory for all publishers to license these rights collectively..

- In 2019, while in the process of implementing Article 15, France created an analogous right for press publishers. News publishers can now request money from platforms when platforms display their content online. In response, Google changed the way news articles appeared in search results, but this did not prevent the French competition authority from ordering Google in April 2020 to pay French publishers based on the new law; and while, in October 2020, Google and the “Alliance de la Presse d’Information Générale” (representing newspapers such as Le Monde) announced that future licensing agreements would be based on criteria such as the publisher’s audience, non-discrimination and the publisher’s contribution to political and general information, the French competition authority imposed a €500 million fine on Google in July 2021 as it considered that the company did not negotiate “in good faith” with the press industry over licensing fees.

Austria - Digital Services Tax: Austria imposes a 5% DST on revenue from online advertising. The threshold is for companies with worldwide revenue of €750 million and local revenue of €25 million. Further, there are ongoing political discussions about introducing additional obligations in the form of an extra levy or an investment obligation on VoD services under the AVMS Directive.

Belgium - Digital Services Tax: In 2025, the new ruling government of Belgium put forward a plan to implement a 3% “digitax” by 2027 at the latest, pending further European and global discussions. If it follows Belgium's 2019 proposal, it would apply to companies with worldwide revenue of €750 million and local revenue of €5 million and would have the same scope as the European Commission's DST proposal, which would allow the revenue streams of advertising services, intermediation and marketplace services, and data transmission to be taxable. Parliament debated a legislative proposal in June 2026 and continues to consider digital taxes, signaling continued political support for unilateral digital taxation of U.S. companies.

Croatia - Digital Services Tax: In 2019, the government of Croatia announced plans to adopt a digital services tax, potentially modeled after the DST in Austria. NFTC urges USTR to encourage Croatia to refrain from enacting a DST and instead re-commit to the multilateral project through the OECD/G20 Inclusive Framework to address tax challenges of the digitalizing global economy. While there is no immediate movement on this proposal, it may well return at a later stage and should therefore remain on the radar.

Czechia - Digital Services Tax: In 2019, the Czech government proposed a 7% DST on revenue generated by (a) supplying targeted advertising on a digital interface to Czech users; (b) making available to Czech users a multisided digital interface that facilitates the provision of goods and services among users; and (c) transmitting data about Czech users derived from their activities on digital interfaces. In-scope companies would have global revenue exceeding EUR 750 million, revenue from supplying covered services in Czechia exceeding CZK 100 million, and revenue from supplying covered services in the EU amounting to at least 10% of total revenue in the EU. Discussions on the proposal were not concluded in the Chamber of Deputies, with the bill stalling before the third reading in 2021. The topic of the DST has not been discussed in Czechia since 2021, and the tax has not been adopted to date. Although there is no immediate sign of progress on this proposal, it should nevertheless remain on the radar.

Cyprus - Data Residency and Cloud Procurement Requirements: Cyprus’s Cloud Policy, approved in

March 2026, establishes the hybrid Government Cloud (G-Cloud) as the default platform for covered government services, with alternative deployments requiring a justified exemption from the Cloud Technical Design Committee. Covered entities must use providers evaluated and approved by the Deputy Ministry of Research, Innovation and Digital Policy. Although the Policy sets out provider criteria and envisages a published list of approved vendors, it does not specify how prospective providers seek approval or a timeline for decisions. The Policy imposes EU residency requirements and Cyprus-specific hosting requirements for sensitive and critical data, while also permitting hosting in other EU or EFTA countries with equivalent data protection regimes, and allowing for approval-based exceptions. These provisions create uncertainty about permissible hosting arrangements. Collectively, the residency, approval and compliance requirements can restrict cross-border service delivery and market access for U.S. cloud providers.

Estonia - Streaming Investment Obligation/Levy Proposal: In June 2026, the Estonian government released a draft law requiring streaming services in Estonia to pay 5% of their Estonian revenues as a levy or an investment in Estonian content. If the draft law is enacted, the burden of the law is intended to, and will, fall on U.S. streaming services. The draft law covers VOD only and does not cover linear TV. While a majority of the covered companies are U.S. streaming services, many linear TV providers in Estonia are Estonian or other European. Further, the covered local companies invest in Estonian content as part of their core business and so will not be burdened by the requirements. In practice, the measure will function as a 5% revenue-based tax paid by U.S. companies - essentially a sector-specific DST.

Finland - Streaming Investment Obligation/Levy Proposal: On September 30, the government introduced into the parliament a bill requiring providers of on-demand television services to pay 5% of their Finnish revenues as an investment in new Finnish content or as a levy to the Finnish government. Qualifying investments must be new content that is in Finnish, Swedish, or Sami and is closely related to Finland's history, culture, or society, and the producer or co-producer must be an EU company. If the law is enacted, the burden will fall disproportionately on U.S. companies. U.S. companies represent two thirds of the companies the government expects to be covered. Further, there will be little impact on the local companies that will be covered because their business models are based on Finnish content. Additionally, linear TV companies in Finland are not subject to a levy or IO. Compared to streaming, the companies providing linear TV services in Finland are significantly more Finnish and European. In practice, Finland's proposed streaming investment obligation/levy measure will function as a 5% revenue-based tax on U.S. companies, similar to a DST.

France - SecNumCloud Certification Requirement: In March 2022, France's national cybersecurity agency (ANSSI) revised its cybersecurity certification and labeling program SecNumCloud (version 3.2) to disadvantage and effectively preclude foreign cloud providers from providing services to government agencies and 600+ organizations operating "vital" and "essential" services. Specifically, SecNumCloud and France's 'Trusted Cloud Doctrine' require certified providers to be "immune to non-EU laws" ("Immunité au droit extra-communautaire") and explicitly disqualify from certification any provider that is more than 24% foreign owned (i.e., non-European). As a result, U.S. providers must partner with and transfer technology and control to a local provider to provide cloud services to covered entities. This provision appears to be a clear violation of Article 3 of the WTO Government Procurement Agreement. Article 31 of France's 2024 SREN Law established an obligation to use SecNumCloud-certified providers for the state's sensitive data, and Decree 2026-272 of April 2026 defined additional covered entities. Covered entities include central government administrations, and designated public-interest groups. The French legislature continues to expand these requirements to additional sectors through various amendments, often without explicitly referencing SecNumCloud, but incorporating its ownership restrictions. This growing trend of amendments across different sectors suggests a pattern of discriminatory regulation under the guise of security requirements, with the ownership criteria being the

primary focus rather than actual security measures.

France - Digital Services Tax: France maintains a 3% DST on revenue from services connecting users through a digital platform and the sale of advertising space and digital data. The threshold is for companies with worldwide revenue of €750 million and local revenue of €25 million. France introduced the DST in 2019 as a transitional measure pending an OECD solution but has maintained it in force since. As of October 2026, the tax remains in effect, with no end date set. Furthermore, recent French budget proposals have contemplated increasing the rate.

Germany - Competition / Ex Ante Rules: Section 19a of Germany's Act against Restraints of Competition (ARC), known as the UPSCAM provision, equips the Federal Cartel Office (FCO) with enhanced powers to regulate companies designated as having "paramount significance for competition across markets." Unlike the EU's Digital Markets Act (DMA), which targets specific core platform services, Sec. 19a applies on a group-wide, cross-market basis. To date, only five U.S.-based companies have been designated — Alphabet, Meta, Amazon, Apple, and Microsoft — while no European or non-U.S. company has been designated.

The provision allows the FCO to prohibit conduct that merely has the potential to restrict competition, without requiring proof of actual competitive harm, and reverses the burden of proof onto designated companies. The FCO has used Sec. 19a to open investigations and has adopted its first prohibition decisions against designated companies.

Both the DMA and Sec. 19a address overlapping concerns but operates under different enforcement regimes, creating a risk of parallel investigations into the same conduct with potentially conflicting outcomes. AI and cloud are emerging as a potential focus area for future UPSCAM enforcement.

Germany - Digital Levy Proposal: German Cultural Minister (an independent, CDU/CSU appointee) has proposed the introduction of a 'platform/digital levy' of up to 10% on large digital platforms that use media or cultural content. While no official draft legislation exists yet, the minister repeatedly indicated the publication of a proposal soon, most recently for autumn 2026, and has repeatedly singled out U.S. companies such as Google and Meta and citing Austria's digital services tax as a model. Political pressure is also building. The Social Democratic Party (SPD), the coalition partner that holds the Finance Ministry, has called for a broader digital services tax on "Big Tech" and has linked it to retaliation against U.S. tariffs.

Germany - Streaming Investment Obligation Proposal: Germany's federal cabinet approved a draft law, the Mediendienste-Investitionsverpflichtungs-Gesetz (MedienInvestVG), on May 27, 2026, targeting U.S. and other foreign streaming providers with an obligation to invest at least 8% of their German net turnover in European productions. Sub-quotas would mandate that 60% go toward 'New European Works,' 70% to independent producers, and 80% meet a 'German cultural character' requirement (defined as 80% German-language content). Additionally, the proposal has IP ownership and exploitation restrictions for works counting towards the independent producer sub quota. These restrictions apply even when the producer does not bring its own financial means to the production and instead relies on federal or EU production incentives — meaning U.S. streamers that finance a production can still be forced to relinquish rights. These layered sub-quotas and rights reversion provisions significantly constrain how U.S. streaming services can allocate their mandated investment spending. The government submitted the bill to the Bundestag on September 2, 2026, with a first reading scheduled for September 24 and entry into force as early as January 1, 2027. Services generating less than €10 million in annual German turnover would be exempt. Industry has pushed for voluntary investment arrangements in place of the

mandate, but the bill is now formally before parliament, and legislative risk is high.

Hungary - Data Localization: In Hungary, data management rules for state and local government bodies providing essential services are governed by Act No. 50 of 2013 on the Electronic Information Security of State and Local Government Bodies (Act). The data managed by state and local government bodies under this Act may only be processed and stored on Hungarian territory, except where the supervisory authority authorizes the processing on the territory of another EEA country. Any entity not registered in Hungary handling data covered by the Act must appoint a representative in Hungary.

Italy - Digital Services Tax: Italy maintains a 3% DST on revenue from advertising services, intermediation and marketplace services, and data transmission (i.e., the transfer of data collected from users and generated through the use of digital interfaces). The tax applies to companies with worldwide revenue of €750 million.

Italy - Discriminatory Tax Investigations: Milan's public prosecutor has pursued a years-long campaign of aggressive and legally dubious tax investigations targeting U.S. technology and logistics companies, resulting in over \$4 billion in discriminatory taxes, fines, settlements, and claims against American companies over the last decade. Examples include:

- Tax authority not entering in good faith negotiations concerning common tax issues, such as transfer pricing or withholding tax issues, and instead applying a heavy-handed approach including criminal penalties.
- Italian Competent Authority denying access to or refusing to participate in mutual agreement procedures (MAP) under applicable income tax treaties.
- Tax authority taking technical positions that are contrary to their own tax laws or long-established international tax principles, as embodied in OECD tax treaty commentary (e.g., *Principio di Diritto No. 5* of February 20, 2023, which imposes royalty withholding taxes on mere distribution of software in contravention of OECD Commentary).
- Italy's application of VAT to standard "free" digital services for consumer data diverges from established international tax principles and recent EU Commission guidance, creating significant compliance uncertainty for U.S. platforms.

In the context of the ongoing trade negotiations with the EU, USTR is encouraged to request its counterparts to remove this barrier to trade by requiring the Italian government to reform its tax administrative practices and tax policies to be consistent with internationally accepted norms. Similarly, reform of the tax court system is necessary to ensure that courts respect international law obligations of Italy and deliver a level of adjudication that is appropriate for high-stake controversies resulting from exaggerated assessments imposed by the Italian tax authority. An additional step would be if USTR (in coordination with US Treasury) could convince Italy to accept binding arbitration in its tax treaty with the US, which arbitration could be initiated at the request of the taxpayer in the event that MAP does not lead to an agreed resolution.

Italy - Network Fees: Despite the EU's commitment in the EU-U.S. Joint Statement, the Italian telecom regulator (AGCOM) is currently setting a precedent for the introduction of backdoor network usage fees. On August 5, AGCOM ruled that CDNs fall within the scope of the European Electronic

Communications Code (EECC), and are therefore subject to dispute resolution mechanisms. This will allow Italian telecom operators to initiate disputes with U.S. tech companies as a means of extracting payments for the delivery of traffic requested by users. By multiplying disputes, and building on the precedent set by these disputes, Italian telecom operators intend to establish *de facto* network usage fees. If left unchallenged, this could create a precedent for other countries and the European Commission to follow.

Italy - Data Localization in Education: The Ministry of Culture's current interpretation of the Italian Cultural Heritage Code (D.Lgs. 42/2004) creates barriers to the provision of cloud services to educational institutions. Specifically, the broad classification of public archives (including school records and educational documentation) as “cultural heritage” under Italian law effectively restricts the storage and transfer of digitalized public documents outside Italian territory. The lack of clear harmonization between cultural heritage protection requirements and modern cloud computing needs creates an obstacle to digital trade, particularly impacting non-EU cloud providers seeking to serve Italian schools and educational institutions.

Latvia - Streaming Investment Obligation/Levy Proposal: In July 2026, the government approved bills amending the Film Law and the Electronic Media law that will require streaming services to pay 3.5% of their gross Latvian revenues as an investment in Latvian content or a levy to the National Film Center. If the bills are enacted, the burden will fall disproportionately on U.S. streaming services. The bills’ obligations apply only to VOD services. As in other countries, a majority of streaming services in Latvia are U.S. companies, while linear TV providers are predominantly Latvian or other European. In practice, covered U.S. streaming services will experience the bills as a tax on gross revenues, similar to a DST.

Malta - Data Mirroring and Hosting Requirements: The Malta Gaming Authority (MGA) requires licensees whose primary servers are hosted outside Malta to maintain a live or real-time mirror of essential regulatory data on servers in Malta, accessible to the MGA for supervision. Although the framework permits overseas hosting of core systems, the local replication requirement entails additional infrastructure, data duplication and ongoing operational and compliance obligations. These requirements can increase the cost and complexity of using cross-border cloud services, including those supplied by U.S. providers.

Poland - Digital Services Tax: On July 31, 2026, the Polish Ministry of Digital Affairs published a draft bill proposing a DST. The proposal sets the tax rate at 3% of taxable revenue attributable to Poland. The proposed tax would apply when both of the following thresholds were exceeded during the preceding financial year: (i) the worldwide revenue of the entity or its consolidated group exceeded EUR 1 billion, and (ii) revenue generated in Poland exceeded PLN 25 million. Entry into force is currently intended for 1 January 2027.

Slovakia - Streaming Investment Obligation/Levy Proposal: In March 2026, the government introduced into parliament a bill requiring streaming services to pay 3.5% of the gross revenue they earn in Slovakia either as a levy or in funding Slovak content. Parliament passed the bill in October 2026. Under the bill, at least 0.5% of domestic revenues will have to be paid as a levy to the Slovak Audiovisual Fund. A company could satisfy the remainder of the obligation by paying the full amount as a levy or by investing in Slovak content and paying the outstanding balance as a levy. The burden of the bill will fall predominantly and disproportionately on U.S. companies. Most of the top streaming services in Slovakia are U.S. companies. By contrast, many top private TV companies in the market are Slovak or other EU companies. Slovakia requires linear TV companies to contribute to the Audiovisual Fund but at

significantly lower rates than 3.5%. Additionally, the few local companies that may be covered invest in local content as their business model and so will be far less burdened than covered U.S. companies.

Spain - Digital Services Tax: Spain maintains a 3% digital services tax imposed on online advertising, online intermediation and data transmission services carried out in Spain. The threshold is for companies with worldwide revenue of €750 million and local revenue of €3 million.

Services Barriers - Telecommunications

Upper 6 GHz Spectrum Allocation: More than five years after the US first made the full 6 GHz band available for unlicensed operations, Europe continues to debate the issue. On the 12th of November, the Radio Spectrum Policy Group (RSPG), a group of EU regulators, is expected to present its final recommendation on the long-term allocation of the upper 6 GHz band. That recommendation will guide a final decision of the European Commission by late 2026/early 2027.

While a hybrid sharing scenario between 5G/6G and unlicensed technologies like Wi-Fi is the most likely recommendation, we expect the RSPG to recommend only a small portion of the band to be allocated to unlicensed technologies, with the rest allocated for 5G/6G. This is mainly due to several factors: 1/Tech sovereignty: Wi-Fi being perceived as a US technology; 2/Preference for EU champions: several Member States such as France, Finland and Slovenia strongly advocating for 5G/6G; 3/Misinterpretation of the recent One Big Beautiful Bill by EU stakeholders, who assumed the US reversed its position on the upper 6Ghz band.

This outcome will not only hurt US technology companies that manufacture Wi-Fi products, but also European consumers and enterprises that rely on Wi-Fi for their connectivity needs. By limiting Wi-Fi's capabilities, Europe will force consumers and enterprises to use 5G/6G connectivity, which costs more than Wi-Fi and has significant limitations for indoor connectivity. In addition, Chinese companies dominate 5G/6G technology and will likely benefit greatly from this outcome in terms of product sales and licensing revenue.

Investment Barriers

Proposal for a Foreign Investment Screening Regulation: In January 2024, the European Commission published a proposal for a new foreign investment screening Regulation. The Regulation would require EU Member States to impose an *ex ante* authorization requirement on all foreign investments involving companies that (i) are active in one of 42 listed “critical technology areas” (e.g., AI, cloud), (ii) are subject to dual-use or military export controls, (iii) provide critical financial or healthcare services, or (iv) participate in a listed EU funding program. This includes investments that do not currently qualify for antitrust review, such as minority investments and greenfield investments. Initial engagement with EU policymakers on this regulation suggests that it is likely to have a significant impact on U.S. investors, subjecting them to extensive review processes.

Ireland - Grid Connection Rules: Ireland's electricity regulator, the Commission for the Regulation of Utilities (CRU), has approved grid-connection rules that unfairly penalize U.S. cloud providers that invested in Ireland in good faith under the connection agreements and grid standards in force at the time. In September 2026, the CRU approved EirGrid Grid Code Modification MPID 345 (Fault Ride Through, Rate of Change of Frequency, and Post-Fault Active Power Recovery for Demand Facilities), taking legal effect in October 2026. The modification requires large demand facilities — predominantly U.S.-operated data centers — to remain connected to the grid during transmission faults and to restore pre-fault demand

within milliseconds, behaving like electricity generators. Critically, these obligations are imposed retrospectively on existing facilities. Every operational U.S. data center in Ireland was designed, built and connected in full compliance with the Grid Code standards and connection agreements applicable at the time, when Fault Ride Through obligations applied only to generators on the supply side and demand-side backup systems were specifically engineered — and approved by the grid operator — to disconnect safely during voltage disturbances to protect sensitive IT equipment. Applying generation-style FRT duties retrospectively to demand customers is, to the industry's knowledge, without international precedent in any other jurisdiction, and reverses the very design parameters operators were previously required to meet. The CRU approved this measure without conducting an independent cost-benefit analysis, despite being asked to, and provided no mechanism for cost recovery for the substantial retrofit investment U.S. operators must now make. It has also imposed tight compliance deadlines even though no fully proven technical retrofit solution yet exists for all facility types, and brownfield sites face real physical, planning and supply-chain constraints. The result is a retrospective change to the regulatory bargain that disproportionately burdens the U.S. firms that have made some of the largest capital investments in Ireland, undermines the legal certainty of their existing connection agreements, and imposes significant unrecoverable costs — penalizing companies that connected to the Irish grid in good faith.

Subsidies

EU Foreign Subsidies Regulation (FSR) implementation: In July 2023, the EU's FSR entered into force, giving the EC new powers to target economic distortions in the EU market caused by foreign subsidies. Under the FSR, the Commission has broad powers to request sensitive business information regarding companies' interactions with non-EU governments, including confidential contracts. The Commission also has broad discretion to decide whether a non-EU subsidy distorts the EU single market and to impose strict sanctions. While the EC claims that the FSR targets subsidies from non-market economies, the FSR in fact subjects U.S. businesses to the same procedures as companies from non-market economies that unfairly compete in the EU market. From October 2023, for example, any company operating in the EU market will be required to disclose "financial contributions" from non-EU governments (e.g., subsidies, certain fiscal incentives, capital injections) granted up to three years prior to their participation in the following activities: (i) public procurement procedures where the tender exceeds €250M and (ii) mergers and acquisitions in which parties' aggregate EU revenues exceed €500M. In addition, the FSR also provides the EC with an *ex officio* tool to investigate financial contributions on an ad hoc basis from July 2023. If the EC finds businesses to have benefitted from "distortive" subsidies, it could: (i) disqualify them from public tenders and M&As in the EU; and (ii) apply regressive measures such as subsidy repayments. Failure to disclose financial contributions or to comply with regressive measures may result in fines up to 10% of companies' global revenue.

Complying with the FSR's intensive reporting requirements has proven to be exceptionally burdensome, demanding significant human and technical resources across global teams. FSR filings are often the most resource-intensive filings for any global transaction. This is in stark contrast to the Commission's initial prediction that the regulation would create a "limited administrative burden". The regulation also disadvantages non-EU businesses by imposing significantly higher compliance costs on them, as they must track non-EU incentive schemes that are not required to be tracked in the EU.

U.S. businesses are also facing excessive information requests under the FSR. The Commission regularly asks for information far beyond what appears necessary for its assessments, including: data on "financial contributions" granted after a notification, often with unrealistic deadlines; and significant information regarding U.S. federal, state and local incentive schemes that are not limited to specific companies or sectors and therefore do not fall under the FSR's own definition of a subsidy. Further, for public procurement procedures, U.S. businesses have been asked to submit multiple FSR filings and repeatedly

update their “financial contributions” for periods exceeding three years.

In March 2025, the Commission issued draft [guidelines](#) seeking to provide clarity on several important aspects of the FSR. Unfortunately, rather than clarifying the application of the FSR, the draft guidelines seek to expand its scope and would create a more uncertain legal environment for U.S. businesses:

- First, the draft deviates from the FSR's original goal by extending its scope to include subsidies without a clear EU connection, introducing a new cross-subsidization theory that any subsidy can "free up" resources for EU activities, regardless of intent or use. This effectively reverses the burden of proof, requiring companies to disprove cross-subsidization.
- Second, the draft weakens the FSR's distortion test. It proposes a low legal standard, where a "reasonable link" or even a minor contributory relationship between a foreign subsidy and a negative impact on EU competition is sufficient for a finding of distortion.
- Finally, the draft expands the FSR's public procurement scope. Beyond current notification obligations, it adds compliance burdens by allowing examination of any "financial contributions" from any corporate group entity under vague "specific circumstances." This undermines legal certainty and proportionality, potentially hindering businesses from participating in tenders due to demands for extensive information during short deadlines.

Overall, the FSR has created significant legal uncertainty and disproportionate compliance burdens and costs for U.S. businesses and investments in the EU.

Other Barriers

EU Defense Funding and Procurement: The EU is preparing a full revision of its Defense Procurement Directive, with a legislative proposal scheduled for Q4 2026, which are likely to reshape market access requirements and opportunities across the sector. The Security Action for Europe (SAFE) framework, adopted in May 2025, establishes a €150 billion loan instrument to help Member States finance common defense procurement, with strong ‘European preference’ requirements. To qualify, contractors and subcontractors must be established and have their executive management in the EU, EEA, EFTA states or Ukraine, and must not be controlled by third-country entities. Components originating outside these countries must not exceed 35% of the estimated component cost of the end product, and for certain products, contractors must be able to define and evolve the product design without third-country restrictions (e.g., export controls). The European Defence Industry Programme (EDIP), a €1.5 billion grant instrument signed into law in December 2025, also carries similar ‘European preference’ requirements. Looking ahead, the Commission's proposed 2028-34 Multiannual Financial Framework allocates €131 billion to defense and space through the European Competitiveness Fund, roughly five times more than the previous MFF. Detailed eligibility rules are not yet set, but this funding is expected to include 'European preference' requirements similar to those in SAFE and EDIP. For U.S. providers, this could mean several structural barriers. Preference criteria modelled on SAFE and EDIP would favor entities from eligible countries and require U.S.-owned suppliers and their EU subsidiaries to demonstrate freedom from foreign control to qualify.

Spain - Draft Royal Decree on Data Center Requirements

In August 2026, the Ministry for Ecological Transition published a draft Royal Decree introducing

requirements for energy efficiency, environmental sustainability, resilience, and digital sovereignty applicable to data centers. The text underwent public consultation and is expected to be published in the coming months. The regulation will make grid access and connection permits for data centers conditional on compliance with a comprehensive set of requirements that go beyond existing EU frameworks. On the energy side, the draft establishes mandatory energy and water efficiency thresholds (PUE/WUE) that are misaligned with existing EU requirements, an 80% renewable energy consumption quota with hourly matching requirements, additionality requirements for power purchase agreements with narrow time windows, and a financial surcharge regime backed by permit revocation for non-compliance. On the sovereignty side, the draft requires that all data, metadata and operational logs derived from the data center operation to remain within EU territory. It further prohibits the hosting of public sector data under the National Security Framework unless all data – including telemetry, replicas and backups – is processed and stored exclusively within the EU.

Spain - Draft Royal Decree on Foreign Investment Screening

In September 2026, the Ministry of Economy, Trade and Enterprise opened a preliminary public consultation on a new draft Royal Decree on foreign investment screening, which would replace and expand the existing framework under Royal Decree 571/2023. Among the most significant proposed changes, the new regulation would extend the scope of Spain's foreign investment screening regime to greenfield investments that were previously exempt from prior authorization requirements. The draft also contemplates the inclusion of data centers as a specifically listed sector subject to screening. The proposed expansion of the screening mechanism to greenfield investments represents a significant shift from the current regime, which is limited to acquisitions and changes in control of national companies, and could introduce additional regulatory uncertainty for companies planning new infrastructure deployments in Spain.

Guatemala

Import Policies

Physical Inspections and Authorized Economic Operator: Guatemala Customs maintains disruptive physical inspection rates exceeding fifty percent, even for trusted Authorized Economic Operator certified express companies. This undermines compliance programs, causing severe clearance delays and inflating operational costs. NFTC recommends that USTR press Guatemala to honor AEO principles by drastically reducing inspection rates for certified partners and implementing data-driven, selective screening to restore predictability for U.S. exporters.

Honduras

Import Policies

Pearrival Processing and Trade Agreement Compliance: Honduras violates CAFTA-DR Article 5.7 by failing to provide functional digital mechanisms for the submission and processing of manifest data before arrival. Without a prearrival framework, customs cannot clear low-risk express cargo proactively, guaranteeing systemic delays for U.S. exports. NFTC recommends that USTR initiate formal compliance reviews to compel Honduras to deploy integrated systems that support rapid, automated clearance.

Modernization of Customs Information Technology Infrastructure: Honduran customs operations are

heavily restricted by a severe lack of investment in modern information technology infrastructure. This chronic underfunding prevents the implementation of the automated, paperless, and expedited clearance procedures explicitly required under the CAFTA-DR framework.

Iceland

Services Barriers

Streaming Investment Obligation/Levy Proposal: In December 2025, Iceland introduced a bill in parliament establishing a 5% tax on the gross local revenues of subscription VOD services operating in Iceland. The tax could be offset by qualifying investments. The target of the bill is U.S. streaming services. The Explanatory Memorandum accompanying the bill was explicit that the purpose of the bill was to change the competitive balance between international (U.S.) and domestic streaming services and benefit local producers.¹⁰ The Memorandum emphasized that local streaming services would not be covered by the measure or would not be burdened by it because their business is based on Icelandic content. Iceland withdrew the bill in February 2026. However, in September 2026, the Minister of Culture announced that Iceland would be reintroducing the proposal in fall 2026.

India

Import Policies

Duplicative Package Screening: Currently, India requires all inbound volume, regardless as to whether it enters the Indian market or is merely transiting through India, to be off-loaded and screened a second time. (The first time being outbound from the previous country or origin along the route). Cargo is required to transfer through the Transfer Cargo Security Hold Areas (TCSHA). However, shipments routed through domestic transit points are often subjected to duplicate package-level screening at both origin and transit points. This increases dwell time and reduces network efficiency. Further, while volume is held in TCSHAs there can be delays in approving release, due to the limited availability of approving offers. We recommend accepting a single security screening for secured Unit Load Devices (ULDs) at either the origin or a previous point of transit. In sum, India should be encouraged to alter regulations to allow international-to-international tail-to-tail transfer of sealed ULSs for AEO certified operators. India should also be strongly encouraged to launch or adopt a digital transshipment approval platform that can operate 24/7. This will reduce cargo dwell time, process transshipments faster, and improve aircraft connectivity and turnaround time. It will lower operating costs, enhance logistics efficiency and strengthen India's position as a regional transshipment hub.

Unfair Import Tariffs: Since 2014, India has imposed a 20% tariff on imported switches and other products that fall under HS 85.17 and should be tariff-free because its bound rate for this tariff code is zero. This is unfair because the United States accords duty-free treatment of such products when they are imported from India. In its recent Union Budget, the Indian government harmonized the differential duty rate between carrier grade and enterprise grade switches to a uniform rate of 10%. Earlier, carrier grade switches had a 20% customs duty. While a step in the right direction, the lower duty rate is still not zero.

Import Authorization for Ultra-small Form Factor Computers and Servers and Information and Communication Technology (ICT) Equipment: In August 2023, the Indian government announced that

¹⁰ <https://www.althingi.is/altext/157/s/0444.html>

beginning November 1, 2023, import authorizations are needed to import laptops, tablets, all-in-one personal computers, and ultra-small form factor computers and servers. India has implemented an import monitoring system (“IMS”) to monitor the import of ICT products. The Ministry of Electronics and IT deliberates on the applications before the Directorate General of Foreign Trade (DGFT) can grant the authorizations. This import authorization requirement delays and disrupts imports of in-scope information and communication technology (ICT) equipment into India. U.S. companies have applied for import licenses for servers.

Additionally, India has implemented an import monitoring system (IMS) to monitor the import of ICT products such as laptops, tablets, PCs, and servers. This is intended to discourage imports and force local manufacturing. U.S. companies have applied for import licenses for servers. However, India only granted licenses for approximately 25-35% of the value of imports requested. India has continued the IMS through calendar year 2026. Under DGFT Policy Circular No. 08/2025-26, importers must obtain authorization through the IMS, with authorizations valid through December 31, 2026. The current framework does not impose a stated quota or hard cap, but it preserves the possibility of a midterm review and gives DGFT broad authority to amend, suspend, or withdraw the procedures based on policy requirements. India’s action is an unfair restriction on market access that negatively impacts the ability of U.S. companies to compete in the Indian market. Additionally, there are concerns of the IMS evolving into a quota system which would cause supply chain disruptions or include requirements for local sourcing/manufacturing before import licenses are granted. Introducing such a quota would also be a violation of India’s WTO obligations.

Export Controls: In an effort to diversify supply chains away from China but continue to have a regional fulfillment model, U.S. companies have recently invested in India manufacturing capabilities. The Indian government has stringent export control rules for dual-use items, called Special Chemical, Organisms, Materials, Equipment & Technology (“SCOMET”) Rules. India considers specific telecom products to be dual-use, and therefore, to export from India, U.S. companies are mandated to obtain an export license.

Under the SCOMET rules, the OEM must submit End-User Certificates (EUC) from all end users. This is a challenge, as the exports are likely to be re-transferred multiple times within the supply chain before they reach the end user. Further, there is also a requirement for post-reporting of exports made from India to the stockiest, transfers made by the stockiest to the final end-users and inventory with the stockiest as on December 31 of each calendar year, by January 31 of the following year. A failure to do so may entail penalty and/or cancellation of authorization. Meeting this requirement even on a post shipment basis would be impossible. Most importantly, there is no global precedence of such documentation for export licenses.

U.S. companies have provided an end user certificate on behalf of customers and have also agreed to facilitate Post shipment verification of the items at end users' site if required by the Government of India, after prior/suitable notification. Some companies obtained licenses for a period of two years based on exemptions, especially from the EUC from customers. This is unfair, because the U.S. government provides bulk export licenses without such onerous requirements to exporting companies for dual-use items. A failure to obtain export licenses other than on an exemption basis hurts U.S. company’s ability to scale manufacturing for additional products.

Illicit Trade: Illicit trade is becoming a more substantial challenge for U.S. companies operating in the region, raising health and safety concerns for patients. One issue of concern is the increase in illicit trade crossing the border between India and Bangladesh. NFTA urges USTR to encourage intensive training,

strategic deployment of resources, and greater partnership between Indian and Bangladeshi authorities – which should include a cross departmental task force with MoH, DoP, and Ministry of Home and Customs. In addition, authorities should take greater action against websites selling illicit medicines and local distributors facilitating their spread.

Express Cargo Clearance System Reliability: In June 2026, a nationwide failure of India's customs electronic data interchange system halted clearance of courier and express shipments at major international airports. Thousands of time-sensitive import and export shipments were stranded until manual workarounds were arranged. With no standing backup procedure, every outage turns into a case-by-case negotiation, which erases the speed advantage express shipping depends on. NFTC recommends that USTR urge India to adopt reliability standards for the Express Cargo Clearance System (ECCS) and a published, binding backup plan that automatically allows manual or deferred clearance of express shipments during outages.

Technical Barriers to Trade

Mandatory telecom certification framework: Indian Telecom licensees are required to connect their networks only with telecom equipment that has been tested and certified under the Mandatory Testing and Certification Framework (MTCTE). The mandatory testing and certification scheme is operational for certain IT and telecom products on parameters of safety, functionality, and perhaps security as well. The scope of this requirement was recently increased to include cloud software (Hypervisors), which goes beyond telecom products. This marks a significant policy shift, extending regulatory oversight from physical network equipment to virtualized and software-defined network elements, thereby broadening the ambit of compliance obligations for cloud service providers and telecom operators alike. This expansion introduces onerous localization and testing requirements for software that is not manufactured or deployed solely in India. Hypervisors and other virtualization software are typically developed, tested, and maintained globally, often as part of multi-tenant, cloud-native architectures. Requiring such software to undergo local testing – and potentially disclose proprietary source code or security configurations — can expose intellectual property, conflict with global security standards, and delay product deployment cycles. Moreover, since MTCTE is applied only to equipment and software used by Indian telecom licensees, it disproportionately affects foreign suppliers who serve the Indian market, while domestic software or cloud providers may face fewer compliance hurdles if their infrastructure is already localized. In practice, this creates a de facto barrier to market access, inconsistent with India's commitments under the WTO's Agreement on Technical Barriers to Trade (TBT), which discourages discriminatory treatment and mandates that conformity assessments not be more trade-restrictive than necessary. The inclusion of cloud-based software like hypervisors under MTCTE represents an undue regulatory burden — one that duplicates existing international certifications and cybersecurity frameworks (such as ISO/IEC 27001, SOC 2, or FedRAMP) already adhered to by global providers. Instead of enhancing national security, it risks fragmenting global cloud operations, increasing compliance costs, and reducing the competitiveness of international firms in India's rapidly growing digital infrastructure market.

Restrictions on Multi Brand Retail: India has restricted American e-commerce providers from operating in the market on a level playing field as domestic companies, including through limitations on foreign companies operating in “multi-brand retail trading (MBRT).” This means that any company with foreign investment, including American e-commerce companies, cannot sell its own inventory directly to customers, requiring significant changes to their business models. These rules, which began in 2012 but were expanded in 2016 and 2018, establish several obstacles to American companies operating in India. American companies cannot invest more than 51% in a firm operating in India, with a minimum investment requirement of \$100 million that carries obligations micromanaging companies' business decisions. For example, at least 50% of this initial FDI must fund backend infrastructure such as

processing, storage, distribution, and logistics, and at least 30% procurement of manufactured or processed products must be from Indian micro, small, and medium industries. American companies are prohibited from selling their own inventory directly to consumers and are only permitted to operate a marketplace business model. They also face severe restrictions for marketplace e-commerce operations, including being unable to set prices, facing limitations on inventory management, and being prohibited from entering seller exclusivity arrangements. Specifically, American marketplaces and their group entities cannot provide more than 25% of the inventory for any of the vendors using their service. The regulation undermines American companies' ability to efficiently reach Indian consumers and optimize their supply chains. None of the above restrictions apply to domestic, non-FDI-funded entities. Domestic companies are permitted to operate inventory-based models without any additional conditions and have complete flexibility in pricing, inventory management, and seller exclusivity agreements for their e-commerce operations. These restrictions prevent leading U.S. e-commerce companies from accessing the rapidly growing Indian market, undermine current and potential investments in the U.S., and diminish U.S. technology leadership.

Market Access Challenges (Pharmaceuticals): The Indian government's largest public health program, Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (AB-PMJAY), which provides health coverage to over 700 million Indian citizens, does not reimburse any patented medicines. Instead, it only covers locally produced generic drugs, creating a significant barrier to market access for innovative U.S. pharmaceutical products. The Indian government uses a different pricing mechanism for patented drugs that requires them to meet unreasonable prices resulting from a cost effectiveness analysis that is not suited to India's socio-economic parameters. By design, this framework excludes all innovative medicines by deeming them 'not cost effective'. This is in contrast to the approach followed for locally produced generics for incorporation into the AB program, thereby creating a de facto ban on innovative medicines. While generic drugs are priced based on existing government-negotiated rates for programs such as CGHS and ESIC, patented medicines are subject to a health technology assessment (HTA) analysis that typically demands up to an 80% lower price, effectively pricing out U.S. innovators. These barriers stand in stark contrast to the substantial access Indian companies have to the U.S. pharmaceutical market contributing to the trade imbalance. Increasing U.S. companies' share of the AB program will increase exports and jobs in the United States, while also creating tremendous revenue potential.

- **Regulatory Uncertainty & Delays:** At present, Indian authorities require significant additional local data and studies to approve new therapies and clinical trials for the market that are already approved worldwide. In 2024, India issued guidance to implement Rule 101 that allows drugs approved by U.S. FDA (and others) to be approved in India without requirement of local trials, if companies undertake to conduct post launch trials in the country. However, this process (Rule 101) is not being used as expected in practice. The lack of operationalization of this rule amounts to a technical barrier to trade in our view and unfair treatment of U.S. companies, as Indian companies are not required by the FDA to submit local data.
- **Price Controls on Innovative Medicines:** India imposes price controls on drugs that are supplied not only to the government but also in the private non-reimbursed market. Several provisions of this pricing policy place unreasonable commercial restrictions on medicines, including patented/innovative medicines developed by innovative bio-pharmaceutical companies. A rational and predictable pricing policy will go a long way in enhancing confidence, allowing for longer-term market entry planning, and creating reasonable expectations in the marketplace.

Government Procurement

Discriminatory Government Procurement Policies: India's public procurement policy has evolved over the years and required stricter implementation, especially for the telecom sector. Various regulations, such as the General Financial Rules ("GFR") 2017, the Public Procurement (Preference to Make in India) ("PPP-MII") Order, 2017, and sector-specific regulations, establish procurement guidelines for central ministries, departments, and public sector enterprises. The PPP-MII Order was updated in 2020 to create specific classes of local suppliers with varying levels of value addition. This is further customized by each Department for each notified product. The Department of Telecom's PPP-MII policy mandates extremely high value addition thresholds for telecom products and requires 100% component localization and a high percentage of value attributable to an Indian intellectual property (i.e. a design patent residing in India).

Such government procurement policies are unfair, because they favor domestic suppliers and discriminate against U.S. companies that seek to compete fairly in India's government procurement market.

Local Content Requirement: Aligned with the Government of India's continued rhetoric on self-reliance, the Public Procurement (Preference to Make in India), Order 2017 and subsequent revisions mandates that only Class-I suppliers (with local value addition >50%) and Class-II suppliers (local value addition – 20% to 50%) are eligible to bid for government procurement. This is applicable to both products and services. This order poses a significant compliance challenge in particular to foreign software and cloud service providers (CSPs) to demonstrate local value add. This model does not consider the investments and other contributions made by foreign CSPs that enable the Indian Tech ecosystem and their global competitiveness, such as skilling initiatives, cloud innovation centers, quantum computing lab etc. Even if CSPs don't directly bid for government contracts, partners need to certify their percentage of local content, for which they rely on their vendors' local value addition as well. For example, where cloud services are a substantial cost element in a public procurement bid, the percentage of local value added from a CSP becomes important. Moreover, the Indian government is considering revisions to the order and increasing the minimum local content requirement for Class-I suppliers to 60% and Class-II suppliers to 30%.

Intellectual Property Protection

IP Challenges: American companies face continued IP violations in India including lack of regulatory data protection, patent linkage, and patent term restoration. Substantial reform is needed in the IP policy frameworks to meet trade obligations and ensure American IP is treated the same as Indian IP in the United States. We were encouraged by a recent amendment to patent rules addressing concerns around pre-grant opposition delays. However, there are larger issues at hand that must be addressed to prevent patent infringements in India. Such infringements are enabled by a gap between federal patent grants and state drug approvals. India should amend the IP and regulatory laws to make it necessary for drug approval authorities to verify absence of existing patents prior to granted approvals for generics. Additionally, it should institute a system where all applications for drug approvals are put up on a public platform so that patent holders can take preemptive legal action where it is merited.

Services Barriers

Requirement to Report Importation of "Non-physical Imports": Indian banks have a requirement to advise Indian Customs of the importation of "non-physical imports" when related to Direct Import Remittances. This requirement appears to originate from a 2010 Circular "Master Circular on Import of Goods and Services" of the Reserve Bank of India. Specifically, the requirement is: "Payment for

software download. If the import payment is towards design and drawing, advance payment for Software import, a Declaration from the importer is required confirming that they will inform customs of such import.” Therefore, a U.S.-origin sale to an Indian buyer of downloaded software would be considered a capital good under Indian regulations. Thus, the payment is leaving India to the U.S, and the requirement forces the importer to obtain specific certifications in order to release funds from the bank.

Financial Services: The United States has continued to raise concerns relating to informal and formal policies with respect to electronic payments services that appear to favor Indian domestic suppliers over foreign suppliers. The National Payment Council of India (NPCI) is a quasi-government agency that operates the largest domestic payment system in the country, including Unified Payments Interface (UPI) and RuPay (debit and credit) cards. In the past several years, the Government of India has taken many direct and indirect actions that give preferential treatment to NPCI, creating a non-level playing field for international EPS providers, including:

- RuPay and NPCI are the de facto solutions for any Government disbursement programs, known collectively as Direct Benefit Transfers (DBT), and are now being pushed in government-driven credit and commercial transactions, keeping U.S. international networks out of consideration.
- Storage of cards on file and tokenization are globally recognized to offer faster, more secure, and seamless customer experiences where B2C or Account to Account transactions are concerned. In September 2020, the RBI issued guidelines disallowing storage of cards on file by merchants and payment aggregators. Given that this ban did not extend to the UPI network it provides NPCI with an unfair advantage.
- In November 2020, the state-owned National Payments Corporation of India (NPCI) announced a market share limitation of 30 percent (measured by transactions) for foreign electronic payment service suppliers processing online payments made through India’s Unified Payment Interface, which is owned and operated by NPCI.

India has enabled the linking of credit cards to the UPI through RuPay credit cards. While UPI has become an increasingly important channel for digital payments, other qualified card networks authorized by the RBI do not currently have an equivalent pathway to enable their credit card credentials for UPI transactions. The absence of transparent and non-discriminatory access criteria may limit competition and consumer choice in the provision of credit-based payment services conducted over UPI.

USTR should urge India to establish and publish transparent, objective, and non-discriminatory eligibility, technical, security, routing, certification, and commercial requirements that permit all qualified RBI-authorized card networks to participate in UPI credit-card functionality on fair and reasonable terms. Expanding access would promote competition and consumer choice while preserving the security, interoperability, and regulatory oversight of the UPI ecosystem.

Transit - National Common Mobility Card: India continues to promote the National Common Mobility Card (NCMC) for public-transit payments. Government requirements and implementation practices centered on NCMC-specific compliance can limit the ability of transit operators, banks, and other ecosystem participants to accept existing globally interoperable EMV contactless cards and credentials.

The R

BI's support for a controlled industry pilot involving card payments at transit touchpoints is a constructive development. India should build on this progress by establishing a durable, transparent, and technology-neutral framework under which public-transit operators may accept existing EMV contactless debit, credit, prepaid, and tokenized mobile credentials alongside NCMC products.

USTR should urge India to establish a permanent, transparent, and technology-neutral framework that permits globally interoperable EMV contactless payment credentials to operate alongside NCMC in public-transit systems. Participation, certification, security, liability, and commercial requirements should be applied on fair, reasonable, non-discriminatory, and non-exclusive terms, allowing transit operators to select among qualified payment networks and technology providers.

Credit on Unified Payments Interface (UPI): India has enabled the linking of credit cards to the UPI through RuPay credit cards. While UPI has become an increasingly important channel for digital payments, other qualified card networks authorized by the RBI do not currently have an equivalent pathway to enable their credit card credentials for UPI transactions. The absence of transparent and non-discriminatory access criteria may limit competition and consumer choice in the provision of credit-based payment services conducted over UPI.

USTR should urge India to establish and publish transparent, objective, and non-discriminatory eligibility, technical, security, routing, certification, and commercial requirements that permit all qualified RBI-authorized card networks to participate in UPI credit-card functionality on fair and reasonable terms. Expanding access would promote competition and consumer choice while preserving the security, interoperability, and regulatory oversight of the UPI ecosystem.

Sovereign Cloud Framework: In March 2026, India's IT ministry, (MeitY), advised government ministries and departments to classify their data by sensitivity. The advisory sets out tiers, and the top tier, "Category A," covers the government's most critical systems. Examples include Aadhaar (India's national digital ID), UPI (Unified Payments Interface, India's instant payments network), tax systems, and land records. Category A systems may be hosted only on a government-run cloud or by an approved "Sovereign Cloud Provider," a vendor specifically cleared to host such data. Classification is left to each department, but most departments are likely to label their most important systems Category A to be safe. That behavior could pull a wide swath of government workloads behind these hosting limits.

MeitY has proposed a Sovereign Cloud Framework (the "Framework") to decide which companies may become approved Sovereign Cloud Providers. The Framework sets 26 conditions and works as a pass-or-fail test, so a company that misses even one condition may be disqualified. Several conditions are based on ownership, not on how secure or capable its technology is. As proposed, an approved provider must be majority Indian-owned, led by Indian citizens, and answerable only to Indian law. Its core cloud software and security tools must also be Indian-built or open-source, meaning publicly available, non-proprietary code rather than a vendor's own systems.

Under the proposed conditions, no U.S. cloud provider can currently qualify as a Sovereign Cloud Provider, because none are Indian-owned. As a result, a large share of Indian public procurement business may be closed to U.S. firms based on country-of-origin rather than the security of the technology. This outcome is concerning given that it may apply to U.S. firms that have invested heavily in India and offer strong technical safeguards.

Digital Commerce/Digital Trade Barriers: In 2018, the Reserve Bank of India (RBI) implemented a requirement that all payment service suppliers store all information related to electronic payments by

Indian citizens on servers located in India. RBI announced this rule without advance notice or input from stakeholders. In 2019, RBI stated the requirement to store payments data locally also applied to banks operating in India. Foreign firms assert that the data storage requirement hampers the ability of service suppliers to detect fraud and ensure the security of their global networks.

Potential data localization under Data Protection Rules: The Digital Personal Data Protection (DPDP) framework permits cross-border transfers of personal data, subject to any restrictions that the Central Government may subsequently specify. The framework therefore does not impose blanket data localization requirements. At the same time, the DPDP Rules create a mechanism for targeted localization. For Significant Data Fiduciaries (SDFs), the Government may specify categories of personal data, based on the recommendations of a committee (yet to be formed/notified), that cannot be transferred outside India, along with traffic data relating to the flow of such data. The specific categories of data to which these restrictions would apply have not yet been clarified. There is consequently some uncertainty around the eventual scope and application of these provisions, including which data categories may be subject to localization and how the requirements would apply to SDFs in practice. Greater clarity on these parameters would provide businesses with greater certainty when designing cross-border data and infrastructure arrangements.

Direct Tax Permanent Establishment Issue for Cloud Service Providers (CSPs): India's income tax laws are ambiguous on whether the provision of data center services by an Indian entity to a foreign entity establishes a taxable presence, such as a permanent establishment (PE) or business connection, for that foreign entity. This risks overly broad tax liability for cloud service providers (CSPs) on their tax liability in India. CSPs typically have arrangements with the data hosting service providers (which may be a group affiliate of the CSPs) owning and operating the data centers across the globe including India. The data centers can serve the customers of any region and are not limited to the local customers. CSPs operating in India are facing tax uncertainty, as in their recent tax audits/ assessments the tax authorities are claiming that CSPs constitute Permanent Establishment ("PE") in India. Tax authorities are claiming that the CSPs have control over data centers through the technology/ software that gets deployed on the data center and cloud services are provided by CSPs through clusters of servers in the data centers in India. This creates a net new, large direct tax impact on American CSPs who are investing billions of dollars in the country and need business and taxation certainty to operate. In July 2025, the case of *Hyatt International* raised further questions over taxation certainty when India's Supreme Court ruled that continuous and substantive control over operations of Indian entities established fixed place PE.

Content Moderation: India's digital economy presents significant opportunities for U.S. digital service exporters, yet increased government control over online speech poses a growing concern. Indian policymakers have rapidly escalated censorship practices and restrictions on companies that fail to remove content deemed "objectionable", leading to novel and aggressive enforcement actions against U.S. firms. Direct censorship measures like internet shutdowns have resulted in substantial human rights impacts and economic losses, with U.S. social media companies like Facebook, Instagram, YouTube, and Twitter incurring an estimated \$549.4 million in losses between 2019 and 2021 alone.

Legislative changes in 2023, particularly the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (amended in 2023), further challenge U.S. exporters by imposing onerous obligations on intermediaries. These rules require online platforms to prevent the display and sharing of an extremely broad range of information, including content deemed obscene, harmful to children, or that "threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognizable offence, or prevents investigation of any offence, or is insulting other nation". The rules also impose strict content takedown timelines, onerous due diligence requirements, and localization and traceability mandates that could compromise security

encryption, leading to privacy and security risks, a chilling effect on human rights, and potential over-removal of legitimate content. Additionally, the IT Rules provide expansive government oversight and regulatory control over Internet content through Grievance Appellate Committees and fact-checking bodies, blurring the lines between self-regulation and state control. The Sahyog portal, launched in October 2024, expanded government powers to issue takedown and blocking notices, a move recently upheld by the Karnataka High Court, raising concerns about the fundamental rights of foreign companies.

Further, efforts by the Telecom Regulatory Authority of India (TRAI) and the Ministry of Information and Broadcasting to expand the regulation on online service providers raise concerns of regulatory overreach and duplication, and censorship:

- In July 2023, TRAI proposed to bring OTT providers into the same licensing and registration framework as telecommunications operators, and “selective banning” of certain OTT services. TRAI has, however, yet to issue final binding rules for licensing or selective banning of OTT providers.
- The Ministry of Information and Broadcasting proposed a draft Broadcasting Services (Regulation) Bill in 2023, expanding the scope of broadcasting regulation from traditional broadcasters and platforms with online curated content to also include social media platforms and independent content/video creators, potentially subjecting them to broadcast-style oversight, including content evaluation committees and registration requirements. While the Bill was ultimately withdrawn in 2024, the government’s intent to extend broadcasting-style regulation to online services raises alarms both for the internet ecosystem and the ability for online services providers to operate in India with regulatory certainty while also raising grave freedom of expression concerns.

India's escalating censorship, internet shutdowns, and stringent IT Rules, including localization and traceability mandates, impact digital service providers that are disproportionately American by increasing compliance burdens, compromising security and privacy, and creating a chilling effect on human rights and future investment. Additionally, the expanded government oversight and potential for selective banning and regulation of OTT and other online content services and producers further threaten the operational freedom and market access for these entities.

Delays in Bureau of Indian Standards Certificate: Entities (factories) looking to export certain ICT equipment (including server-racks) into India must apply for a BIS certificate. Applications from factories based in South-East Asian countries require a No-Objection Certificate (NOC) from the Ministry of Electronics and IT (MeitY). The requirement for the NOC substantially delays the release of the certificate for factories delivering Highly-Specialized Equipment (HSE) into India adversely impacting the supply chain of critical equipment into India. Global AI development cycles are rapidly accelerating with evolving customer demands where they need data center capacity (infrastructure and racks) immediately on a very short notice (in weeks). Delays and long lead times often render equipment obsolete by the time it is certified/ready to land in-country. To import the AI/ML server racks (containing servers), the current process of dual licensing system, involving both BIS certification and DGFT import authorization, requires ~6-8 months, which risks delaying the deployment of the latest technology. This delay affects the speed with which customers are able to access cloud services. The BIS should be removed for equipment that is for self-use if CSPs are complying with the international regulatory safety standards in accordance with IEC and local safety laws. Removing the 100-unit HSE cap would allow for rapid deployment of the latest AI/ML technologies in India, securing India’s place as an industry hub. Streamlining the certification process and removal of the MeitY NOC restriction based on manufacturer

location will also address concerns on ability to scale and meet our demands in India.

Ex ante digital competition proposals: India withdrew its draft Digital Competition Bill (DCB) in 2024 following stakeholder opposition. The bill was modeled on the EU’s Digital Markets Act and would have established an ex-ante regulatory framework applicable to “Systemically Significant Digital Enterprises,” imposing obligations not applied to other market participants. The Indian government subsequently commissioned a market study, now being conducted by the Management Development Institute (MDI) Gurgaon, to examine revised thresholds for SSDE designation. Stakeholder questionnaires and public reporting indicate the government intends to retain the core ex-ante framework, with higher thresholds under consideration that would exclude major Indian platforms while continuing to capture large foreign firms, including U.S. companies. A revised bill could be introduced as early as the Winter Session in December 2026 or the Budget Session in February 2027. Separately, the Competition Commission of India has initiated multiple proceedings against U.S. companies and has indicated it will open new investigations into the deployment of AI tools by U.S. firms in India. USTR should continue to monitor the DCB’s development and engage with Indian counterparts in advance of any revised legislative proposal.

Data localization and data flows: In October 2018, the Reserve Bank of India (RBI) implemented a requirement for all foreign payment system providers to ensure that data related to electronic payments by Indian citizens are stored on servers located in India. The requirement for local storage of all payment information is explicitly discriminatory as it raises costs for payment service suppliers and disadvantages foreign firms, which are more likely to be dependent on globally distributed data storage and information security systems. Government data on the cloud is also localized in India and the upcoming privacy bill might impose further data localization requirements for all companies, including US CSPs.

The now-withdrawn Personal Data Protection Bill, 2019 (PDP Bill) proposed a data localization mandate requiring businesses to ensure the storage of certain categories of personal data in India. Under this now-withdrawn bill, cross-border transfers of sensitive personal data would only be allowed on limited legal bases, such as under contracts that are approved by a proposed regulator. The PDP Bill is currently being revised, and while government statements indicate streamlining and limiting the data localization measures, it remains to be seen if this will be the case. Retention of the data localization mandates could seriously impede cross-border data flows and free trade.

In February 2021, MeitY released the 2021 Intermediary Guidelines and Digital Ethics Code (Guidelines), which impose significant and burdensome requirements on a wide range of internet-based service providers, particularly those that operate social media, messaging, and streaming news and entertainment services. The Guidelines were notified to the Gazette of India without public consultation and are significantly different from the version MeitY had initially released for public comment in December 2018. Many of the new requirements entered into effect immediately, while “significant social media intermediaries” (5 million or more registered users in India) were given only three months to comply with sweeping regulatory changes that in some cases require significant technical re-structuring of services. These changes include the appointment of a Chief Compliance Officer, who can be held legally liable if the intermediary fails to observe the “due diligence” requirements. In addition to concerns over the lack of comprehensive stakeholder engagement, the Guidelines contain many troubling elements that could undermine privacy, security, and freedoms of speech and expression. There are also concerns about whether the Guidelines force the localization of company operations and restrict market access for non-Indian companies through the imposition of burdensome regulatory requirements that erode safe harbor protections in India’s Information Technology (IT) Act and significantly overstep international best practices. Additionally, the Indian government is reported to be currently working on a significant revision to the IT Act governing intermediary liability protections in India (the “Digital India Act”)

Electronic Payment Services: India has made significant progress in expanding digital payments and financial inclusion. However, certain government policies, incentive programs, and infrastructure initiatives continue to provide preferential support to payment systems and payment brands operated by the National Payments Corporation of India (NPCI), including RuPay and the Unified Payments Interface (UPI). For example, government incentive programs supporting digital-payment acceptance have been directed toward RuPay debit and BHIM-UPI transactions, while equivalent opportunities have not been made available to other qualified payment service providers. As a result, government-linked payment, acceptance, promotional, and infrastructure programs may not always operate on a technology-neutral or competitively neutral basis. A more network-neutral approach would support competition, consumer choice, innovation, security, and the long-term sustainability of India's digital-payments ecosystem.

USTR should urge India to adopt a network-neutral approach to digital-payment policies and programs by ensuring that government incentives, acceptance initiatives, promotional measures, and related infrastructure support are available to all qualified payment system operators on fair, reasonable, transparent, and non-discriminatory terms.

E-Commerce Restrictions: India has made significant progress in expanding digital payments and financial inclusion. However, certain government policies, incentive programs, and infrastructure initiatives continue to provide preferential support to payment systems and payment brands operated by the National Payments Corporation of India (NPCI), including RuPay and the Unified Payments Interface (UPI). For example, government incentive programs supporting digital-payment acceptance have been directed toward RuPay debit and BHIM-UPI transactions, while equivalent opportunities have not been made available to other qualified payment service providers. As a result, government-linked payment, acceptance, promotional, and infrastructure programs may not always operate on a technology-neutral or competitively neutral basis. A more network-neutral approach would support competition, consumer choice, innovation, security, and the long-term sustainability of India's digital-payments ecosystem.

USTR should urge India to adopt a network-neutral approach to digital-payment policies and programs by ensuring that government incentives, acceptance initiatives, promotional measures, and related infrastructure support are available to all qualified payment system operators on fair, reasonable, transparent, and non-discriminatory terms.

Source Code Disclosure as Precondition for Product Certification: As a part of its Communication Security (“COMSEC”) scheme, implemented pursuant to the India Telecom Security Assurance Requirements (“ITSAR”), India’s Department of Telecom requires U.S. companies to disclose valuable U.S. source code as a condition for market access. USTR raised this issue via the U.S. Ambassador to India in January 2025. Submission of source code was originally mandated and then the Indian Government reformed the requirement via a notification in June 2025. OEMs are no longer required to submit source code for certification. Instead, they are now required to submit the following: 1/internal test report excluding IP information, including summary of security vulnerabilities/weaknesses classified by risk; and 2/ The “Self Declaration of Conformity” stating that the source code is free from specific vulnerabilities and an undertaking stating, in case of an attack due to product in question, source code will be submitted for testing.

This new requirement continues to be a challenge. The threshold and arbitration of attack or incidence is not defined. Source code includes algorithms, protocols, or defence-in-depth mechanisms that are export-controlled under US Law. The requirement to provide source code in the event of an attack/incident remains. The threshold and arbitration of attack or incidence is not defined. Source code includes algorithms, protocols, or defense-in-depth mechanisms that are export-controlled under US law. The

format proposed by the government for internal test reports is not relevant as they generate a lot of false positives. Vulnerabilities flagged under this tool do not always translate to actual threats in deployed environments. There is also an unrealistic expectation of the code being free from certain vulnerabilities. Industry recommends the following:

1. Security certifications must be based on international standards (e.g., Common Criteria, ISO/IEC 27001/62443).
2. Penetration testing and product-specific Vulnerability Assessment and Penetration Testing (VAPT) by certified labs under agreed scopes instead of source code testing.
3. Support for secure-by-design and secure development lifecycle processes.

The United States does not require the disclosure of source code as a precondition of market access. Second, U.S. companies cannot provide this source code without the appropriate U.S. export licenses issued by the Bureau of Industry and Security (“BIS”) under the U.S. Department of Commerce. Third, the disclosure of source code creates an unacceptable risk that important intellectual property may be stolen. The ITSAR documents for LAN Switches are currently under consultation and are expected to be notified soon. India also requires that all OEMs change their source code to “clean up” security vulnerabilities across notified products, but a deeper understanding of the source code development cycle is required to adequately address the country's security concerns. Moreover, India is demanding that companies turn over internal test reports and testing algorithms, which are proprietary. Again, submitting such reports could constitute a technology transfer that would require a U.S. export license.

Services Barriers - Telecommunications

Draft Telecom Bill: India has put out a draft telecom bill that significantly broadens the definitions of telecom services and telecom equipment to include almost all digital or telecommunications goods and services. Such services including email, messaging, machine-to-machine communications, cloud services will need to be licensed under this new law, and will be subject to onerous licensing, KYC conditions, and raises serious privacy concerns. **With the bill currently under consideration, NFTA urges USTR to take active steps to push back against its proposals.**

Other Non-Market Policies and Practices

Tax Issues: US multinationals continue to face a challenging tax environment in India. Systemic issues with India’s tax system have been highlighted repeatedly during the last decade or so, and while the Indian government has recognized problems with its administrative practices, there has been only limited progress towards alleviating them. The poor success rate in India’s courts by India’s tax authorities is an indication of improper handling of these assessments. The situation is exacerbated by the backlog of tax appeals and litigation in India’s overburdened courts, resulting in an extremely lengthy (often 15-20 years or longer) and costly process to resolve a tax controversy. Further, US companies have experienced that India’s tax auditors quite often refuse to follow a controlling judicial decision or provide unsupported reasons not to refund taxes following an adverse court ruling.

NFTA urges USTR to insist that India implement reforms to its tax administration, including but not limited to: (1) assessing tax if and only to the extent supported by reasonable technical positions with a

basis in the law and taking into account likelihood of success in the court system; (2) removing any incentive for tax auditors to take unsupported positions, such as by requiring for government budgeting purposes the inclusion of a fair estimate of refunds likely to be recovered by taxpayers; (3) creating an incentive structure for assessing officers to be measured based on making well-grounded assessments; and (4) promptly issuing refunds to taxpayers when they are appropriately due, particularly if required to do so by court decision. An additional step would be if USTR (in coordination with US Treasury) could convince India to accept binding arbitration in its tax treaty with the US, which arbitration could be initiated at the request of the taxpayer in the event that MAP does not lead to an agreed resolution.

Indonesia

Import Policies

WTO Information Technology Agreement Commitments: Indonesia continues to contravene its WTO binding tariff commitments by charging tariffs on a range of imported information technology (IT) products that are covered by Indonesia's commitments under the Information Technology Agreement (ITA) which should receive duty free treatment. Indonesia has only implemented ITA commitments that fall under 5 categories of goods/HS codes (Semiconductors, Semiconductors Equipment, Computers, Telecommunications Equipment and Software, and Electronic Consumer Goods). Further, Indonesian Customs has also sought to re-classify IT products into dutiable HS codes that are outside of the 5 categories as a means to raise revenue, but in most cases the reclassified dutiable HS codes are also themselves covered by Indonesia's ITA commitments. For example, Indonesia continues to impose duties on printers and related parts, data center and networking equipment (e.g., routers, switches, servers and server racks, optical modules, and optical cables), and other ICT products, such as solid state drives, that are covered by the ITA. This practice widely affects the IT industry and negatively impacts U.S. investors and their workers.

Inconsistent tariff classification and valuation decisions: Indonesia consistently applies inconsistent classification decisions and valuation methodologies that violate WTO/WCO rules, which include but extend beyond ITA commitments. The administrative process for addressing customs issues in practice does not exist which leaves the importer no other option but to litigate. Indonesia's customs frequently targets importers claiming that they undervalue imported goods by comparing declared values to prices mentioned on random websites and values declared by other importers, rather than on the actual price paid or payable (transaction value). Documentary evidence like Purchase Order, Supplier Payment Invoice, Bank Payment document, SAP Ledger Postings which are typically accepted as evidence by customs in other countries are not being accepted by Indonesia Customs. These arbitrary decisions by Indonesia customs authorities never provide a basis or justification as to why the value is being increased. Further, there is no mechanism on how past imports and future imports of the same items will be treated by Indonesia Customs.

These measures contravene WTO Article VIII of GATT Customs Valuation Agreement which stipulates that the "transaction value" as defined in Article 1 should be used for such determinations.

Restrictions on imports under \$100: In September 2023, the Ministry of Trade ("MOT") issued Regulation No. 31/2023 ("Reg 2023"), which prohibits foreign merchants from selling any goods valued below \$100 to Indonesian customers via online marketplaces and includes several other discriminatory requirements that will restrict imports and foreign investment in Indonesia, including a requirement for foreign ecommerce platforms to receive a permit from the Ministry of Trade in order to conduct business activities in Indonesia and mandates that platforms that meet certain criteria appoint a locally based

representative. Additionally, it prohibits companies with a marketplace business model from acting as a manufacturer and selling their own branded products. Reg 2023 appears to violate Indonesia's international trade commitments, including under the WTO, and will directly affect U.S. exports and the ability of U.S. companies to operate in the country. Regulation No. 31/2023 has since been replaced by Minister of Trade Regulation No. 19 of 2026 on Electronic Commerce. Foreign e-commerce platforms meeting specified thresholds — at least 1,000 transactions or shipments to Indonesian consumers annually, or traffic equivalent to at least 1 percent of domestic internet users — must appoint a local representative through a Foreign Trading Company Representative Office (KP3A). The regulation also maintains a minimum price of \$100 per unit for finished goods sold directly from abroad, prohibits social-commerce providers from facilitating payment transactions directly, and requires covered platforms to configure search, recommendation, and ranking systems to prioritize Indonesian products, including by displaying domestic products in the first row of the first page of results.

Import Restrictions - Survey Report (SR) Requirement: The Ministry of Trade (“MOT”) Regulation No. 87/2015 (“Reg 2015”) applies to imports of goods classified in specific HS codes including servers. The importer is required to appoint a company accredited by the Indonesian Government (known as the “Surveyor”) to inspect its shipment in the origin prior to Customs clearance. The SR requirement was initially enforced by Indonesian Customs (“Customs”), until MOT Regulation No. 51/2020 (“Reg 2020”) introduced a post-entry SR inspection process administered by the Directorate General of Consumer Protection and Trade Compliance of MOT, effective on August 28, 2020. Reg 2015 was repealed and replaced by MOT Regulation No. 20/2021 (“Reg 2021”) effective on November 19, 2021 to introduce new HS codes requiring SR. The product scope covers imports including servers, cooling equipment, hard disk drives, network interface cards and battery back-up units. The SR can cost up to US\$1,600 per shipment and significantly increase the supply chain costs. Although both Reg 2015 and Reg 2021 allow capital goods to be imported without SR if an exemption letter from the MOT is obtained, there has been limited transparency and timeline provided for applying for and issuing such exemption. Under the February 2026 U.S.-Indonesia ART, Indonesia has committed to reforming its pre-shipment inspection mechanism — including through regular engagement with USTR — no later than three months after the Agreement enters into force, and USTR should closely monitor implementation to confirm the reforms eliminate duplicative inspection requirements and establish transparent, predictable exemption procedures.

Import Licensing Complexities: On top of the SR described above, MOT regulation 36/2023 and its subsequent revisions have increasingly become stricter with additional import licensing and SR aimed at protecting domestic industries and managing trade balances. We suggest revising the regulation to exclude goods shipped under \$1,500USD from the requirement to obtain import permits and SR.

Lack of Preclearance Processes: Finance Minister Regulation 190/2022 does not establish a pre-clearance system for physical goods before their arrival in Indonesia. This distinguishes Indonesia from most other markets that do. Indonesian Customs clears goods only upon physical arrival in the country, as they require a physical inspection before releasing the shipment. They argue that they need to verify that proper duties and taxes are collected. Yet this is in contravention to best practices promulgated by the World Customs Organization, but it also marks Indonesia as an outlier in ASEAN. Most other ASEAN countries and territories have implemented pre-clearance processes. Doing so will address port congestion and reduce logistics costs.

Prohibitively High Importer Liability: Finance Minister Regulation NO. 96/2023 holds logistics providers responsible for fines related to importer of record errors. In particular, undervaluation. Further, a new and more recent Finance Ministry Regulation, No. 4/2025, requires brokers to ensure that declarations are completely accurate but levy steep penalties that are disproportionate to the impact of the

small error. Instead of investigating the actual party at fault, Customs holds the transporter liable if the importer is non-compliant and cannot be located. USTR should encourage Indonesia to follow WCO standards and allow for minor post-entry amendments or changes when the error is a mere typo. But in addition, Indonesia should only go after the actual party at fault for errors. Liability should remain with the faulty importer of record and not the transportation provider or carrier.

Halal Pre-Border Verification: Halal Assurance Body (BPJPH) Regulation No. 4/2026 requires imported halal products to undergo mandatory pre-import halal conformity verification in the country of origin or loading. This includes document checks, physical inspections, and issuance of a shipment-specific Halal Product Conformity Report (LPPH) before making a customs declaration in Indonesia. This measure impedes trade by creating an additional non-tariff barrier that increases compliance costs, administrative burdens, and import lead times through mandatory overseas inspections, shipment-by-shipment approvals, and reliance on BPJPH-designated inspection bodies.

Prohibition on Import of Refurbished Products: Indonesia does not permit the import of refurbished products. This policy is unfair because refurbished products and components are essential to supporting customers with warrantied products that have reached end-of-sale without components available as new products. In particular, critical infrastructure customers are unable to obtain replacement parts to service and maintain important infrastructure without access to refurbished products.

Technical Barriers to Trade

Cross-Border Processing and Chip Standards: Core market access concerns of - (i) formalizing offshore processing of domestic credit card and e-commerce transactions, and (ii) permitting internationally accepted EMVCo chip standards for contactless debit - have been substantially addressed through Article 2.29 ("International Payment Networks and Chip Standards") of the U.S.-Indonesia Agreement on Reciprocal Trade (ART), signed February 19, 2026. Under Article 2.29, Indonesia commits to continue allowing U.S. international payment networks to process domestic credit card and card-not-present/e-commerce transactions cross-border, and to allow use of internationally accepted chip standards for all domestic card transactions, including contactless debit.

The United States should monitor Indonesia's implementation of Article 2.29, including whether Bank Indonesia formalizes the current discretionary exemption practice into durable rule changes under PBI 10/2025 and its implementing regulation PADG 32/2025 (effective March 31, 2026, superseding PBI 23/6/PBI/2021, PBI 23/7/PBI/2021, and PBI 23/11/PBI/2021), and whether domestic debit routing continues to default to the national NSICCS standard in practice.

Product Compliance Certification and Testing Requirements for Imports: Under Kominfo Regulation 3/2024, Indonesia requires the individual importer of a product to obtain a product compliance certificate for each product to be imported. A partner or distributor of U.S. products importing products for customers in Indonesia must obtain individual certificates for the products in its own name and cannot rely on certificates obtained by a U.S. company. This means that the U.S. company's contracted importer of record ("IOR") must obtain certificates held in its own name even when importing products for a company's own internal use.

Furthermore, Indonesia requires importers to acquire a separate certificate for the same product that is imported by different parties. A separate certificate is required for a product that has the same IOR but has a different country of origin. Such burdensome regulations deviate far from other countries' certification programs.

Indonesia also requires product labelling on both the chassis and the packaging. Because certification is tied to the IOR, this requires the IOR to open the package to relabel the product. However, an IOR does not have a legal right to open a package. Such impractical and contradictory regulations create high compliance risks for U.S. suppliers.

Additionally, Indonesia requires in-country conformity assessment testing for many consumer goods, including ICT products. Such requirements are covered in various regulations, including Komdigi's Ministerial Regulation 12/2025 that requires a product compliance test report to be issued by a domestic telecommunications device testing center, or by testing centers in countries that have mutual recognition agreements ("MRA") on testing with Indonesia. Komdigi Ministerial Regulation 13/2025 was announced later to enforce the mandatory MRA requirement from Dec 31, 2026. The United States does not have such an MRA arrangement with Indonesia. Korea remains the only country with an MRA with Indonesia, and there is no indication that Indonesia would negotiate MRAs with other countries.

Indonesia's Ministry of Trade is preparing to expand the scope of regulated goods required to obtain Safety, Security, Health and Environment (K3L) registration. The new proposed K3L obligations would cover a broader range of product categories, including electrical and electronic goods. The expanded scope of mandatory local testing is redundant and adds no extra safety value commensurate with additional burden, significantly delays market entry, and increases costs for both industry and consumers. The regulation's requirement for samples to be collected from warehouse through random sampling adds layers of logistical burden, as keeping products stored in-country until the K3L certification process is complete would disrupt supply chain and delay customer fulfillment delivery times. There should also be harmonization and recognition of test reports done by other agencies such as the Ministry of Communications and Digital Affairs. There is also a need to provide for a sufficient transition period (at least 12-18 months) for vendors to manage the change of scope of products covered, with exemption for legal and existing products in the market.

Indonesia's certification and testing requirements are unfair, because they unduly increase costs for U.S. exporters. The tests are duplicative and burdensome for U.S. suppliers whose products have already been tested for safety and conformity elsewhere. Such regulatory hurdles also result in delays and hurt the Indonesian customers' access to products.

Satellite Coordination Prerequisite: In Indonesia, new entrants must complete radiofrequency coordination with one or more national operators before the satellite authorization application can proceed. It is reasonable for a regulator to expect a new entrant to demonstrate that its operations will not cause unacceptable interference. Coordination between two operators, however, can be concluded only where both are willing to engage in good faith. Where a national framework makes the new entrant's authorization dependent on the agreement of an incumbent operator but provides the regulator with no mechanism to resolve the matter if that operator declines to coordinate, the new NGSO entrant can be delayed indefinitely through no fault of its own. There is currently no procedural backstop — a defined timeframe, best practice for protection criteria, a dispute-resolution step, or a regulator-led determination — so that the obligation to protect national service becomes, in effect, a veto on market access in a country.

Government Procurement

Hardware, Software, and Public Procurement: Local Content Requirements (LCR) create uncertainty and limit the ability of multinational service providers to serve Indonesian customers. Ministry of Industry (MoI) Regulation 35/2025 ("Reg 35") explicitly governs "Industry 4.0 Support Services," which

MoI has confirmed includes data center and cloud services. However, the prescribed calculation methods do not account for the unique nature of cloud, creating compliance uncertainty. In government procurement, the minimum LCR threshold for prioritization has been reduced from 40% to 25%. Senior MoI officials have indicated that 25% is attainable for data center and cloud providers where workers are Indonesian nationals and physical infrastructure is in Indonesia, even with fully imported equipment — but local certifiers conducting TKDN assessments lack clarity on how to apply the formula to cloud services in practice, suggesting misalignment between policy intent and on-the-ground enforcement. Meanwhile, the government's e-catalogue still does not recognize cloud as a separate product category, further complicating compliance. Under the U.S.-Indonesia Agreement on Reciprocal Trade (ART), finalized in February 2026, Indonesia committed to exempting U.S. companies and originating goods from LCR. However, MoI issued Reg. 35 less than two months after the ART framework was announced, without any carve-out for U.S. goods or services. The U.S. government should press Indonesia for clarity on LCR enforcement as it applies to cloud service providers operating in Indonesia and ensure full implementation of the ART exemption commitment.

Services Barriers

Localization under E-Commerce Regulations: Indonesia's Government Regulation No. 80/2019 (GR80) on E-Commerce draws a clear distinction between domestic and foreign e-commerce business actors and prohibits personal data from being sent offshore unless otherwise approved by the Ministry of Trade through a list of countries which can store Indonesian e-commerce data. This effectively requires e-commerce business actors to locally reside on personal data for e-commerce customers. GR80 poses *de facto* data localization measures and local content requirements, which increase overhead costs for foreign entities and create undue market barriers.

Import Duty on Electronic Transmission of Digital Goods: Throughout 2018-2022, Indonesia's Ministry of Finance (MoF) issued regulations that aim to collect duties on digital goods. MoF Regulation No. 17/PMK.010/2018 added software and other digital products transmitted electronically, including applications and multimedia products ("intangible goods"), to Indonesia's tariff schedule with import duty rate set at 0%. Later, MoF Regulation No. 190/PMK.04/2022 required an import declaration for intangible goods, which effectively established a customs administrative regime that would result in significant compliance costs and administrative burdens for businesses, such as a custom declaration within 30 days of paying for the intangible goods and import and custom duties, and enable Indonesia to collect duties on intangible goods if Indonesia decides to increase the applicable duty rate from the existing 0%. No other country in the world has similar regulations in place. Under the ART finalized in February 2026, Indonesia has committed to eliminate existing HTS tariff lines on "intangible products" and suspend related requirements on import declarations. Indonesia is also to support a permanent moratorium on customs duties on electronic transmissions at the WTO immediately and without conditions. The Indonesian government should deliver on its commitments by removing intangible goods from its tariff schedules and eliminating the related import declaration requirement, as well as continuing to support the WTO Moratorium on customs duties for intangible goods.

Electronic Payment Services: Government of Indonesia should continue to provide a level playing field. Including by ensuring that:

- Bank Indonesia does not undertake regulatory requirements that hinder U.S. electronic payment services (EPS) companies from processing data internationally and introducing innovations in risk and security to the Indonesian market. Specifically, Under Article 71 (6) of Bank Indonesia Regulation (PBI) 23/7/2021, Bank Indonesia has the discretion to exempt transactions from

onshore processing requirements. [Article 71 (6): “The payment transaction may be processed outside the territory of the Republic of Indonesia to the extent it has been approved by Bank Indonesia”] Therefore, Bank Indonesia should formalize the current market practice of allowing domestic credit card and e-commerce transactions to be processed offshore. This aligns with the Bank Indonesia (BI) Payment System Blueprint 2030's goal of enhancing transaction security and protecting the payments ecosystem and consumers.

- BI should amend regulations on card security to allow for use of internationally accepted chip standards for all domestic card transactions, including for contactless debit (tap-to-pay).

Specifically, current regulations related to card security for contactless (tap-to-pay) transactions require a separate domestic chip standard (NSICCS) that is NOT interoperable or compatible with international (EMVCo) standards [BI Regulation (PBI) 23/11/2021 and Board of Governors Regulation (PADG) 24/7/2022]. In practice, this has resulted in only the domestic chip standard (NSICCS) being used for routing/processing of domestic debit transactions, which in turn prevents Indonesian banks from enabling tap-to-pay features for domestic debit transactions. To facilitate greater participation of all networks and a wider range of choices for consumers, BI should amend the regulation to allow for use of the international standard, with interoperable EMVCo chips, to be used for contactless debit transactions. Both EMVCo and NSICCS standards are complementary and in alignment with BI's approach to developing the QR Indonesia Standard (QRIS), which leveraged internationally accepted EMVCo QR standards. Both standards, governed by PBI 23/11/2021 and PADG 24/7/2022, emphasize the use of standards to enhance payment security. Using national standards that are not interoperable with global standards contradicts the goal of creating a secure payments ecosystem.

Financial Services — Direct Oversight of Third-Party Technology Providers: Bank Indonesia (BI) Regulation No. 10/2025 (PBI 10/2025) and implementing Board of Governors Regulation No. 32/2025 (PADG 32/2025), effective March 31, 2026, transform the oversight model for Supporting Operators — third-party service providers, including cloud service providers, that support payment system participants. While this category existed under BI's previous regulatory regime, Supporting Operators were supervised only indirectly through the payment service providers they served. The new framework shifts to a hybrid model in which BI designates Supporting Operators as direct objects of supervision, asserts authority to impose administrative sanctions directly on them, and establishes a mandatory tiered classification (Critical, Important, Standard) with registration required for Critical and Important operators by March 31, 2029. Operators that fail to register will be barred from collaborating with payment service providers. The regulations also introduce new obligations across operational resilience, governance, data reporting, and cooperation agreements. Key classification thresholds and implementing details remain undefined, creating regulatory uncertainty for U.S. cloud providers and risking compliance burdens disproportionate to their role in the payment ecosystem.

Electronic Transaction Tax (ETT): Under Law 2/2020, Indonesia introduced a series of changes to its tax code, including an expansion of the definition of permanent establishment for purposes of Indonesia's corporate income tax and a new electronic transaction tax (ETT) that targets cross-border transactions where tax treaties prohibit Indonesia from taxing corporate income from the transaction. The ETT blatantly discriminates against foreign companies as it only applies to non-Indonesian operators. Its efforts to deem foreign companies with SEP (significant economic presence) as permanent establishments undermine the traditional definition of a permanent establishment and create a significant barrier to cross-border trade. MOF would need to issue additional legal measures for these new taxes to go into effect. Such proposals are based on an unprincipled and unsupported distinction between digital and non-digital companies. The ART's digital trade provisions, if fully implemented, should preclude activation of the ETT. However, the enabling authority under Law 2/2020 remains on the books and could be invoked at

any time through a Ministry of Finance regulation.

Data Localization: Indonesia is currently planning to revise Government Regulation No. 71/2019 (“GR71”) that, based on the 2024 draft, potentially includes the expansion of data localization mandate to include five (5) broadly defined categories of data: civil registration, immigration, health, financial and ‘other’ data as determined by relevant ministries or institutions. The ‘other’ category is intentionally vaguely defined to allow for practically unlimited scope of data that must be stored in Indonesia. Data localization requirements limit the ability of international service providers to serve Indonesian customers with features and services that may not be available locally, as well as potentially restrict Indonesian enterprises from providing their services to global customers. Expanding data localization requirements will also result in significant expenses that could otherwise be allocated to research and development to benefit Indonesian enterprises. Meanwhile, given the advances of technology and the cross-border nature of cyber threats, such restrictive policy may not necessarily improve the security posture and sovereignty of data that the government wishes to achieve.

Compounding the uncertainty, the Government enacted GR 33/2026 on July 16, 2026, implementing the Personal Data Protection (PDP) Law, with enforcement from January 16, 2027. While its substantive requirements are broadly comparable to international frameworks such as the EU’s GDPR, GR 33/2026 does not recognize international certifications, foreign standard contractual clauses (SCCs), or binding corporate rules approved in other jurisdictions — requiring instead Indonesian-specific instruments that do not yet exist. Every viable cross-border transfer mechanism is gated on the PDP Authority, which has not been established, creating a regulatory vacuum in which U.S. providers face enforcement risk but lack the legal tools to lawfully transfer data out of Indonesia. This compounds existing localization pressures under GR71 and sectoral financial data rules.

The 2020 Law is now implemented via Government Regulation No. 33 of 2026 (“PP 33/2026”), effective January 16, 2027, which requires appointment of a data protection officer, completion of data protection impact assessments, strict breach- and data-subject-request response windows, and documented safeguards for cross-border data transfers, with fines of up to 2 percent of relevant business-variable revenue for non-compliance.

Data Localization (Financial Services): Bank Indonesia (BI) continues to require payment transactions to be processed domestically under its payment system regulations, including PBI No. 10/2025 and its predecessors. Meanwhile, the Financial Services Authority (OJK) has gradually allowed certain financial services entities, such as insurance companies and non-bank financial institutions with specific asset thresholds, to use offshore electronic systems and data centers. Commercial banks may also use offshore electronic systems and data centers for non-core workloads, such as for risk and internal management purposes, but core banking workloads must still be stored and processed in Indonesia unless approved by OJK.

One Data Indonesia Bill: Indonesia’s draft One Data Indonesia Bill (RUU Satu Data Indonesia or “RUU SDI”) establishes a national data governance framework requiring government ministries and agencies to share interoperable data on shared infrastructure. Several provisions pose significant market access barriers. The bill requires parliamentary approval for all cross-border data transfers — a requirement with no global equivalent and incompatible with real-time cloud operations. It prohibits inputting strategic data into AI systems “not under Indonesian legal sovereignty,” an undefined term that effectively creates a national-origin restriction on AI capabilities regardless of security posture. The bill also includes discriminatory provisions including mandates for prioritization of domestic technology in security standards, and imposes data sovereignty audits without defined scope or methodology. Collectively, these

provisions risk isolating Indonesia from global AI development and establishing origin-based barriers that diverge from technology-neutral approaches adopted by ASEAN peers.

Access to Electronic Data and Systems: On top of data localization, the planned revision of GR 71 may also allow government and law enforcement greater access to electronic data and systems. This may lead to excessive government power in demanding data and system disclosure without due process. In practice, digital platforms and service providers have experienced challenges with addressing government data requests, as many are made without clear objectives and legal basis and with arbitrarily short timelines. GR71 revision may expand this authority even further, while unclear scope and mechanism of “access to electronic systems” will also increase cybersecurity risks and undue exposure of trade secret and proprietary information.

News Media-Related Digital Service Taxes: In February 2024, the government signed a Presidential Regulation directing specific digital platforms to pay news organizations for news content that appears on those platforms. This regulation, while seemingly neutral, primarily targets U.S. companies – the goal of extracting revenues from such companies and subsidizing local news outlets is evident from the explicit goal of the regulation, which states that digital services companies have a “responsibility” to support news organizations. The regulation mandates collaboration (paid licenses, profit sharing, data sharing) and empowers the Implementing Committee (the KTP2JB), comprising mostly media company members, to implement rules and oversee arbitration, creating a conflict of interest. The Regulation also allows for directing platforms to design algorithms supporting quality journalism, though it lacks clear mandates for disclosing algorithmic changes or user data to publishers.

Broadcasting Bill Proposal: In September 2026, parliament approved a revision of the Broadcasting Bill that would expand the broadcasting regulatory framework to cover OTT services (including user-generated content and SVOD services). The draft from parliament introduces an extremely high 25% local content quota for OTT platforms, restrictions on “deviant” portrayals focused on LGBTQ themes, a local registration requirement, increased AI oversight, and broad oversight and access requirements on platform content for “law enforcement and national security.” A local content quota for streamers and a burdensome mandatory registration rule would be inconsistent with the U.S.-Indonesia Agreement on Reciprocal Trade (ART), signed on February 19, 2026. New requirements on AI oversight and government oversight and access may also raise concerns under the U.S.-Indonesia ART. Following parliamentary approval, the bill will be submitted to the government for input and deliberation.

Content Moderation: Indonesia is advancing a series of content moderation regulations that create significant uncertainty and operational risks for the digital ecosystem. Regulations such as GR No. 5/2020 and the Child Protection/PP Tunas regulation impose unworkable compliance demands on digital platforms. The regulations impose extremely short content removal deadlines (4-24 hours), use vague definitions of prohibited content, and require government access to systems and data without a robust legal process. Non-compliance carries severe penalties, including substantial fines and the blocking of access to services. Further, new regulations are on the horizon, including a leaked broadcasting bill and a planned revision to the Police Law that could grant authorities expansive powers to censor content and restrict internet access. Overall, Indonesia is creating a regulatory environment that trends backward for freedom of expression and predictable business operations. Government Regulation 43/2023 introduces additional financial penalties of up to US\$30,000 per non-compliant URL.

Child Safety Regulation (PP Tunas): Government Regulation No. 17/2025 (“PP Tunas”) establishes a broad online child-safety framework, with implementing Regulation No. 9 of 2026 (effective March 6, 2026) requiring digital service providers to assess and report risk profiles for products, services, and

features that are designed for, or may be used or accessed by, children. The framework divides minors into five age bands and assesses services across contact with unknown persons, harmful content, commercial exploitation, data protection, addiction, and psychological and physiological harms; a high-risk finding in any one category results in an overall high-risk classification for the entire service, and children ages 13–15 may maintain accounts only on services classified as low-risk and with parental consent. The framework's broad scope, granular age-assurance requirements, and subjective, discretionary risk criteria create substantial compliance uncertainty, particularly for general-purpose platforms not designed specifically for children.

Certification Requirements for Public procurement: Through various regulations, the government has been requiring service providers to possess Indonesian National Standard (SNI) certificates as part of the public procurement process, while not acknowledging the international equivalence (ISO). Most recently, the Ministry of Communications and Digital Decree No. 519/2024 requires public cloud providers to possess local certificates to pre-qualify to be part of the National Data Center Ecosystem. The standards listed are SNI ISO 9001, SNI ISO/IEC 27001, SNI ISO/IEC 27017, and SNI ISO/IEC 27018 – without accepting the international ISO equivalent. The requirements are designed to be more easily met by local providers, including requiring a local entity and local presence, as well as local content, presenting an uneven playing field for international providers. Furthermore, some requirements are listed without further implementing guidelines, resulting in local certifiers incapable of issuing such certificates. The recent draft of cybersecurity law also suggests potential additional local standards and certifications for cybersecurity services and infrastructure providers. These requirements add to compliance costs and prevent international cloud providers from serving potential customers, especially in the public sector.

Cybersecurity Bill: Indonesia's proposed Cybersecurity Bill raises significant concerns for cloud service providers and data center operators due to its expansive scope and overlapping regulatory authority. The draft legislation creates regulatory uncertainty by distributing cybersecurity governance and incident response authority across multiple agencies — Komdigi, BSSN (National Cyber and Crypto Agency), Police, and Military - without clear delineation of roles and responsibilities. This fragmented oversight structure could create significant operational complications for cloud and data center providers, particularly during security incidents where multiple agencies may issue conflicting directives.

The bill contains several provisions that could substantially impact data center operations, including new security requirements, certification processes, and compliance monitoring systems. Of particular concern is the potential expansion of government access requirements and unclear incident reporting mechanisms, which could conflict with global security standards and best practices. The legislation's current form suggests a move toward increased data localization and more stringent compliance requirements that could create unnecessary operational barriers for international service providers.

These requirements, combined with the overlapping regulatory authority, could lead to increased compliance costs, operational disruptions, and implementation challenges for U.S. cloud service providers and data center operators. The lack of clear authority delineation between agencies not only creates regulatory uncertainty but also raises concerns about the ability to maintain consistent security standards and operational efficiency. The bill's current structure appears to deviate from international best practices for cybersecurity governance and could create unnecessary market access barriers that may impact the quality and availability of cloud services in Indonesia.

Ex-Ante Competition Regulation: Indonesia's competition authority is actively promoting the introduction of a "digital markets law" to strengthen regulation of digital platforms, while a parallel movement in parliament supports adapting DMA-style concepts into existing competition law. The

Ministry of Digital is also exploring ex-ante obligations in existing regulations governing electronic systems and transactions.

Copyright Law Revision: The government is revising Law No. 28 of 2014 on copyright, introducing AI provisions for the first time. The draft defines "fair use" for AI training as limited to non-commercial purposes only — inconsistent with established international approaches and discriminatory against U.S. AI developers who train models commercially, and without having text and data mining (TDM) exemption mechanisms. This would effectively prevent Indonesia from hosting AI training workloads, discourage investment in data center and cloud infrastructure, and position Indonesia as an outlier that penalizes the foreign companies most active in AI development.

MOCDA blocking Global Companies. Indonesia's Ministry of Communication and Digital Affairs (MOCDA or Komdigi) has notified 36 global companies (including US-based companies) to register as electronic system operators (ESOs) with Komdigi. Several companies have had to block access to users due to a lack of ESO registration. Though some companies have been able to restore access to users following consultations with the Indonesian government, some may be required to establish a local entity in Indonesia. Further, Indonesia also announced that a 0.5% income tax on e-commerce transactions would take effect in February 2026, then postponed to August 2026 — is now scheduled to take effect November 1, 2026, with major platforms designated as tax collectors.

Services Barriers - Telecommunications

Submarine (Telecom) Cable Connectivity: Various measures create significant barriers for international operators to deploy and operate submarine cables in and around Indonesia. These include: Ministry of Fisheries and Marine Affairs Decree No. 14/2021, which limits all submarine cables in Indonesian waters to a limited number of prescribed routes and landing points that different ministries have different interpretations of; requirements for submarine cable operators to obtain overlapping licenses from multiple ministries; and requirements by the Ministry of Communication and Digital Affairs for international submarine cable operators to have minimum 5% ownership by local partners who must meet unreasonably stringent qualification criteria.

Other non-market policies and practices

Local Content Requirements: Local content requirements (LCR) are a growing concern for global industries, including the pharmaceutical industry. Recent developments include the issuance of Minister of Industry Regulation No. 35/2025, which introduces potential flexibility in local content calculations for global companies by formally recognizing "brainware" contributions. However, the certification process for product-based local content remains challenging, particularly for fully imported goods. Moreover, the regulation's mandate prioritizing products with local content may disadvantage those with minimal or no local input—regardless of their quality or performance. Articles 327 and 328 of the Omnibus Health Law (Law No. 17/2023) explicitly dictate that the government and healthcare facilities – both public and private – must prioritize the procurement and utilization of domestically produced and sourced pharmaceuticals and medical devices, imported products will only be used if there are availability or supply issues. This further escalates the aggressive import substitution policy pursued in recent years, which has centered around the imposition of local content requirements as well as the "freezing" of imported products from the public procurement catalog should local alternatives be available. Separately, Presidential Instruction No. 6/2016 mandates local content requirement calculation to be used as a criterion for government procurement of biopharmaceutical and medical device products. Finally, this trend was further bolstered by Presidential Decree 2/2022, which prioritizes government procurement of

products with domestically produced raw materials, specifically those with a local content threshold of at least 25 percent. It is critical that these requirements are not applied in a manner that restricts patient access to innovative medicines in Indonesia and that greater recognition is given to biopharmaceutical innovators for their contribution in bringing innovative therapies to Indonesia.

Local Content Certification Requirements: Indonesia maintains several local content policies applicable to ICT equipment and is contemplating a range of other limitations. For example, the “Neraca Komoditas” (commodity balance) policy is intended to force domestic production by using trade imbalances as a rationale for quotas or outright bans. ICT and electronic devices could potentially be included in the scope of the policy. In addition, in September 2020, the Indonesian Ministry of Industry released Regulation No.22/2020 (IR22) on the Calculation of Local Content Requirements (“LCR”) for Electronics and Telematics, with a government target to achieve 35% import substitution by 2022. Although it is unclear whether the government has achieved this target, the recent ban on imports of ICT goods suggests that this policy will continue to place an additional administrative burden on the production of physical ICT products that are indispensable for ICT companies to operate in Indonesia. Such onerous requirements cannot be met without vendors establishing a manufacturing presence in Indonesia.

These local content policies are unfair, because they discriminate against American companies in favor of local Indonesian companies, without any consideration of quality or security. In particular, electronic public sector bids require participating vendors to pre obtain a certificate demonstrating the vendor’s qualification in meeting local content requirements, including having manufacturing facilities in Indonesia.

There is also a plan to revise the Ministry of Trade Regulation 08/2024 regarding the third Amendment to the Minister of Trade Regulation 36/2023 regarding Import Policies and Provisions. While the regulation aims to address container backlog at the port, the new revisions are likely to re-introduce additional hurdles to the import process and more restrictive technical consideration (Pertimbangan Teknis/Pertek), Import Approval (Perizinan Import/PI) and quota. These actions, aimed at protecting domestic markets, represent major non-tariff barriers for all products entering Indonesia. The regulatory changes would be graduated, with an initial focus on clothing goods and other commodities, including electronics, potentially at a later stage.

The ICT and electronics industry actively advocated for a higher allocation of non-physical product factors, such as R&D and training, in Indonesia’s LCR calculation. While the Indonesian government has shown some receptiveness to these proposals, it remains unclear whether such inputs had been incorporated in the inter-ministerial discussions on the LCR regulation revision. The Indonesian government is currently considering a more streamlined and integrated method for calculating LCR. However, the LCR computations heavily rely on the cost of materials, labor and factory overhead, and the proposed revisions would still require the industry to invest and build manufacturing facilities in Indonesia.

Price Controls: Indonesia is moving in the direction of increased state control over drug and medical device prices under the pretext of ensuring equitable and affordable health access for patients, while in fact it could threaten patient access to innovative treatments. The Omnibus Health Law, which was issued in August 2023, gives the government authority to regulate and control the price of drugs and medical devices in the context of securing their accessibility for public health and making necessary interventions. It is yet unclear how controls will be implemented. The government is also developing an online “pharmaceutical and medical device dictionary” where the public can get access to information about the

products, including their price. With this kind of price transparency policy, the government expects that hospitals and pharmacies will feel discouraged to set high drug prices so that people can buy drugs at affordable prices. In addition, listing decisions on the National Formulary (FORNAS) appear to be primarily based on price, whether the medicine and vaccine is locally produced, and the overall National Health Insurance (JKN) budget. It is important for policymakers to start looking at value-based pricing to ensure that innovation is being valued properly.

Israel

Services Barriers

Investment Obligations: Under the draft bill released by the Israeli Ministry of Communications in 2022-23, international streaming services and domestic content providers classified as “medium” or “large” (e.g., those with annual revenues over NIS 300 million) would be required to invest in local productions at rates of 2 % of annual revenue for medium players and 4 % for large players. If enacted, proposed streaming content obligations would have imposed new financial and operational burdens on U.S. streaming platforms. Due to U.S. government advocacy, the Broadcasting Law was passed in the Knesset in July 2025 with a complete exemption from local content obligations for international SVOD services, including U.S. companies. However, on 25 September, the Attorney General asked the Supreme Court to freeze the Broadcasting Law in full while legal challenges are considered, citing procedural flaws, weakened safeguards for news independence, and concerns over implementation during an election period. The Court had already temporarily suspended provisions due to take effect immediately in July; the latest request seeks to extend the freeze to the law as a whole while the challenges are considered. The issue warrants continued close monitoring.

Japan

Import Policies

Express Delivery: U.S. operators remain concerned by unequal conditions of competition between Japan Post Co., Ltd. (Japan Post) and international express delivery suppliers. Private U.S. express carriers are required to declare all shipments for customs clearance and calculate duties and consumption taxes based on cost. Different procedures called a duty assessment system apply to Japan Post including their competitive product of Express Mail Service (EMS). NFTC urges USTR to insist Japan to establish equivalent conditions of competition between Japan Post and international express delivery suppliers in terms of customs procedures and requirements.

The customs issues came from the privatization process of Japan Post back to 2007. When the privatization was determined, the Ministry of Finance, in response to industry’s strong push for equivalent conditions of competition, enacted a bill to revise customs clearance procedures for international postal mail. The bill requires Japan Post to adopt a duty declaration system for international postal import and export items with a value of more than JPY200,000. The threshold is very high and the imported items with a value of more than JPY200,000 in 2007 constituted only 0.06%. Thus, industry has been requesting GOJ to lower the threshold over the years, which GOJ explained to the industry as their plan in 2007. They still maintain the threshold and the issue remains heavily as a non-tariff barrier in Japan.

Security Clearance Requirements for Private Sector: Japan formulated security clearance

requirements for private companies to handle confidential-level government information. The current rules require companies to have dedicated physical space, security measures such as fence and locks, storage containers with keys, and stand-alone computing system with no internet connection. Such requirements favor on-prem solutions and discriminate against the use of cloud services/solutions (e.g. access controls) to handle sensitive government workloads (e.g. in public sector procurement opportunities). A risk-based and technology neutral approach to security clearance would be a fair alternative.

Excessive Information required under Economic Security Scheme: Japan has introduced the Economic Security Scheme to ensure the protection of critical infrastructure. This regulation requires suppliers to submit an excessive amount of detailed, proprietary information for the government to evaluate made-in-China products. The United States and other similar economies do not require such information.

Technical Barriers to Trade

Repeated Price Cuts to Patented Medicines: Japan devalues new innovative medicines through draconian rules that set low prices for patented medicines at launch and then exacerbates this problem by aggressively cutting prices throughout the patent period. Following National Health Insurance price listing, Japan applies a growing number of re-pricing rules in a highly unpredictable and arbitrary manner that significantly erode prices and expected revenues of patented medicines. Overall, about half of patented medicines launched in Japan are subjected to annual price cuts.

Biased Health Technology Assessments: For new innovative medicines awarded a price premium at launch for demonstrating clinical superiority over a comparator, Japan conducts biased “cost-effectiveness” evaluations using low and outdated monetary thresholds per life year gained to cut these price premiums by up to 90%.

Government Procurement

Information System Security Management and Assessment Program: Japan’s Information Security Management and Assessment Program (“ISMAP”) is a security certification scheme that applies to government procurement of cloud services. ISMAP has historically imposed significant compliance burdens and costs to service providers. Japan then expanded ISMAP to cover all key infrastructure, including telecommunications.

Most cloud and telecommunication service providers already have internationally accredited certifications (e.g., ISMS-JISQ/ISO 27000 series, SOC2), but ISMAP requirements go above and beyond these certifications without providing any additional security. They create additional costs not imposed by U.S. authorities procuring similar services.

Intellectual Property Protection

Patent Term Restoration (PTR): Japan’s PTR laws as currently interpreted by the Japanese Patent Office (JPO) often result in extensions for subsequent marketing approvals which are shorter in term than the extensions for the original approval and can thus act as a disincentive to conduct research on additional medical uses and indications, including new formulations for an approved product.

Patent Enforcement: Actions by the MHLW to approve generic versions of an innovative product, including during ongoing litigation, raises concerns for industry as to Japan's commitment to effectively enforce patents. While injunctive relief is typically available in Japan, such relief can take at least several months to secure, thereby frustrating the ability of the innovator to seek an injunction before potentially infringing products are allowed to enter the market. MHLW is considering reforms to Japan's early patent dispute resolution practice.

Services Barriers

Digital Platform Regulation: The Act on Improving Transparency and Fairness of Digital Platforms (the Digital Platform Act) imposes additional obligations on large companies designated by METI as "specified digital platform providers" for specific services, including "general online shopping malls selling goods," "application stores," "media-integrated digital ad platforms," and "ad intermediary digital platforms." The "specified digital platform providers" designated by METI have disproportionately captured U.S. firms compared to their Japanese and third country competitors and therefore undermine U.S. competitiveness in Japan by increasing the compliance costs on certain U.S. firms while not placing a similar burden on their competitors.

Japan's co-regulatory framework also raises concerns that recurring government evaluations, information requests, and ongoing dialogue with designated platforms may create de facto expectations for disclosures or changes to business practices beyond clearly established statutory requirements. Japan should ensure that these regulatory expectations remain necessary, proportionate, and firmly grounded in law.

In a similar way, in 2024, Japan adopted the Mobile Software Competition Act, modeled after the European DMA, targeting major mobile OS, app stores, browsers, and search engines of a certain size. In March 2025, the JFTC designated only two U.S. companies under this law, excluding domestic competitors based on their monthly active user calculation methods. As the law's subordinate guidelines are reviewed for final approval, there remains a risk that if not adjusted the guidelines will include overly prescriptive rules (with draft guidelines exceeding 100 pages) and lack the incorporation of crucial concepts like "user convenience" despite a Diet resolution emphasizing its importance, placing significant compliance costs and prohibitions on certain U.S. firms without placing a similar burden on their Japanese or third country competitors.

In a similar way, in 2024, Japan adopted the Smartphone Software Competition Promotion Act, modeled after the European DMA, targeting major mobile OS, app stores, browsers, and search engines of a certain size. In March 2025, the JFTC designated only two U.S. companies under this law, excluding domestic competitors based on their monthly active user calculation methods. There is a significant risk this measure will place significant and discriminatory compliance costs on the affected U.S. firms.

De Minimis Threshold for Consumption Tax on Imported Goods: Effective April 1, 2025, Japan introduced a platform taxation regime under which certain designated digital platform operators are responsible for collecting and remitting consumption tax on specified B2C digital services supplied by foreign businesses to consumers in Japan. Platform operators may be designated as "Specified Platform Businesses" when the value of qualifying transactions handled through their platforms exceeds JPY 5 billion. In addition, starting in April 2028, Japan intends to expand marketplace-based consumption taxation to certain low-value imported goods. While ensuring a level playing field among platforms is important, implementation should provide clear and predictable rules and sufficient lead time for necessary system changes. Separately, Japan is considering reform of the customs duty exemption for low-value imports. Eliminating the customs de minimis threshold would impose disproportionate

administrative and customs costs on low-value cross-border trade, particularly affecting U.S. SMEs and individual exporters. Japan should preserve an appropriate de minimis threshold and avoid creating unnecessary barriers to legitimate low-value trade. Furthermore, as Japan refines its digital platform taxation framework, it is important to further promote the digitalization of administrative procedures to ensure the system's effectiveness. Fully digitizing tax and customs-related procedures and additionally making them accessible in English will help reduce compliance costs for U.S. companies.

Economic Security Promotion Act: Subsidies for the provision of Cloud services/GPUs under the Economic Security Promotion Act has distorted the level playing field for US cloud service providers in Japan. Japan service providers benefiting from subsidies have an unfair advantage, winning government procurement contracts with bids that are significantly lower than comparable market prices. The Economic Security Management Guidelines (Version 1, January 2026) present three principles—autonomy, indispensability, and governance—and recommend reducing excessive dependence on specific countries, regions, or suppliers. Notably, neither the ESPA itself nor official government statements explicitly restrict or exclude foreign companies. However, the practical effect of the subsidy and procurement framework creates an invisible barrier: subsidies are channeled almost exclusively to domestic firms, government cloud procurement prioritizes domestic providers, and LDP policy documents (AI White Paper 2.0, Digital Japan 2026, Cybersecurity Strategy HQ recommendations) consistently favor domestic solutions. This "domestic preference by design" operates as a de facto non-tariff barrier without any overt discriminatory language in the legislation, making it particularly difficult to challenge through conventional trade mechanisms.

Barriers for Cloud Adoption in National Security and Defense: The government's information security guidelines restrict the use of public cloud by requiring a stand-alone system, on-site inspection, and installation of physical facilities for restricted and classified information in national security and defense area. Such requirements favor on-prem solutions and limit use of cloud services, hindering interoperability with allies including US in national security, cyber, and defense areas. While the Ministry of Defense announced its plan to adopt "hybrid cloud" approach for its next-generation of telecommunication infrastructure by FY2029, cloud adoption would still be limited and most of the critical workloads would remain at on-premise system without amending the security guidelines. The LDP's June 8, 2026 recommendation advocates "trusted digital infrastructure" including domestic foundation models and high-security sovereign cloud/data infrastructure, potentially creating new barriers for foreign cloud providers.

Subsidies / Duty Evasion

GPU purchase subsidy for frontier AI: The government plans to support the development of frontier AI models by providing a subsidy to select local businesses for their GPU purchase. The government budget for this project is expected to be billions USD. Such an arrangement favors on-premises solutions and excludes cloud service providers from supporting the project. Massive GPUs purchased by local entities could entail the risk of transshipment of computing resources to third countries, including adversaries.

Jordan

Services Barriers

Electronic Payment Systems: The Central Bank of Jordan's CBJ 2019 Circular No. 3/10/6474 aims to empower banks to make risk-based decisions under AML/CFT rules. However, its misinterpretation has delayed key global updates and innovations, harming Jordan's financial sector. An amendment to the

circular is needed to exclude global payment network updates and technological advancements, ensuring seamless, secure connections to global payment systems.

CBJ is considering establishing a national domestic switch to route all local transactions. The proposal could integrate issuers and acquirers into the national switch while limiting international payment networks to XB transactions. The United States should urge to adopt an open processing model that preserves sovereignty and competition, allowing international schemes to process domestic transactions alongside any local switch.

Customs Clearance Procedures for Express Shipments: Following the launch of the E-Commerce and Express Transport Customs Center by the Jordan Customs Department and Telecommunications Regulatory Commission in August 2024, customs clearance for express shipments has been centralized through the Jordan Post facility in Amman. Express operators that do not maintain airport-based clearance facilities are required to process shipments through the centralized clearance model rather than through airport-based processing. Although the new model provides 24/7 clearance availability, including weekends and public holidays, it increases processing and operational costs for affected operators, raising the overall cost of providing express transportation services in Jordan.

Kenya

Import Policies

Documentation Requirements: Effective 1 September 2026, the Finance Act 2026 introduced Section 23B of the Tax Procedures Act, requiring importers to obtain, retain, and provide export declarations or equivalent customs export documentation issued by the country of export. Importers must retain these records for at least five years and produce them upon request by the Kenya Revenue Authority (KRA). The additional documentation requirements increase compliance costs and administrative burdens and have raised industry concerns regarding customs clearance processes, particularly where export documentation is unavailable, difficult to obtain, or differs across exporting jurisdictions. Failure to provide the required documentation may also expose importers to customs valuation and tax assessment risks.

Import Declaration Fee (IDF) and Railway Development Levy (RDL): Kenya continues to impose the Import Declaration Fee (IDF) and Railway Development Levy (RDL) under the Miscellaneous Fees and Levies Act, administered by the Kenya Revenue Authority (KRA). Originally introduced as part of Kenya's import levy framework and subsequently amended through various Finance Acts and the Miscellaneous Fees and Levies (Amendment) Act, 2026, these charges apply in addition to customs duties and VAT. The measures continue to increase the landed cost of imported goods.

Services Barriers

Data Localization: Kenya's 2019 Data Protection Act allows personal data to leave the country when safeguards are in place, but some workloads are required to remain in-country. Specifically, data linked to the state's strategic interests, including civil registration, elections, public finance, protected systems, basic education and primary or secondary healthcare, must be processed in Kenya or have a copy in a Kenyan data center. 'Critical Information Infrastructure' operators must also store critical information in Kenya unless offshore hosting is approved. Cloud providers must therefore offer suitable local hosting solutions. In parallel, Kenya is also finalizing a National Data Governance Policy that could extend the

Data Protection Act beyond personal data to commercial and machine-generated data. The final version of the Policy will determine its effect on cross-border flows.

Cloud Policy: Kenya's 2025 National Cloud Policy requires sensitive categories of data to be hosted locally through local accredited providers or government cloud. While framed as a measure to strengthen national infrastructure, the preference for local storage and local providers risks excluding or disadvantaging foreign suppliers, creating discriminatory barriers to market access that conflict with Kenya's trade commitments and undermine the competitiveness of U.S. cloud and digital service providers.

Cloud Accreditation for Public Procurement: The Government's 2025 Cloud Policy classifies government workloads by sensitivity. 'Top Secret' data must remain on dedicated government infrastructure in Kenya, 'Restricted' data requires an accredited provider with a local presence, and 'Open' data may be hosted abroad by an accredited provider. Public bodies must comply, and suppliers seeking government contracts are expected to follow the Policy. Accreditation is therefore essential, while workloads above 'Open' require a local presence.

Digital Services Tax: Kenya's 3% 'Significant Economic Presence' tax applies to qualifying income earned by non-resident digital service providers. It taxes a deemed profit of 10% of gross turnover at 30% and is paid monthly. Since July 2025, it has covered internet-based services, including cloud computing.

Withholding Tax and VAT introduced on Card Transactions: The Finance Act 2026 introduced withholding tax on interchange and merchant service fees, both fees having been classified as "management or professional fees,". In addition, withholding tax was introduced on payment-network fees after they were classified as royalties in the tax law. VAT exemption was also removed for certain payment-processing services. Industry's concern is that these are operational payment and settlement flows, not professional services or intellectual-property royalties, and taxing gross flows may exceed the actual economic margin. The combined corporate income tax, WHT and VAT burden could increase merchant and consumer costs, create cash-flow and compliance challenges, discourage card acceptance and infrastructure investment, and slow digital-payment adoption, particularly among Micro and Small Enterprises (MSMEs). It may also weaken Kenya's competitiveness in tourism, cross-border commerce and foreign investment. Industry recommends excluding interchange and merchant service fees from tax law definition of "management or professional fees," removing payment-network participation and transaction-based fees from the royalty definition, and restoring the VAT exemption for payment processing and related platform services.

Content Moderation: Industry remains concerned about overbroad content moderation in Kenya, risking the stifling of innovation and free speech. In June-July 2024, the Kenyan government severely restricted internet access during protests, causing a 40% connectivity drop and costing the economy approximately US\$6.3 million daily, despite prior commitments against such actions. On September 18, 2024, the Computer Misuse and Cybercrime Bill was introduced to the National Assembly, which would grant the National Computer and Cybercrimes Coordination Committee authority to block websites and apps for promoting "illegal activities" and "extreme religious and cultic practices". The Bill is still under consideration, but, due to vague definitions in the Bill, there is a significant risk of abuse were the Bill to pass. More recently, in June, 2025, amid nationwide protests marking the anniversary of the previous year's controversial Finance Bill, the Communications Authority of Kenya (CA) ordered TV and radio stations to stop live broadcasts of demonstrations. Several major stations were taken off air for non-compliance.

Services Barriers / Tax and Regulatory Compliance

Electronic Tax Invoice Management System (eTIMS) Requirements: The Kenya Revenue Authority (KRA)'s eTIMS framework continues to impose significant compliance obligations on businesses operating in Kenya. While the underlying requirements were introduced through the Tax Procedures (Electronic Tax Invoice) Regulations, 2024 (Legal Notice No. 64 of 2024), enforcement has continued to expand and businesses continue to incur system integration, implementation, reporting, and ongoing compliance costs. The regulations require businesses to use compliant electronic invoicing systems and transmit invoice data to tax authorities.

Korea

Import Policies

Customs: Onerous new requirements starting from January 2026, Korean Customs Service will require enhanced data elements, like purchase order details, order numbers and website addresses. Specifically, declarations must now include product website URLs and detailed purchase order information (such as item descriptions, unit prices, and proof of payment). Recipient names, phone numbers and postal codes must strictly match their Personal Customs Clearance Code (PCCC) profile. Yet, standard shipping documents (such as air waybills, commercial invoices) do not capture these new fields. This will require costly booking system and API updates that could take years and may be prohibitively expensive without adding safety. Further, carriers cannot access foreign merchant databases to verify customer-provided URLs (which may change dynamically for minor reasons, and which don't indicate fraud), and carriers can't verify order numbers which are exclusively sent to purchases. This creates immediate and ample compliance risks. In sum, government guidelines are unclear on who is responsible for providing and for validating each of these new data fields.

Cross-Border E-Commerce Business Registration Requirement: The Korea Customs Service (KCS) has launched a dedicated clearance platform for cross-border e-commerce. It requires overseas marketplaces, purchasing agents and international forwarders to register for an e-commerce business ID, which is now a mandatory field on import declarations and manifests. Shipments from unregistered businesses, or without customer and transaction data sent to KCS through a direct system connection, lose access to simplified low-value clearance. Those shipments must be formally declared and face more inspections. This shifts registration and data burdens onto U.S. sellers and carriers, which especially hurts small businesses that can't build Korea-specific system connections. NHTC recommends that USTR urge Korea to (1) provide a reasonable transition period, (2) accept carrier-submitted data instead of requiring direct seller connections, and (3) keep simplified clearance for low-risk U.S. shipments, consistent with KORUS customs commitments.

Technical Barriers to Trade

Market Access (Pharmaceuticals): Korea sets prices of new innovative medicines through a combination of referencing the lowest price among OECD countries and using low and outdated monetary thresholds per life year gained from clinically proven treatments. Two government agencies, the Health Insurance Review and Assessment (HIRA) service and the National Health Insurance Service (NHIS), force companies through a gauntlet of assessments to access the market, resulting in lengthy patient access delays following marketing authorization from the Ministry of Food and Drug Safety (MFDS). The monetary threshold per life year gained from clinically proven treatments was set equal to Korea's GDP per capita in 2007 but has not been updated even though Korea's GDP per capita has since

more than doubled.

Government Procurement

Cloud Security Requirements — National Security Framework (N2SF): Korea requires cloud service providers to obtain cloud security certifications to access its public sector cloud market. Previously under a regulatory framework called the Cloud Security Assurance Program (CSAP), this regime has effectively blocked U.S. cloud service providers from entering the public sector market for the past decade. In April 2026, Korea replaced CSAP with a new regime called National Network Security Framework (N2SF), which will be overseen entirely by the National Intelligence Service (NIS). N2SF will remain in a three-tier system based on the importance of government operations. While the new framework adjusted certain requirements to be more aligned with international standards, including for hardware certification, local encryption modules, and network separation, it continues to mandate physical separation of servers and storage between public and private sector use in the Sensitive and Classified tiers. This requirement alone prevents U.S. CSPs from qualifying for an estimated 90-95% of public sector workloads. NIS's cloud security guidelines under N2SF are expected to be released in H2 2026, followed by a one-year grace period before the new verification regime takes effect in H2 2027. The Sensitive tier should be updated to accept logical separation as an alternative to physical separation, consistent with the accepted standard across major government cloud frameworks globally.

Government Procurement Requirements in AI: In February 2025, the Ministry of Science and ICT (MSIT) of the Republic of Korea announced a comprehensive National AI Initiative with the strategic objective of positioning the nation among the world's top three AI leaders. This initiative encompasses critical projects, including the development of a world-class Large Language Model (LLM) and the establishment of the National AI Computing Center. However, the subsequent Request for Proposal (RFP) issued by MSIT in May 2025 incorporated a restrictive "domestic companies only" clause, effectively excluding U.S.-based CSPs from accessing a potential market valued at KRW 1.5 trillion (USD 1.1 billion).

This development has raised significant concerns among U.S. stakeholders, as several U.S. CSPs had already made substantial investments in infrastructure preparation based on preliminary discussions with MSIT. The unexpected implementation of exclusionary criteria without prior consultation not only compromises the principles of transparent government procurement but could also set a precedent for similar restrictive practices in other government AI initiatives and technology sectors. In the interest of maintaining fair competition and fostering international cooperation, it is recommended that the "domestic companies only" requirement be removed from the RFP, thereby enabling U.S. CSPs to participate in an open and equitable procurement process.

Intellectual Property Protection

Patent Term Extension (PTE) System: In December 2024, the Korean National Assembly passed the Patent Act Amendment Bill, which revises the patent term extension (PTE) system to limit the number of patents eligible for PTE based on a single drug approval, as well as setting a maximum cap on patent term including PTE (previously no cap, now the maximum cap of 14 years from the product approval date). The current PTE system also lacks due process in the PTE procedures and imposes a high-stakes, all-or-nothing approach to appeals. If the Patent Office determines a certain duration of PTE that is less than the full amount originally requested by the patentee and the patentee challenges that determination and subsequently loses the challenge, no PTE is granted; even the duration previously determined by the Patent Office is lost. This all-or-nothing approach significantly undermines a patentee's right to appeal,

effectively deterring appeals of erroneous calculations, and undermines the patentee's rights.

Services Barriers

Cross-Border E-Commerce Customs and Data Requirements

Korea has introduced the Electronic Commerce Customs Clearance System for Shipment (ECCS), requiring foreign e-commerce operators to register to use simplified customs clearance procedures. Registered operators may also submit transaction data in connection with certain benefits, but the scope and practical implications remain unclear. Korea should provide clear guidance and avoid disproportionate reporting or technical requirements.

Network Usage Fees: Korea's sender party network pays (SPNP) framework creates the conditions for content providers to bear the costs associated with delivering data over networks ("network fees"). Korea's 2016 Interconnection Standards Notification established under the Telecommunications Business Act, imposed the rule. The rule established a "Tier 1" group of Internet Service Providers (ISPs) and required them to pay each other interconnection fees based on the amount of data traffic between them. This created a right for the ISPs to formally charge others when they are a net receiver of traffic. The Tier-1 ISPs then pass on the traffic-based fees to other ISPs and to content providers, generally in the form of domestic transit and peering fees much higher than in any other comparable market. This second category of fees functions like network usage fees.

Essentially, the SPNP rule eliminated price competition among Korea's three dominant ISPs and allows them to charge U.S. cloud service and content providers the second highest internet network fees in the world following China. Because U.S. providers must reach Korean users through these ISPs, the rule functions as a government-created charge on U.S. digital exports to Korea rather than a market outcome.

The burden falls directly on U.S. companies and grows as data volumes rise in the AI era, producing a continuous outflow of payments from U.S. providers to Korean ISPs that widens the U.S. trade deficit with Korea in digital services. This barrier is inconsistent with the commitment in the Joint Fact Sheet (November 2025) from the Trump-Lee summit that U.S. companies not face barriers "including network usage fees," and with KORUS FTA principles on digital trade. The United States urges Korea to eliminate the SPNP rule in its Interconnection Standards Notification, adopt settlement-free interconnection as used in the United States, Europe, and the rest of Asia, and refrain from enacting retail-level network usage fee mandates.

Discriminatory Platform Legislation and Regulations: Several pending or proposed platform regulatory initiatives - notably the Online Platform Monopoly Act (PMA), the Platform Fairness Act (OPFA), and Food Delivery Platform Act) - threaten to disproportionately impact U.S. technology and service providers at a disadvantage vis-à-vis domestic incumbents and Chinese competitors. The OPFA was drafted to capture only large U.S. companies. The legislation projects neutrality by lowering revenue thresholds found in the original PMA. In reality, the OPFA is focused on sectors where U.S. companies are market leaders, thereby maintaining its discriminatory intent. Globally unprecedented, the OPFA pairs rigid behavioral mandates and severe sanction regimes with expansive administrative leeway for the KFTC.

The KFTC and its allies in the National Assembly are similarly advancing the Food Delivery Platform Act, which would impose unprecedented government-imposed price controls and ability to oversee contract terms—an approach that runs directly contrary to free market principles. Like the PMA, which

received significant pushback, the leading versions of this proposed legislation would reinstate ex-ante thresholds engineered to capture U.S. market leaders, while explicitly shielding domestic competitors. It also gives the KFTC broad enforcement discretion and includes fines of up to 10% of sales based on vague standards, while adding the explicit threat of criminal penalties.

Apart from platform regulation, Korea has also adopted or proposed: discriminatory limitations on U.S. maps providers and geospatial data export prohibitions; discriminatory cybersecurity certifications and mandated network segregation; requirements that effectively lock out U.S. cloud service suppliers from Korea's public procurement and limit cloud usage in the financial service sector; data localization mandates, including for reinsurers; and EU-inspired AI Act that would put significant restrictions and obligations on American AI models and services.

Fair Trade Commission (KFTC) - Amendments to Korea's E-Commerce Act: On July 14, 2026, Korea approved revisions to its E-Commerce Act, effective 21 July 2026 (domestic agent provisions follow 21 January 2027). The changes require foreign e-commerce operators to designate a domestic representative if they meet any one of three thresholds: KRW 1 trillion (~\$750M) annual revenue, 1 million+ average monthly Korean users, or KFTC designation for potential consumer harm. Because only one threshold must be met, a U.S. company with minimal Korea revenue could be caught on global revenue alone. The KFTC is expected to consult on operational guidelines.

Restrictions on Mobile Application Marketplaces: In August 2021, Korea enacted legislation compelling mobile app marketplaces to permit in-app purchases via third-party payment systems, directly prohibiting app stores from requiring exclusive use of their own payment system, and specifically targeting U.S. companies. The Korea Communications Commission (KCC) approved implementing rules on March 8, 2022, and initiated investigations into Google, Apple, and SK Group's OneStore on August 16, 2022, for potential violations concerning in-app payments. The KCC specifically warned Google and Apple against imposing discriminatory conditions or inconvenient usage processes for third-party payments. In October 2023, the KCC proposed fines of KRW 68 billion (approximately \$52 million) against two U.S. companies for alleged breaches, a decision both firms are currently still contesting. The lack of clear implementation procedures and stakeholder input has created uncertainty for businesses and risks harming Korea's burgeoning developer ecosystem. Further, the discriminatory nature in which the rules are being applied, particularly the ban on specific payment mechanisms solely for app stores, poses fundamental questions of fairness, and raises concerns about potential conflicts with Korea's trade commitments under the KORUS and Article XVII of the WTO General Agreement on Trade in Services (GATS), which prohibit discriminatory treatment against foreign service suppliers.

In May 2026, Korea lawmakers introduced Bill No. 2219036, an amendment to the Telecommunications Business Act that would require mobile operating system providers to grant technical access necessary for interoperability with device hardware and software functions and would prohibit unjustified refusal or restriction of such access. The bill remains pending and would leave significant implementation details to subordinate regulation, meaning its technical, security, privacy, and commercial effects will depend substantially on rules yet to be written. The lack of clarity on how mandated access would be implemented, and on whether affected providers could recoup associated development and maintenance costs, creates uncertainty for businesses and risks disproportionately burdening U.S. mobile OS providers relative to domestic competitors.

Targeted enforcement:

The KFTC continues to utilize protectionist competition policy in ways that disadvantage U.S.

companies, and has doubled down on its aggressive enforcement measures from public threats of criminal prosecution to unannounced site visits, and intrusive investigations for standard commercial practices.¹¹ The KFTC recently revived its "Key Investigation Planning Unit" specifically to focus on large-scale cases, a bureau-level task force designed to intensify regulatory pressure on foreign digital service providers.

Korea continues to ignore legitimate concerns from senior U.S. officials about the KFTC's heavy-handed and targeted enforcement toward certain American companies. KFTC's leadership has had the opportunity to reverse course; unfortunately, it has instead doubled down on its discriminatory treatment of U.S. companies, which has led to frictions in the bilateral relationship.

This pattern extends itself when looking at the KFTC's use of fines. Two recent studies have shown that American firms' share of KFTC fines is disproportionate to their presence in the Korean economy. Looking at ten years of KFTC enforcement data, they found that the KFTC penalizes U.S. companies at rates four to seven times higher than those applied to Korean companies relative to their business activity in the country. Although the KFTC has argued that it "determines the level of fines ... based on related sales," the KFTC is the agency that determines what counts as "related sales," allowing it to calculate fines based on firms' sales in other markets, not just their Korean sales, which represents an unfair practice.

The Korean aggressive regulatory approach is very different than the experience Korean companies experience in the United States, where they are able to invest and compete under transparent, consistent rules that are applied across the board. When issues do arise, there are structured pathways and clear avenues for redress.

U.S. companies investing in Korea should be able to receive this same treatment based on consistent rules applied equally, and meaningful due process protections.

Cloud Services: The Cloud Security Assurance Program (CSAP) was established by the Ministry of Science and ICT (MSIT) in 2016 and elevated from administrative guidance to a legal requirement through a March 2022 revision to the Cloud Computing Promotion Act. The CSAP, which applies to Korea's central, provincial, and local public sector with very limited exceptions, creates significant barriers to foreign cloud service providers (CSPs) seeking to sell to Korea's public sector. CSPs are required to comply with data localization of cloud systems, backup systems and data, and ensure that operations and management personnel of CSPs are located within the territory of Korea. CSPs must also use only National Intelligence Service (NIS) certified domestic encryption algorithms (ARIA, SEED, LEA or HIGHT), and information security systems and network equipment deployed for cloud service provision must use products verified for stability by NIS, such as those with Common Criteria (CC) certification or security function verification. Moreover, to obtain the CSAP Moderate tier certification, CSPs must build physically segregated facilities for exclusive use by public sector customers. These requirements differ significantly from internationally accepted standards and create significant barriers to U.S. CSPs seeking to sell to Korea's public sector. As of 2025, the CSAP certification remains valid through March 27, 2030, and continues to be administered by KISA under MSIT supervision. U.S. CSPs remain effectively excluded from nearly all of Korea's public sector market, as they are unlikely to qualify for the Moderate and High tier certifications that represent the majority of government procurement opportunities. Only those CSPs that have at least the Moderate CSAP certification can effectively

¹¹ <https://judiciary.house.gov/media/press-releases/new-report-exposes-south-koreas-discriminatory-attacks-american-owned>

participate in the government's digital transformation initiative. The United States has urged Korea to align its cloud security certification requirements with other internationally accepted standards.

Audiovisual Services: Notwithstanding KORUS commitments to not impose new restrictions on audiovisual services, multiple Korean Government agencies and the National Assembly have been discussing ways to incorporate online media streaming platforms into the existing restrictive regulatory framework for legacy media, including potential Korean content requirements and National Broadcasting Fund contributions for U.S. over-the-top platforms. USTR should continue to urge Korea to ensure that its laws and regulations are consistent with its KORUS commitments concerning audiovisual services and with the commitments in the U.S.-Korea Joint Fact Sheet of November 2025.

New PIPC Personal Data Guidelines for Foreign Companies. The Personal Information Protection Commission of Korea (PIPC) published explanatory guidelines in July to help foreign companies comply with the Korean personal data protection law. When a foreign company processes data of Korean citizens or carries out personal data processing on Korean territory, it is subject to Korean legislation. The guidelines specify the main legal provisions in force, as well as some decisions taken by the PIPC or by local courts to clarify the applicable legislation for companies. This is a complex and challenging task for both domestic and multinational corporations in Korea, as there is presently no industry benchmark.

Content Moderation: Korea's *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.* (Network Act) regulates how information and communications networks are used and policed. A new Article 44-7(5), added in January 2024, creates new content moderation burdens for providers that operate domestic servers of a certain type or scale. These providers must implement measures to identify and restrict access to unlawful information, subject to review by the Korea Communications Standards Commission. They are also required to request uploaders to halt further distribution, record and store logs of enforcement actions, and adopt additional preventive measures as mandated. For cross-border service suppliers, this provision creates significant concerns by potentially pressuring foreign companies to maintain local servers in Korea, acting as a de facto data localization requirement. It also expands liability by obligating providers to monitor, restrict, and document user content in ways that may conflict with global business models and international trade commitments.

Furthermore, the Korea Communications Commission (KCC) is reportedly working on additional amendments to the Network Act aimed at introducing new digital content censorship. These measures would require large online platforms, primarily those based in the U.S., to censor vaguely defined "False Manipulated Information" under threat of government investigations and substantial fines. Modeled after the European Union's Digital Services Act (DSA), these proposed measures are expected to replicate the DSA's risks, including discriminatory burdens on U.S. firms and vague, onerous content regulation that may target lawful political speech. The KCC would have the power to investigate platforms' censorship systems and impose administrative fines of up to 4% of domestic sales for non-compliance, creating an incentive for platforms to over-censor and remove vast amounts of content to avoid penalties. The proposed measures also include a local agent requirement for "Large-scale" platforms without a domestic business establishment, which could violate Korea's market access obligations under the Korea-U.S. Free Trade Agreement. This pattern of discriminatory digital policies and aggressive enforcement actions against U.S. firms is troubling.

Overall, these content moderation measures are part of a troubling pattern of discriminatory digital policies in Korea, similar to other platform regulations identified above, as well as a track record of aggressive enforcement action against U.S. firms. By importing the DSA model through, Korea would be

imposing similar unwarranted economic burdens on U.S. service providers, and embracing a regulatory philosophy fundamentally at odds with shared U.S.-Korea democratic values and free speech.

Artificial Intelligence: Korea's AI Basic Act, effective January 1, 2026, broadly regulates AI business entities, including developers and deployers, without clear distinctions in obligations or liability. This creates significant uncertainty for large, often U.S.-based, AI developers who could be held liable for uncontrolled downstream uses. Concerns for cross-border service suppliers include: unsupported compute-based thresholds for "high-impact" AI, potentially targeting U.S. firms and conflicting with trade commitments; mandated public disclosures and labelling of AI outputs, risking commercially sensitive information; the requirement for foreign providers to designate a domestic agent, which could act as a disguised local presence mandate; and low thresholds for intrusive fact-finding investigations. Unless clarified, these provisions could hinder market access, impose disproportionate compliance costs, and raise trade law concerns for international AI suppliers.

Kuwait

Services Barriers

Electronic Payment Services: The Central Bank of Kuwait (CBK) is currently developing its domestic payment scheme, with potential implications for international card schemes (ICS). While no formal guidance has been issued regarding adoption or implementation, past experiences in other markets suggest that central banks may opt for models that disintermediate ICS from domestic transactions. Such approaches can create a non-level playing field and put U.S. providers on an unlevel playing field.

Malaysia

Import Policies

Refurbished Products: Malaysia requires importers to obtain a certificate of approval issued by the Standard and Industrial Research Institute of Malaysia ("SIRIM") to import communications equipment. However, SIRIM does not undertake testing of refurbished products as import of refurbished equipment is prohibited in Malaysia. This ban on refurbished products limits U.S. suppliers' ability to support customers in Malaysia. For products still in production, new components must be sourced to support customers. For products that are no longer in production, such products cannot be supported or replaced with available refurbished parts, meaning that U.S. suppliers are forced to stop customer support or the customer is forced to upgrade to a newer version of the product.

Additionally, SIRIM requires Internet Protocol Version 6 ("IPv6") certification at the level of "IPv6 Ready Logo" for all products imported into Malaysia. While the "IPv6 Ready Logo" is a voluntary certification led by the IPv6 Forum, the certification is mandated in Malaysia. This requirement is unfair because, in the United States, this requirement only applies to government procurement. Malaysia's unique practice of specifically requiring MalaysiaIPv6 compliance for market entry is excessively burdensome and out-of-step with other countries' practices.

Charges: USD 1/RM5 charge on per shipment basis for export import in Kuala Lumpur and Penang. Collected by the airport operator Malaysia Airport Holding Berhad. The fee collected was meant to be reinvested for infrastructure development and security of the complex. After more than two decades of contribution we have seen minimum improvement.

Local Ownership: The Malaysian Ministry of Finance requires companies wanting to operate public bonded warehouses to at least have 30% ethnic Malaysian ownership and board structure. This contradicts with Malaysia Investment and Development Agency's incentives of 100% ownership through the Integrated International Logistics Status (IILS).

Government Procurement

National Sovereign AI Cloud: In 2026, the Malaysian Communications and Multimedia Commission (MCMC) issued a tender for the National Sovereign AI Cloud (NSAIC), part of Malaysia's AI Nation 2030 agenda. The tender excludes solutions subject to the U.S. CLOUD Act, which in practice disqualifies U.S. cloud service providers because of their nationality and not their security capabilities. The technical specifications also favor a single vendor's proprietary technology instead of open, outcome-based standards. Malaysia should remove nationality-based exclusions, use technology-neutral specifications and give U.S. suppliers a fair chance to compete in public sector AI and cloud procurements.

Services Barriers

E-Commerce Bill: Malaysia's Ministry of Domestic Trade and Cost of Living is expected to table a dedicated E-Commerce Bill in late 2026 or early 2027, which would sit alongside the country's existing Communications and Multimedia Act reforms as a further platform-specific regulatory framework.

Cybercrimes Bill 2026: Passed by both houses of Parliament (Dewan Rakyat, July 1, 2026; Dewan Negara, July 20, 2026) and awaiting Royal Assent and gazettment, this law repeals and replaces the Computer Crimes Act 1997. It expands cross-border law-enforcement cooperation, classifies a broader range of cyber offenses as extraditable, and introduces new offenses targeting the use of technologies including AI in fraud and digital crime. It is distinct from the separate Cyber Security Act 2024, which governs critical infrastructure.

Personal Data Protection Amendment Act (In Force): The PDPA Amendment Act 2024, phased into force between January and June 2025, introduced a mandatory data protection officer (threshold-based), breach-notification and data-portability requirements, and a "substantially similar protection" test for international data transfers, which shifts the burden onto the platform to audit and demonstrate that a recipient country's data protection standards are equivalent to Malaysia's, rather than relying on a pre-approved transfer mechanism. Penalties reach RM1,000,000 and/or three years' imprisonment.

AI Sovereignty: In recent developments, Malaysia's National AI Office (NAIO) has outlined a Sovereign AI Strategy, introducing a tiered approach to AI governance with implications for international technology providers. The strategy establishes strict requirements for compute infrastructure, data residency, and operational flows, particularly for highly sensitive government workloads. Of note, NAIO is proposing the implementation of government-owned cloud/compute capabilities for top-tier (L3) workloads and introduces new sovereignty certification requirements, even when engaging with global companies. While NAIO maintains an "ecosystem-supportive" stance open to both foreign and local providers, the strategy raises concerns about potential market access barriers and preferential treatment for domestic companies. The introduction of mandatory requirements for handling sensitive government data, coupled with new certification and auditability standards, could result in increased operational complexity and compliance costs for US companies operating in Malaysia. This evolving regulatory landscape warrants close monitoring, as it may establish precedents that significantly impact the ability of international technology firms to operate effectively in the Malaysian market.

Social Media Licensing: In 2024, the Malaysian government established a Social Media Licensing (SML) regime on social media and internet messaging platforms, imposing local registration requirements and criminal liability for local employees, as well as financial penalties. With no US company having registered to date, the government has given itself powers to “deem” US companies as licensees to place them under the regime. The government is prone to censoring political speech and content on royalty, race and religion and has arrested political opponents as well as members of the public for offences related to online speech. The SML regime gives it greater powers to censor online speech and heighten the chilling effect on US companies.

Law Enforcement Access Powers: Recent [amendments](#) to the Communications and Multimedia Act, passed with minimal consultation, grant law enforcement enhanced powers for data access and interception, which create significant operational and compliance risks for global service providers. The new provisions empower law enforcement authorities to compel the warrantless disclosure of broadly defined “communications data”, potentially placing U.S. companies in a position of legal conflict – compliance with this mandate to avoid penalties up to RM1 million (approx. US\$236,000) and/or up to five years in prison could necessitate a breach of strict U.S. legal requirements that limit such disclosures. The amendments also empower law enforcement officers to enter any premises without a warrant to install interception devices which would be a red-line critical security risk for U.S. service providers, as it jeopardizes the integrity and security of communications networks; interference with this entry carries potential severe penalties of RM1 million (approx. US\$236,000) and/or up to 10 years imprisonment. Given these concerns, the U.S. government should insist that Malaysia use the U.S.-Malaysia Mutual Legal Assistance Treaty (MLAT) as the sole and standard legal mechanism for requesting data from U.S.-based service providers, and concurrently seek the repeal of the intrusive power that permits warrantless entry for interception as it poses a direct threat to service integrity and security.

Other non-market policies and practices

Local Content Requirements: Local content requirements being proposed by both State and Federal authorities in Malaysia. Malaysia is moving toward imposing a Local Content Requirement (LCR), with Selangor sets to apply 30% LCR for hardware as a condition for business licenses. Federal agencies such as MITI and MDEC are advancing parallel measures, including possible reductions in import duty incentives to spur local supply chains. The government is also linking electricity tariff rebates to local purchases. Selangor’s move is expected to set a precedent for other states, and the initiative is being framed as a national strategy to strengthen Malaysian semiconductor firms’ access to domestic and global markets, modeled after localization policies in India and Indonesia.

Mexico

Import Policies

Shipments Valued Under 2,500: On December 30, 2024, Mexico’s Tax Administration Service (SAT) published amendments to the regulations governing the clearance of express shipments, which took effect on January 1, 2025 (less than 48 hours later). This created operational havoc, widespread confusion, etc. The new regulations included a host of additional information requirements, including some that Mexico has since relaxed. Furthermore, the regulations now disqualify from express clearance procedures any shipments due ADCVD duties. Without an exemption for USMCA partners, shipments valued between US\$50 and US\$2,500 will likely incur higher duties than the current flat rates of 17-19%. This change not only increases operational burden but also introduces new risks related to misclassification and heightened regulatory scrutiny. Overall, these changes are yet another example of Mexico’s failure to

provide sufficient prior notification of changes to the trading public. On substance, these changes continue to degrade the simplified clearance channeled set out in USMCA article 7.8.2.

Shipments Valued \$2,500 and Over: In a 2025 regulatory change, Mexico modified its regulations to disqualify all shipments valued at \$2,500 and above from the simplified express clearance process. However, the USMCA requires in article 7.8.1 that Mexico maintain such a process regardless of value.

Cargo Security: The high levels of cargo theft is a critical security and safety concern spanning every NFTC member that trades in the region. The security environment in Mexico is being prioritized in bilateral discussions, but cargo security needs special attention as the risks extend far beyond the border, translating into significant costs, supply chain disruptions, and investment risks for Mexico. These costs and disruptions affect both U.S. exports and imports, and where imports are inputs destined for further processing can lead to manufacturing disruptions. In addition to Mexico's commitments on border security that are being prioritized in bilateral negotiations, NFTC urges USTR to obtain commitments from Mexico of additional resources and actionable security measures to prioritize cargo safety and theft. This cooperation could be a pillar under the recently launched U.S.-Mexico Security Implementation Group, where, as appropriate, the United States can offer technical assistance, intelligence sharing and resources to support cargo safety and security.

Customs Barriers and Trade Facilitation: Mexico continues to provide insufficient prior notification of procedural changes. Regulatory amendments to trade rules are frequently introduced without opportunities for public comment, undermining transparency and predictability for U.S. exporters.

Recent amendments to the General Rules on Foreign Trade (*Reglas Generales de Comercio Exterior*) and the General Rules and Criteria on Foreign Trade (*Criterios de Carácter General en Materia de Comercio Exterior*) were published with immediate application, without allowing for a comment period, disrupting trade operations for U.S. exporters. Each year, a new version of the General Rules on Foreign Trade is issued in the last days of December to enter into force on January 1 of the following year, leaving businesses with virtually no time to adapt to new requirements.

The newly established Council responsible for examining and processing courier licensing applications has increased delays for new approvals. The process remains slow and unpredictable, creating additional disruptions to operations. Furthermore, certain goods are still not permitted to be imported through all ports of entry. Restricting goods to designated ports has made it difficult for U.S. exporters to arrange efficient transportation and increases logistics costs.

Customs facilitation: In establishing the Agencia Nacional de Aduanas de Mexico (ANAM) as an independent customs agency separate from its tax authority, Servicio de Administracion Tributaria (SAT), industry and freight operators are experiencing significant clearance delays at the U.S.-Mexico border. Since 2022, career customs officials have been replaced with military personnel who are not experts in trade facilitation, and created a fragmented border clearance with responsibilities diffused between the Army at land ports, the Navy at seaports, and the Air Force and private actors at airports. As a result, to this day the Import/Export community is experiencing significant pain points in cargo movements, and technical and regulatory challenges in the coordination between SAT and ANAM. To cite a specific example, an existing and valid regulation, *Regla General de Comercio Exterior 3.7.27*, could allow shipments cleared for export by up to three different customs brokers to be consolidated into a single vehicle at the Nuevo Laredo–Laredo land border crossing. Such consolidation could improve transit times, help alleviate the hours-long queues at the crossing, reduce carbon emissions, lower operating costs, and provide other benefits. However, the regulation remains unimplemented, allegedly because of a

technical limitation that prevents the DODA customs document from including references to more than one customs broker. Other sources indicate that international bridge authorities are concerned that implementing the rule could reduce the revenue generated from bridge-crossing fees.

Furthermore, Mexico has thus far failed to implement a reasonable, effectual method to comply with the periodic assessment and collection of import duties and taxes on express shipments provision set forth in Article 7.8.1.(f) of the USMCA, raising concerns regarding compliance with this Agreement's obligations.

Tax ID registration affecting US SMEs: In 2020, Mexico enacted legislation requiring U.S. businesses that store inventory in Mexico to obtain a local tax identification number from the Tax Administration Service (SAT) and to file monthly tax reports. While registration requirements are not themselves unusual, the process to obtain this tax ID, known as a Registro Federal de Contribuyentes (RFC), is so complex, slow, and costly that it has become the primary barrier for U.S. small and medium-sized enterprises seeking to reach Mexican consumers. To obtain an RFC, a U.S. business must maintain a local Mexican address and appoint a local legal representative who assumes joint liability for 50% of the company's tax obligations, and it must pay income tax on all income generated in Mexico. Registration cannot be completed online. It requires apostilling the company's documentation in the United States, having it translated into Spanish by a certified translator, legalizing it before a Mexican notary, securing an in-person SAT appointment that can take one to four months to obtain because of limited availability, and finally registering the RFC at a SAT office. Completing these entirely offline steps can take more than five months and cost over US\$5,000, on top of the ongoing cost of meeting income-tax obligations. The requirement for a locally liable legal representative is a particular deterrent, as it exposes an individual in Mexico to half of a foreign company's tax liability, and few qualified representatives are willing to accept that risk. Mexico should streamline RFC registration for foreign SMEs by allowing remote or electronic enrollment, accepting foreign-issued documentation without apostille and notarization, and removing the joint-liability requirement for local representatives.

2026 Customs Law Reform and Express Operator Liability: Mexico's reform of its Customs Law took effect on January 1, 2026. It makes importers and customs agents jointly liable, requires a detailed electronic file for every operation, and requires verification that foreign suppliers legally exist and can physically supply the goods. Fines for missing non-tariff requirements rose from 70–100% to 250–300% of the goods' value. Express operators clearing high volumes of low-value shipments can't run supplier checks or file-level documentation on every parcel. These requirements raise the risk of fines and seizures that are out of proportion to the risk the shipments pose. NFTC recommends that USTR press Mexico to (1) create simplified, risk-based procedures for express shipments, (2) allow minor clerical errors to be fixed without penalty, and (3) make sure express-specific requirements don't exceed those on postal shipments, consistent with USMCA Article 7.11.

Technical Barriers to Trade

Adhering to National Treatment in MA Procedures (Pharmaceuticals): Proposed amendments to Mexico's marketing authorization procedures appear to undermine its national treatment obligations under the USMCA. Under the draft legislation, companies holding a sanitary license for a domestic manufacturing facility producing generic or biological medicines would be granted access to an expedited marketing authorization process. By limiting this streamlined pathway exclusively to manufacturers that meet these criteria, the proposal introduces a discriminatory measure that undermines the principle of national treatment enshrined in the USMCA; specifically, Annex 12-F.5, which governs the application of regulatory controls. The legislation was published in the Gaceta Parlamentaria on September 26, 2025.

USTR should urge the Mexican government to ensure marketing authorizations, recognition letters, and regulatory controls are administered equitably and without discrimination based on origin, in line with national treatment obligations.

Delays in Regulatory Approval & Market Access (Pharmaceuticals): Under Mexican law, products approved by the FDA, should receive an expedited review by COFEPRIS within 90 days. COFEPRIS has been inconsistent in its use of this review pathway, resulting in long approval delays that prevent market access. These delays are inconsistent with Mexican law and USMCA (Annex 12-F).

Government Procurement

Proposed Offset Requirements: In addition to numerous changes to government procurement rules for medicines in recent years, the Mexican government issued a decree in June 2025 linking public sector pharmaceutical purchases to domestic production and/or investment. The proposal was also included in the draft revision to the General Health Law published in the Gaceta Parlamentaria on September 26, 2025. This policy, commonly referred to as an offset or performance requirement, also introduced a points-and-percentages system for evaluating bids in public tenders. This is inconsistent with several of its international trade obligations related to procurement.

Mexico Localization and Procurement Policies

Mexico has adopted a series of measures requiring domestic pharmaceutical manufacturing and investment in order to be competitive in government procurement. President Sheinbaum's June 2025 procurement decree, subsequent reforms to the General Health Law, and implementing rules issued in February 2026 provide preferential treatment to companies that manufacture, invest, conduct R&D, or establish facilities in Mexico. These measures include awarding additional procurement evaluation points to firms with a local presence, conditioning participation in certain procurement processes on investment commitments in Mexico, and providing expedited regulatory treatment for activities tied to domestic production. Together, these policies condition market access on US pharmaceutical companies to localize operations in Mexico in order to compete for government contracts.

These localization measures appear inconsistent with Mexico's obligations under the WTO and USMCA. The policies raise concerns under GATT Articles III:4 and XI:1 by according less favorable treatment to imported products and effectively restricting access to Mexico's public procurement market based on local investment and production criteria. Under the USMCA Government Procurement Chapter, the measures appear to violate national treatment and non-discrimination obligations (Article 13.4), the prohibition on offsets that require local investment or domestic content as a condition of procurement (Article 13.4(6)), and restrictions on participation conditions unrelated to a supplier's technical or commercial capability (Article 13.7). By conditioning procurement advantages and market access on local manufacturing, investment, or R&D activities, these policies disadvantage U.S. pharmaceutical, vaccine, and medical device manufacturers and create significant barriers to market access for U.S. exporters seeking to compete fairly in Mexico's healthcare market.

Telecommunications Procurement: Mexico made commitments related to government procurement to which it no longer adheres. Specifically, the Comisión Federal de Electricidad's ("CFE") Telecomunicaciones y Internet Para Todos program is not explicitly covered under CFE's listing. Although the Mexican Secretariat of Economy confirmed that the 'Telecomunicaciones y Internet Para Todos' program would be covered under Mexico's existing government procurement commitments, the Mexican government has not confirmed this commitment in writing to date. CFE's failure to list the

program violates its USMCA obligations, and CFE's discriminatory treatment of U.S. suppliers violates its USMCA commitments, especially notices of intended procurement (Article 13.6), qualification of suppliers, (Article 13.8), technical specifications (Article 13.11), time periods (Article 13.13), and compliance commitment (Article 13.2). Moreover, CFE issues procurement notices that are designed in such a way that the only products that qualify are from Chinese suppliers. This unfair practice discriminates against U.S. suppliers.

Government Procurement / Cybersecurity: The Government of Mexico is updating its cloud services framework agreement for public procurement, and there are indications that Mexico will be lowering the cybersecurity standards required to provide cloud services to the Mexican government and other public sector entities. The Secretariat of Finance is currently undergoing a market study that started at the end of September and will conclude by the end of November. It is anticipated that key international certifications such as ISO 27017, ISO 22301, SOC 1, 2, and 3, Cloud Security Alliance (CSA) STAR Level 2, FedRAMP, and FIPS 140-2 Level 3 or higher will no longer be required. This development means that leading Chinese cloud providers that previously did not meet the requirements will now be able to provide cloud services to some of Mexico's most critical public sector workloads.

Software Requirements: A new National Law to Eliminate Bureaucratic Procedures, published on July 16, 2025, creates a significant and immediate concern for the U.S. technology sector. While the law aims to digitize government services and laudably establishes a principle of "technological neutrality" in its Article 6, this principle is directly contradicted by the mandates in Article 93. This article inexplicably requires government entities to favor free and open-source software and to "limit the acquisition" of proprietary software solutions. Furthermore, it imposes a requirement that proprietary software vendors provide their source code as a condition of contracting, a practice that is fundamentally contrary to the nature of proprietary software and effectively precludes its consideration. This provision violates Mexico's obligations under Article 19.16 of the USMCA, which prohibits conditioning market access on the transfer of source. This discriminatory policy undermines fair competition, prevents the government from acquiring the best-suited technology, and introduces a significant conflict that must be addressed ahead of the 2026 USMCA review. Therefore, ITI urges the U.S. government to engage in a constructive dialogue with the Mexican government address this mandate.

Procurement Commitments: Mexico made commitments related to government procurement to which it no longer adheres. Although the Mexican Secretariat of Economy confirmed that the 'Telecomunicaciones y Internet Para Todos' program would be covered under Mexico's existing government procurement commitments, the Mexican government has not yet confirmed this commitment in writing to date. The Comisión Federal de Electricidad's (CFE) failure to list the program violates its USMCA obligations, and CFE's discriminatory treatment of U.S. suppliers violates its USMCA commitments, especially notices of intended procurement (Article 13.6), qualification of suppliers, (Article 13.8), technical specifications (Article 13.11), time periods (Article 13.13), and compliance commitment (Article 13.2). Moreover, CFE issues procurement notices that are designed in such a way that the only products that qualify are from Chinese suppliers.

Intellectual Property Protection

Lack of implementing regulations and patent linkage (Pharmaceuticals): The Mexican Institute of Industrial Property (IMPI) has not yet issued the necessary regulations to implement key provisions of the Federal Law for the Protection of Industrial Property (LFPI), such as patent linkage. Additionally, recent

court precedents have undermined patent usage by preventing their publication in the linkage gazette. All of these issues are in direct violation of Mexico's IP commitments under the USMCA. As a result, COFEPRIS has issued numerous marketing authorizations for generic versions of patented protected products, occurring at least 10 times in 2023 and 2024 alone ([PhRMA, 2025](#)). This harms innovation and allows generics in China to take market share away from U.S. companies operating in Mexico.

Lifting injunctions without sufficient legal justification: The Mexican government, including IMPI, has adopted the practice of lifting injunctions against products that infringe industrial property rights under the justification of access to medicines and the right to health. Although the protection of public health is a constitutional principle, this practice affects legal certainty and the protection of industrial property rights. The right to health cannot be interpreted absolutely when it affects constitutionally protected industrial property rights – fundamental rights must be harmonized and are not mutually exclusive. Preliminary injunctions should be maintained valid and should not be lifted unless compelling evidence of lack of access and/or non-infringing evidence is filed by the defendant.

Services Barriers

Mexico's "Kill-switch" and Article 30-B in the 2026 Economic Package: Mexico's 2026 Economic Package amended the Value-Added Tax Law (LIVA) to require digital service providers to grant the Tax Administration Service (SAT) permanent, real-time online access to their systems and records relating to their operations in Mexico. Non-compliance could result in the temporary blocking of digital – widely referred to as the "kill-switch" – as outlined under the LIVA. SAT is coordinating with the newly created National Agency for Digital Transformation and Telecommunications to manage the technological infrastructure and data analysis associated with this obligation. The real-time access was amended but continues to impose a significant and ongoing compliance burden on U.S. digital service providers, and the power to disable a service that entirely functions as a disproportionate enforcement mechanism that hangs over any provider operating in the country. Blocking a service outright is a severe measure that raises concerns about due process and proportionality, and it creates lasting legal uncertainty because the authority retains broad discretion to impose it. Mexico should narrow the real-time access mandate to what is demonstrably necessary for tax administration, provide clear procedural safeguards and replace service-blocking with proportionate, graduated enforcement measures.

Electronic Payment Services: In the U.S.-Mexico-Canada Agreement (USMCA)'s Chapter 17 (Annex 17-A), Mexico adopted new high-standard financial services commitments related to cross-border trade, including application of the national treatment and market access obligations for electronic payment services (EPS). Since the Agreement's entering into force, EPS suppliers faced barriers that prevented them from fully participating in Mexico's domestic payments market.

On August 27, 2026, the National Banking and Securities Commission (CNBV) and the Central Bank (Banxico), published the draft card payment networks and clearing houses regulations for public consultation until September 24.¹² Although the revised drafts published for consultation on August 27, 2026, represent progress, they still contain restrictions and complexity that could limit differentiation based on price, innovation, and security, while leaving uncertainty over roles, enforcement, and the hierarchy of applicable rules.

¹² Comisión Nacional Bancaria y de Valores (CNBV), "Consulta pública del proyecto de disposiciones de carácter general aplicables a redes de medios de disposición," August 27, 2026. Available at: [https://www.gob.mx/cnbv/prensa/consulta-publica-del-proyecto-de-disposiciones-de-caracter-general-aplicables-a-redes-de-medios-de-disposicion?](https://www.gob.mx/cnbv/prensa/consulta-publica-del-proyecto-de-disposiciones-de-caracter-general-aplicables-a-redes-de-medios-de-disposicion?__track=ais)

The final framework should designate the entity that owns and operates a card payment network as its network administrator, with responsibility for defining, updating, interpreting, and enforcing network rules and standards, ensuring clear accountability and effective governance subject to regulatory oversight. In addition, the obligation for clearinghouses to process transactions from all brands should be eliminated and the regulation should expressly recognize that they may operate in connection with a single card brand. Universal acceptance can be achieved by allowing acquirers to connect to multiple card networks, with each clearinghouse processing only the brands it supports, consistent with common practice in the United States, Canada, and most markets.

Mexican regulators should commit to closely overseeing the implementation of the regulation once it is adopted and to proactively resolving any differences in interpretation that may arise among market participants and payment networks. Clear and timely regulatory guidance will be essential to ensure consistent application of the framework and to avoid prolonged implementation timelines driven by disputes among stakeholders. Extended delays would unnecessarily preserve the status quo, postpone the realization of the regulation's intended benefits, and hinder the development of effective competition of U.S. EPS suppliers and broader payment choice for end users.

Mexico maintains an active agenda in the payment sector. Mexican Congress approved legislation introduced by President Claudia Sheinbaum on the Digital Economy Law for Digital and Electronic Payments. While it is an important step toward accelerating digital payment adoption in Mexico and reducing reliance on cash, Mexico must ensure that any public policy derived from this law uphold competitive neutrality across payment methods and between public and private providers so that the U.S. EPS suppliers can justify expanding the export of services they offer in Mexico.

Ensuring that Mexican policy does not entrench preferential treatment for its government endorsed domestic platform is critical to maintaining secure, interoperable, and competitive payment networks that benefit consumers and businesses alike. We urge the USTR to address these concerns proactively, safeguarding U.S. interests and promoting a balanced framework for electronic payments under the USMCA. Eliminating existing measures that favor domestic players and harm U.S. EPS suppliers will not be impactful if new, similar measures are later introduced in a different form.

Barriers for cloud in financial services: Mexico continues to enforce 2021 regulation which requires electronic payment fund institutions to maintain a business continuity plan in the case of disaster recovery that relies on either 1) a multi-cloud approach with at least two cloud service providers from two different jurisdictions, or 2) an on-premise data center in country that doesn't depend on the primary (foreign) cloud provider. The approvals process run by the National Banking and Securities Commission (CNBV) that is required for financial services companies to use cloud services is resource intensive and is discriminatory towards foreign cloud providers, whereas existing local on-premise data centers need to complete a shorter notification process. This de facto data localization requirement is in addition to an already complex and time-consuming process that electronic payment fund institutions face in order to gain regulatory approval to use offshore cloud infrastructure whereas in-country infrastructure enjoys a more expedited process. The United States has raised concerns with the Mexican government that the requirements relating to use of cloud service suppliers by electronic payment fund institutions have a negative competitive impact on the business of U.S. service suppliers.

Proposals targeting American companies and the digital economy – Price Transparency bill: On September 14, the Morena party introduced a bill targeting "drip pricing" on digital platforms—the practice of advertising a low initial price and then adding undisclosed charges (taxes, service fees, administrative costs, payment-processing, and marketplace commissions) during checkout. It would add

three provisions to Article 76 Bis: display of the total, final price from the first moment of the offer inclusive of all charges; a prohibition on raising an announced price through charges not disclosed visibly and in advance; and express identification of platform- or app-specific offers, discounts, and promotions, with the decree effective the day after publication in the DOF. These requirements represent a potential barrier to trade because they impose platform-specific disclosure and pricing-architecture obligations that diverge from general retail rules, forcing cross-border and digital commerce operators to re-engineer checkout flows, pricing displays, and promotional labeling for the Mexican market—raising compliance costs and operational friction that fall disproportionately on digital and foreign-origin sellers relative to traditional channels.

Intermediary Liability: Mexico made reforms to its Federal Copyright Law in 2020 in an attempt to bring its law in compliance with commitments under USMCA. However, the provisions implementing Article 20.87-88 of the USMCA Intellectual Property Rights Chapter inappropriately narrows the application of this framework for internet services. Likewise, the provision implemented through the amendment of Article 232 Quinquies fr. II of the Copyright Law establishes administrative offenses fines when ISPs fail to remove, take down, eliminate, or disable access to content upon obtaining a notice from the right holder; or do not provide to a judicial or administrative authority information that identifies the alleged offender.

Consumer Protection Norm NOM-184 Extended to Streaming Platforms: In 2026, Mexico's Federal Consumer Protection Agency (PROFECO) and the Secretariat of Economy initiated a process to extend NOM-184-SCFI-2018 to over-the-top (OTT) streaming services. PROFECO's concerns center on terms and conditions of compliance under the Federal Consumer Protection Law (LFPC). Applying telecom-oriented obligations to VoD services would be ill-fitting, potentially redundant with the recently reformed Article 76 bis of the LFPC, and could raise potential concerns under the USMCA and set a negative precedent for the company in Mexico. NOM-184 is a consumer-protection technical standard whose scope is limited to telecommunications services provided over a public telecommunications network, and it imposes carrier-oriented obligations such as registration of adhesion contracts and tariffs before the regulator, dedicated telephone customer service, itemized consumption-based billing, terminal-equipment warranties, and minimum service-interruption compensation. Streaming platforms fall outside that scope because they do not operate a public telecommunications network or provide a telecommunications service; they deliver content over the open Internet, so neither the underlying law nor the norm that implements it should reach them. PROFECO nonetheless seeks to bring them in by treating streaming as a form of restricted television and audio, a telecommunications category defined in the Federal Telecommunications and Broadcasting Law (LMTR), and applying NOM-184's obligations on that basis. This stretches a definition written for licensed pay-TV and audio services to reach internet content providers that are regulated differently, giving the extension a weak legal foundation, and because that definition covers both audio and video, it would pull music and audio services into scope even though the stated target is video-on-demand. The result is a non-tariff barrier that disproportionately burdens U.S. providers by subjecting them to a regime designed for network carriers. Mexico should confirm that NOM-184 does not apply to OTT streaming services.

Services Barriers - Telecommunications

6 GHz Spectrum Restrictions and Telecommunications Policy: In contrast to U.S. actions to expand 6 GHz spectrum, Mexico has engaged in unfair trade practices by restricting the 6 GHz band allocation and dissolving the telecommunications regulatory agency in violation of the Telecommunications Chapter of the USMCA. Mexico has also worked to undermine U.S. leadership in promoting 6 GHz and cutting-edge telecommunications technologies, including 5G and Wi-Fi.

Since 2020, the United States has allocated the 6 GHz band (5925-7125 MHz) for unlicensed use, which includes the use for technologies such as Wi-Fi and Bluetooth. By making the entire 6 GHz band available, the United States has enabled Wi-Fi to support new applications such as high-definition video, artificial and virtual reality, and haptic technologies. Most of the countries in the Western Hemisphere have adopted the same spectrum model as the United States, including Canada, Colombia, Argentina, and Peru. Mexico, however, has only allocated the lower portion of the band—5925-6425 MHz—for unlicensed use. Although it has held multiple proceedings examining the possible future use of the upper portion of the band, Mexico has deferred its consideration of the issue for the last two years. These delays have been exacerbated by the recent dissolution of Mexico’s telecommunications regulatory agency, the Federal Telecommunications Institute (“IFT”). Since its dissolution last year, Mexico’s telecommunications policymaking has been largely on hold, as these regulatory responsibilities were moved to the nascent Agency of Digital Transformation and Telecommunications. Mexico’s dissolution of the IFT is in direct violation of the USMCA that requires signatory countries to maintain an independent telecommunications regulatory agency.

More importantly, the prior and current Mexican administrations have sought to undermine U.S. positions on 6 GHz issues. For example, the use of the upper 6 GHz band in the Americas was not on the agenda at the World Radiocommunication Conference in late 2023 (“WRC-23”). Nevertheless, Mexico sought to initiate a regional study of the issue that would have undermined Wi-Fi operations in the band throughout the region, including the United States. Backed by a strong opposition from the Wi-Fi industry, the United States blocked Mexico’s proposal. Unfortunately, this did not stop Mexico from joining with Brazil to add a footnote to the final WRC-23 resolutions that allocated the upper part of the band for International Mobile Telecommunications (“IMT,” i.e., 5G) for their respective countries. Since then, Mexico has exploited the International Telecommunication Union (“ITU”) process to create further uncertainty about the future of Wi-Fi in the upper 6 GHz band in the Americas. For example, Mexico has sponsored an effort at the Inter-American Telecommunication Commission (“CITEL”) to gather Member Countries’ input about present and planned use of the upper 6 GHz band via wireless technologies, including 5G and Wi-Fi. Mexico’s intent behind this effort was to suggest that Wi-Fi is not the preferred technology for the band. With Brazil, Mexico has also sought to delay the CITEL action on resolutions providing technical guidance about how unlicensed technologies, like Wi-Fi, would operate in the upper 6 GHz band. This effort seems intended to delay progress on establishing Wi-Fi in the band and create uncertainty that would discourage other countries from following the U.S. lead on 6 GHz policy.

Withholding Tax Rates on Marketplace Sellers: Mexico’s 2026 Economic Package raised the income tax (ISR) and value-added tax (IVA) rates that digital marketplaces must withhold from the proceeds of sellers operating on their marketplaces, with the higher rates taking effect in January 2026. Digital marketplaces are required to act as withholding agents, deducting these amounts from each sale and remitting them to the Tax Administration Service (SAT) on the seller’s behalf. Because the withholding applies to gross transaction value rather than to a seller’s actual margin, the elevated rates fall disproportionately on small and medium-sized enterprises, whose thin margins mean the withheld amount can approach or exceed their real profit on a sale. This is driving sellers to abandon the formal digital marketplaces and shift toward informal channels where no withholding applies, so the marketplaces are losing sellers from their catalogs and seeing transaction volume erode as a direct result of the measure. The impact falls squarely on the U.S. digital marketplaces that must administer the elevated withholding while watching their seller base contract, undermining the very formalization objectives that Mexico’s own policy agenda promotes. Mexico should recalibrate the withholding rates so that they approximate sellers’ actual tax liability rather than a share of gross revenue, and should avoid rate levels that push sellers out of the formal economy and off the marketplaces that serve Mexican consumers.

Investment Barriers

Investment Climate: It is essential to provide certainty to investments through expedited authorization procedures, including approvals for acquisitions and mergers. The ongoing transition from the former Federal Economic Competition Commission (COFECE) to the National Antimonopoly Commission (CNA) may undermine confidence in the criteria that will be applied to cases currently under review. It could also delay their resolution. The new Competition Law shortened the timeframes for reviewing and resolving merger authorization requests, in part as a recognition by the legislature that lengthy procedures delay investment in the country. However, merger authorization requests filed prior to the reform will remain subject to the timelines set forth in the former legal framework. As of June 2025, COFECE reported having 31 mergers and acquisitions pending authorization.¹ This situation creates uncertainty for investors, potentially affecting decision-making and long-term planning.

State-owned Energy Operators: While the Mexican government started to liberalize the energy sector in 2013, Mexico implemented multiple amendments to the Law on the Electricity Industry and Hydrocarbons Law to increase the market share of state-owned energy companies (Petróleos Mexicanos (PEMEX) and the Federal Electricity Commission (CFE)), with the stated intent of promoting Mexican energy self-sufficiency. Reforms to date have presented serious hurdles for companies seeking to connect to the electricity grid and purchase clean and reliable energy. These hurdles include directing energy consumers to purchase energy from the state-owned utility (CFE) and receiving disproportionate transmission infrastructure requests as part of the process to connect to the grid with the National Center for Energy Control (CENACE). Many of the infrastructure requests are actual recognized obligations of the Mexican state that have simply not been met. Concurrently, the Mexican government has taken steps to prevent the private sector from effectively participating in the local energy market by revoking permits, delaying issuance of new licenses, and preventing companies from operating renewable energy facilities or off-grid generation.

As a result, U.S. companies are unable to adequately source their energy needs in Mexico and hence see their clean energy targets compromised. Additionally, several U.S. companies have stranded infrastructure due to the lack of energy availability and inability to generate energy. We understand the United States has raised concerns with Mexico in several instances, including through dispute settlement consultations under Article 31.4.5 of the USMCA. ITI urges the U.S. government to advocate for the removal of these barriers. These discriminatory policies are impacting U.S. companies' ability to reliably and adequately source energy on the local energy market, especially as U.S. companies are pursuing clean energy targets.

Other Barriers

Tax ID registration affecting US SMEs: In 2020, Mexico passed legislation requiring U.S. businesses that store inventory in Mexico to register for a local tax ID with the Tax Administration Service (SAT) and file monthly tax reports. While this process alone is not novel, the process to obtain this tax ID, known as a *Registro Federal de Contribuyentes* (RFC), is extremely complicated and costly. This process alone has become the primary barrier for U.S. small and medium-sized enterprises (SMEs) that seek to sell their products to Mexican consumers and businesses. To receive an RFC, U.S. businesses are required to have a local Mexican address and a local Mexican legal representative that shares 50% of the company's tax liability, as well as pay income tax on all income generated in Mexico. The registration process is slow and bureaucratic, and involves 1) apostilling of documentation in the U.S., 2) translating all documentation to Spanish by a certified translator, 3) legalizing documentation with a Mexican Notary, 4) obtaining a SAT appointment (which can take one to four months due to limited availability), and 5) registering the RFC in SAT's offices. All of these steps are offline and in-person and can take over five months, costing over \$5,000, in addition to the costs of complying with income tax obligations.

Tax Audits: The broader investment climate for established U.S. multinationals is deteriorating due to a systemic and punitive tax audit regime. Over the past few years, the SAT and related agencies have increasingly targeted U.S. multinational companies with extensive tax audits and assessments. While tax disputes are expected, U.S. companies have been assessed unreasonable tax charges, often based on new audits of previously closed tax filings. The targeting of U.S. MNCs suggests that some of these tax assessments are not based on Mexican accounting rules but are rather an attempt to secure additional corporate tax revenue. SAT's own data reveals a 367% increase in revenue collected from transfer pricing audits of large multinationals in the 2019-2024 period, suggesting audits are in fact used as a *de facto* revenue-extraction tool rather than for routine compliance. Unfortunately, the ability to resolve these tax assessments is difficult given an opaque and costly appeals process. This aggressive posture now also targets U.S. manufacturing supply chains, with SAT announcing its intent to audit 100% of companies in the VAT Certification program, a program essential for IMMEX operations. The targeting of U.S. companies in such a discriminatory and arbitrary manner raises the costs of doing business and undermines the stability pledged under the USMCA.

Barriers to access energy: Since 2025, Mexico concluded the approval process of its comprehensive energy reform with the publication of secondary laws, following the constitutional reforms approved in October 2024. This reform package returned control of the energy sector to the State, giving prevalence to state-owned companies Mexican Petroleum (PEMEX) and the Federal Electricity Commission (CFE), while establishing new schemes for private sector participation under state supervision. These new regulatory changes continue to create hurdles for companies seeking to connect to the electricity grid and purchase clean and reliable energy. These hurdles now include the establishment of CFE's dominance, requiring it to maintain at least 54% of grid-injected energy annually, and the implementation of "binding planning" requirements that give preference to state-owned CFE in generation and marketing activities. Transmission and distribution remain 100% reserved to the Mexican State, with zero private participation permitted, and any private investment in transmission infrastructure must ultimately be transferred to CFE. The creation of a new centralized regulatory body (CNE) replacing independent regulators potentially reduces transparency and regulatory independence. Additionally, the reform restricts self-supply arrangements, eliminates partial permit migrations, adds new requirements for electricity storage systems, and implements stricter controls on grid interconnection. Mexico already faces a structural energy supply gap: in 2024, gross electricity consumption (359,807 GWh) exceeded total generation (352,305 GWh), and achieving the growth targets of Plan México would require 10.1% more electricity demand than official planning contemplates through 2030, a gap current infrastructure cannot close. As a result, U.S. companies face significant challenges in adequately sourcing their energy needs in Mexico, compromising their clean energy targets and operational efficiency. In addition, power quality and reliability remain inconsistent, with frequent intermittencies forcing companies to maintain additional on-site backup power supply, primarily through diesel generators that must be activated far more frequently than their intended emergency-only purpose. This not only increases operational costs but also undermines the viability of sustained, large-scale operations that demand uninterrupted, high-grade electricity, placing U.S. investments at a structural disadvantage in Mexico's energy landscape. While the United States has already requested dispute settlement consultations with Mexico under the USMCA, the 2025 reforms appear to further entrench state control over the electricity sector, exacerbating existing concerns.

Constitutional reforms on independent regulatory bodies: In July 2025, Mexico published comprehensive reforms that fundamentally restructured key regulatory bodies. The reforms eliminated the autonomy of antitrust regulators, the Federal Economic Competition Commission (COFECE) and the Federal Telecommunications Institute (IFT). COFECE was replaced by the National Antimonopoly Commission, now a decentralized public agency under the Secretariat of Economy, while IFT's functions were transferred to the new Telecommunications Regulatory Commission (CRT) under executive branch

control. The reforms altered the regulatory telecommunications landscape by reducing commissioner numbers from seven to five, eliminating independent selection mechanisms, and transferring removal power from the Senate to the Executive. These changes, combined with the first judicial election in Mexico following the judicial reform approved in the previous administration, represent a fundamental shift toward centralized executive authority over key regulatory and judicial institutions. The election, held on June 1, involved selecting 881 federal positions and 1,800 state magistrates and judges through popular vote. Voter turnout was low (approximately 13%), and most winning candidates were publicly aligned with the ruling political coalition. The new judicial leadership took office on September 1, 2025. These reforms raise significant concerns about regulatory independence and institutional consistency, particularly regarding competition enforcement and telecommunications oversight.

Nepal

Services Barriers

Digital Services Taxes: Nepal passed legislation on May 29, 2022 to adopt a 2% DST on a special list of digital services provided by non-residents to consumers in Nepal. The DST took effect on July 17, 2022, without any public consultation on the law or the implementing procedures. The DST: (i) only applies to non-resident companies; (ii) is inconsistent with existing international tax principles; (iii) imposes an additional tax burden and potential double taxation on non-resident companies; and (iv) creates a disproportionate compliance burden as additional resources are required to comply with the DST's payment and reporting requirements.

Data Localization: In March 2024, the Ministry of Communication and Information Technology introduced the draft Information Technology and Cyber Security Bill 2080 to regulate activities related to information technology and cyber security. As written, the Bill would require data centers and cloud service providers to obtain licenses subject to yearly renewal and would require health and financial organizations to store all data domestically. The USTR should continue to track the development of this legislation and its discriminatory impact on foreign data centers and cloud service providers.

Local Switch & Possible Routing Mandate: In October 2025, Nepal Rastra Bank (NRB) published its National Payment Switch (NPS) and National Payment Ecosystem Master Reference Document, which proposes requiring domestic card transactions in Nepal to be routed and processed through the National Payment Switch. The proposed domestic routing mandate would limit the ability of international payment networks to compete in the provision of payment processing and routing services for domestic transactions and could disadvantage foreign service suppliers relative to domestic infrastructure providers. Industry stakeholders have raised concerns that mandatory routing through a single domestic switch could reduce competition, innovation, operational resilience, and consumer choice, while limiting access to globally integrated fraud prevention, cybersecurity, tokenization, and payment security capabilities. Stakeholders have also cautioned that concentrating domestic payment processing through a single infrastructure may create a potential single point of failure and increase systemic risk. The United States should encourage Nepal to: 1) remove any requirement for mandatory domestic routing and processing through the NPS, 2) allow financial institutions and merchants to choose among competing payment networks, and 3) pursue interoperability through open technical standards and network connectivity rather than routing mandates.

Content Moderation: The Nepalese government has progressively introduced measures to increase control over online content, creating significant operational and human rights concerns. Starting in August 2023 with the National Cyber Security Policy, which proposed a centralized "National Internet

Gateway” for filtering and monitoring traffic, the government has pursued greater regulatory power. This was followed by a November 2023 Social Media Directive requiring local platform registration, and escalated with the January 2025 introduction of a Social Media Act Bill, which grants authorities broad powers to remove content deemed “indecent” or “misleading” and imposes severe penalties . In 2025, Nepal temporarily blocked 26 unregistered social media platforms in September 2025. These actions, which critics argue threaten free expression and create barriers for foreign companies, underscore the uncertain and challenging regulatory environment in the country.

OTT Licensing: Nepal has enacted a series of regulations that impose significant local compliance burdens on foreign digital service providers. Starting in March 2022, under amendments to Nepal’s National Broadcasting Rules 2052 , broadcast and video-on-demand OTT services were required to obtain local licenses and maintain local data servers. Subsequently, a draft framework from April 2023 proposed that communications OTT providers must also register a local office or appoint a local intermediary. This regulatory trend has continued with the E-Commerce Act of 2025, which establishes broad extraterritorial jurisdiction, forcing foreign digital platforms to register locally, comply with Nepali laws, and assume liability as intermediaries for third-party activities, thereby creating substantial regulatory and financial hurdles for international firms operating in the market.

New Zealand

Services Barriers

News Media-Related Digital Service Taxes: In August 2023, the New Zealand government introduced the “Fair Digital News Bargaining” Bill, modeled on similar laws in Australia and Canada, and designed to make large digital platforms like Google and Meta pay for hosting local news content. The Bill aimed to generate NZD 40-60 million annually for New Zealand's news businesses. New Zealand’s version, as compared with the Australia and Canada counterparts, includes more specific parameters for designating digital platforms. However, it empowers news businesses to themselves apply to have a digital platform registered to be subjected to the mandatory bargaining code. This power undermines any incentive of platforms to negotiate deals to obtain exemptions, as any disgruntled news businesses could seek designation regardless of whether they have bargained in good faith with the digital services providers. While the New Zealand government has since put the bill on hold, deeming it “not ready”, the U.S. government should continue to monitor and ensure that this discriminatory tax on U.S. platforms does not proceed.

Nigeria

Services Barriers

Data Localization: The National Digital Cloud Policy, adopted in August 2026, places sovereign data in four levels. ‘Classified’ data must run on infrastructure in Nigeria and under sovereign control, while ‘Open’ data has no residency requirements. The middle tiers depend on the final classification framework and sovereignty provisions, which still need Presidential approval. U.S. providers participating in public tenders will need registration/certification and in-country infrastructure for sovereign workloads. Compliance is required by January 2027, and a demonstrable investment roadmap is required for temporary waivers.

The National Information Technology Development Agency’s (NITDA) cloud guidelines and National

Digital Infrastructure Assurance Framework have turned the National Digital Cloud Policy into operating requirements. They cover classification, interoperability, risk management and minimum provider standards, with one certification regime for data centers, cloud services, AI infrastructure and sovereign compute. A national assessment platform and Certified Cloud Register are expected to make certification a practical condition for regulated work. U.S. providers will therefore be faced with a new layer of technical assessments and localization requirements.

Data Localization for Financial Services: On 15 June 2026, the Central Bank of Nigeria issued Circular No. PSS/DIR/PUB/CIR/001/004, requiring all financial institutions and participants facilitating payments in Nigeria to ensure that payment transaction data generated in Nigeria is stored and managed in Nigeria by 1 January 2027. The measure is broadly framed and does not define “payment transaction data” or “managed in Nigeria.” It also does not provide exclusions for cross-border processing that supports cybersecurity, fraud prevention, anti-money laundering controls, tokenization, dispute resolution, operational resilience or cross-border payment services. This creates significant regulatory uncertainty for U.S. payment and technology companies that rely on integrated global infrastructure to deliver secure and efficient services in Nigeria.

If interpreted to require the localization of all payment-related data and supporting processing, the measure would restrict trusted cross-border data flows, require costly duplication or reconfiguration of global systems, and create barriers to the supply of digital and financial services by U.S. companies. It could also weaken access to global fraud, cybersecurity and risk-management capabilities, increase operating costs, deter investment and impair cross-border and regional payment services.”

Levy on Foreign Digital Platforms: The 2021 Finance Act introduced a tax regime for non-resident companies providing digital services and products to persons in Nigeria, including both income and VAT taxes. The 2020 Finance Act first introduced income tax obligations for non-resident companies providing digital goods and services in Nigeria. While the law applies to all non-resident companies earning above a certain threshold, extensive media coverage and analysis by experts has repeatedly mentioned the targeting of US multinationals. The law specifically references non-resident companies with a “significant economic presence” (SEP) in the country which is defined by a number of factors including: a minimum amount of revenue generated from users in Nigeria, transmitting data about Nigerian users, or the availability of local websites or local payment options. Under Nigeria’s SEP regime, non-resident digital services firms may be taxed on a deemed profit basis, often resulting in an effective 6% rate on turnover where SEP criteria are met. Additionally, a 1% levy on foreign digital platforms was proposed in 2023, but has not yet been enacted.

Content Moderation: In September 2022, the NITDA issued a Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries. Under the Code, digital service platforms with more than one million users must incorporate and maintain a physical presence in Nigeria and appoint a liaison officer, obligations that may limit cross-border operations. The Code contains requirements that create risks for free expression, user privacy, and business operations. The Code's vague definitions of “unlawful content”, coupled with aggressive 24-hour takedown mandates, could be used to suppress legitimate speech critical of the government. Furthermore, requirements for proactive content monitoring and “stay-down” obligations effectively erode crucial intermediary liability protections, forcing companies to act as censors. These issues are compounded by rules that allow the government to demand user data under broad pretexts like “public order” and impose burdensome operational requirements, such as mandating local incorporation, which collectively create a high-risk and uncertain regulatory environment for U.S. platforms.

Further, under Nigerian law, all advertising of any kind needed to be pre-approved by the Advertising Regulatory Council of Nigeria (ARCON), a problematic requirement for online platforms, which are disproportionately U.S. firms. In October 2022, ARCON fined Meta \$70 million for allegedly running advertisements without prior vetting and filed a lawsuit, which it withdrew nearly three years later after little progress. ARCON has since issued similar, largely unenforceable fines to TikTok and Google.

FX Controls: In June 2023, the Central Bank of Nigeria (CBN) announced the removal of the exchange rate peg and the introduction of the “Willing Buyer, Willing Seller” model. Despite the liberalization of the foreign exchange market, CBN maintains stringent controls over the repatriation of funds, which are inconsistent with a willing buyer willing seller market. These controls include the requirement for CBN approval to purchase foreign exchange using funds in Non-Resident local currency accounts, despite such accounts being pre-approved by the CBN for the collection of local currency funds by foreign companies. The approval process for the repatriation of funds remains a significant barrier to investment by U.S. entities, as it is frequently subject to delays and denials. It is recommended that the CBN abolish the approval requirement for the repatriation of funds in Non-Resident accounts.

Norway

Services Barriers

Digital Sovereignty and Ownership Requirements: The Norwegian Government plans to create a national cloud solution for a broad range of critical entities, requiring public sector companies to store over 60% of data using this national service. The government is also applying pressure to extend this to sectors such as energy, telecoms and financial services. The national cloud solution can only be developed by Norwegian providers within Norwegian borders.

Oman

Services Barriers

Electronic Payment Services: Oman is planning to launch a local card scheme. This scheme may prohibit Omani Financial Institutions from entering into commercial co-badge agreements with U.S. EPS providers that facilitate international acceptance for locally-issued debit cards. Some Omani financial institutions such as Bank Muscat whose majority shareholder is the State of Oman are refusing to implement U.S.-provided remittances services citing guidance from the Central Bank to only use the intra- GCC AFAQ network, a local network which does not allow the participation of U.S. EPS providers. We urge USTR to encourage a level playing field for U.S. companies.

Omanisation Requirements: In 2025, the Ministry of Labour introduced an enhanced Omanisation mechanism requiring businesses to recruit Omani nationals or implement approved employment plans. Omanisation requirements continue to present workforce and operational challenges for private-sector employers, as localization compliance is linked to work permit approvals and expatriate hiring. Non-compliance may restrict access to expatriate labor and increase recruitment and compliance costs for affected businesses.

Oman - Postal Levy Requirements: Under Oman's postal regulatory framework, licensed postal and express operators are required to pay a **6% regulatory levy** on specified postal and courier services. In February 2026, the Telecommunications Regulatory Authority (TRA) issued guidance confirming the

scope of services subject to the levy and further clarified that operators should not recover the levy as a separate charge directly imposed on customers. As a result, operators must absorb the levy as part of their operating costs or recover it indirectly through broader pricing adjustments. Given that the levy applies only to specified shipment categories, recovery through broader pricing changes may be operationally complex and reduce pricing flexibility. These requirements increase operating costs and place an additional financial burden on postal and express service providers operating in Oman.

Pakistan

Import Policies

New Seller Registration Obligation. The Finance Act 2025 requires non-resident online marketplaces to ensure only sales tax-registered sellers can operate on their platforms starting July 1, 2025, effectively making online platforms liable for blocking unregistered sellers. This specific platform liability is affecting multiple US firms and there are still gray areas on how cross-border sellers are treated, especially when goods transit via local logistics partners. The courier-based enforcement and lack of clarity in application remain important factors to monitor.

Services Barriers

Data Localization: Pakistan launched a Cloud First Policy in 2022. This policy imposes data localization requirements on wide and open-ended classes of data (“restricted”, “sensitive”, and “secret”). In the financial sector, the State Bank of Pakistan (SBP) prohibits financial sector institutions from storing and processing core workloads on offshore cloud. Pakistan has been considering a “Personal Data Protection Bill”. The bill has a broad scope, applying to both digital and non-digital operators, and includes extraterritorial applications. The bill empowers the federal government to restrict cross-border transfer of “certain personal data”. It also conditions export of personal data on explicit consent by the data subject and non-conflict with Pakistan’s public interest or national security. Such broad language, combined with the regulator’s lack of independence from the federal government, raises the risk that the proposed law could be weaponized, with potential harms to civil liberties and industry. The bill also includes a sweeping mandate for defining “sensitive personal data” that explicitly includes financial data, which may have broad implications for online services. Additionally, the bill includes burdensome requirements for data processing as well as a grant of broad powers to the regulator, with few guardrails. The bill also proposes a National Commission for Personal Data Protection which has extensive powers to introduce new regulatory frameworks and access data. In addition, several sectoral regulators have imposed restrictions on cross-border data flows for regulated entities: the Pakistan Telecommunication Authority (PTA) requires its licensees to obtain prior approval before transferring any data outside Pakistan; the Securities and Exchange Commission of Pakistan (SECP) prohibits licensed digital lenders from storing data on cloud infrastructure located abroad; and the SBP similarly requires licensed exchange companies to maintain both their primary and secondary data centers within Pakistan and permits outsourcing only to local cloud service providers. These data localization requirements are ineffective at enhancing data protection, and significantly increase costs for U.S. firms, potentially deterring market entry.

Digital Taxation: In 2025, Pakistan introduced a digital services tax applicable to the sale of goods and services by offshore platforms with a “significant digital presence” (SDP) in Pakistan. However, before the tax came into force, the Federal Board of Revenue (FBR) issued a blanket exemption on its implementation, leaving uncertainty about its future application. Despite this exemption, Pakistan continues to maintain several overlapping taxation measures on digital products and services. Provincial service tax laws extend their reach to companies without a physical place of business in Pakistan,

effectively taxing offshore entities providing services into the country. At the federal level, income tax laws are also applied extraterritorially to offshore companies. In 2023, the definition of “permanent establishment” (PE) was also broadened to cover entities with no physical presence in Pakistan but a virtual business presence, including where transactions are carried out through the internet or other electronic means. While the U.S.-Pakistan Income Tax Convention should protect U.S.-located operations from the imposition of the “virtual PE” and the SDP measure, companies face challenges in practice due to inconsistent application of the bilateral tax treaty in Pakistan. The U.S. government should encourage Pakistan to withdraw both expanded definitions.

Content Moderation: Pakistan’s *Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021* grants the government power to order online service providers to remove content deemed harmful to “Islam”, “security”, “public order”, “decency”, and “integrity”. Providers face 48-hour (12-hour in emergencies) compliance deadlines, or risk service degradation, blocking, or fines up to PKR 500 million (\$1.76 million). Additional requirements include: mandatory local offices if required by the PTA; registration by the entity providing the service within three months; appointment of a local “compliance officer” and a local “grievance officer” (the grievance officer would be required to redress complaints from the public within 7 working days of receipt); intrusive content moderation and monitoring; and providing user data in a decryptable and readable format to investigative authorities in accordance with existing federal law. These rules greatly jeopardize the ability of U.S. firms to operate in Pakistan and undermine freedom of expression in what is a sizable market.

In 2025, Pakistan amended its Prevention of Electronic Crimes Act, creating the Social Media Protection and Regulatory Authority (SMPRA). The SMPRA has broad powers, including over platform registration, fines, and content removal. These amendments have significantly expanded the categories of content subject to takedown, covering material that SMPRA deems contrary to the “ideology of Pakistan”, that it has “reason to believe” is false, or that contains aspersions against any person, including public officials. Government-imposed internet shutdowns during protests and elections have led to substantial economic losses and human rights violations. Industry reports indicate these shutdowns cause uncertainty and encourage investment flight. Recent shutdowns have cost Pakistan an estimated \$892 million to \$1.6 billion. A new internet firewall implemented in August 2024 has already cost the economy \$300 million and is expected to cause further harm. These content moderation measures, including broad takedown requirements and data disclosure obligations, would severely hinder the ability of U.S. firms to operate in Pakistan and undermine freedom of expression within a significant market.

Internet Services: In October 2021, Pakistan issued the *Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards), Rules 2021* (Rules) which superseded the 2020 version of the Rules. The Rules apply to the removal and/or blocking of online content that is deemed unlawful on any “information system”. Local and international industry players have expressed concerns regarding provisions that would pose significant barriers to operating in Pakistan, including requirements to deploy mechanisms to monitor and block livestreaming content, remove content within short timeframes when ordered by the authorities, and provide data to authorities in decrypted and readable format.

Electronic Payment Systems: The State Bank of Pakistan (SBP) is pushing to have its domestic payment system, 1LINK, process domestic transactions despite no regulatory mandate or circular in place. The SBP is driving this through an Industry-Led Steering Committee, which comprises issuing banks, 1LINK, fintech, and the Pakistan Banks Association. This is a marked change from when the SBP was previously allowing banks to choose their payment network rather than be pushed to use one domestic network only. This represents a trade barrier to processing domestic transactions in Pakistan for international payment networks.

In May 2025, the State Bank of Pakistan (SBP) issued the draft circular “Improving the Adoption of PayPak Cards in Pakistan” that would require an active PayPak debit card before consumers can apply for an International Payment Scheme (IPS) card, unfairly advantaging Pakistani electronic payments system (EPS) companies over U.S. firms. The draft circular would also put in place arbitrary justification requirements to apply for an IPS card, limiting the ability of U.S. EPS providers to offer services in Pakistan.

In July 2026, the Senate Standing Committee on Finance & Revenue considered the broader policy direction around strengthening PayPak, against the backdrop of earlier proposals covering PayPak-first issuance, co-badging and domestic routing. The matter received limited discussion and no formal policy proposal or recommendation emerged. However, the underlying policy debate remains relevant, including subsequent proposals to increase the use of PayPak for government-related payments. The US should encourage a framework that preserves competition, consumer choice and routing optionality, allowing domestic and international payment networks to compete and coexist on fair and non-discriminatory terms.

Panama

Services Barriers

Data Localization and Prior-Authorization Requirements for Public-Sector Cloud Services (AIG Resolution No. 42 of 2024, amending Norm 30.8 "Data Sovereignty"): Panama's Government Innovation Authority (Autoridad Nacional para la Innovación Gubernamental, AIG) issued Resolution No. 42 of October 4, 2024, amending Norm 30.8 ("Data Sovereignty") of the General Standards for the Management of Information and Communication Technology (ICT) in the State. The resolution repealed Resolution No. 52 of 2021, which had imposed broad in-country localization of government databases, and narrowed the localization mandate to databases containing information sensitive to State security or institutional data of a sensitive nature, defined as information classified as confidential in matters of national security whose disclosure, alteration, or loss could compromise the country's security. This is a meaningful liberalization. However, two residual barriers remain. First, for all other cloud services, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and databases not linked to State-security platforms or sensitive institutional data, public-sector entities may store data outside Panamanian territory only after obtaining prior evaluation and authorization from the AIG on a case-by-case basis, submitting a description of the data, the provider, the country of storage, the retention period, and the provider's security measures. This prior-approval requirement introduces delay and administrative friction that a notification-based mechanism would avoid, and is more restrictive than the practice in peer jurisdictions. Second, because the categories of "State security" and "sensitive institutional data" are broadly defined, an expansive interpretation could pull a significant share of public-sector workloads back into mandatory localization, since internationally competitive providers, operate no in-country region in Panama. Building on the progress achieved through Resolution 42, Panama should replace the prior-authorization requirement with a notification mechanism featuring clear timelines, define the "sensitive" and "State-security" data categories narrowly and precisely, and adopt a technology-neutral, risk-based framework that recognizes cloud multi-region resilience and internationally recognized security certifications (e.g., ISO 27001, SOC) as compliant, consistent with Panama's ambition to serve as a regional digital and logistics hub, which depends on open cross-border data flows.

Proposed Adjustments to Express Delivery Regulations: The U.S. express delivery industry is concerned by proposed regulations from Panama's National Customs Authority (ANA) designed to unify

regulations governing express delivery services under a single resolution. Although NFTC commends ANA for including in this important digitization processes that are critical for the modernization of import/export processes, the proposal also seeks to make mandatory complex data requirements for each shipment and aggregates daily consignee values to strip the \$100 duty-free de minimis status. These restrictive measures violate Chapter 5 of the U.S.-Panama Trade Promotion Agreement (PATPA). NFTC recommends that USTR utilize bilateral channels to encourage ANA to follow international standards and comply with its commitments under international trade agreements in its new trade policies.

Electronic Payment Services: Panama’s banking supervisor is increasing its focus on electronic-payment risk management and on the roles of emerging market participants and global payment networks. USTR should monitor future rules or supervisory expectations to ensure that they remain risk-based, proportionate, technology-neutral, and developed through meaningful consultation, with clear allocation of responsibilities across regulated entities and payment networks.

Peru

Import Policies

Trade Facilitation: Under Article 5.7(g) of the U.S.-Peru Trade Promotion Agreement (the “Agreement”), the parties established a de minimis, the value threshold below which no customs duties or taxes are charged on imported goods. The Agreement’s de minimis threshold is set at \$200. However, the Peruvian government has implemented limitations to the number of shipments (three maximum) under the express delivery shipments that an individual without tax number (RUC) can do per year. Also, for individuals, it is uncertain if above the three shipments these personal imports would be considered commercial and create new income tax obligations. Thus, this RUC requirement limits the ability for individuals to import goods for personal use, which constitutes a trade barrier and a limitation to the use of express delivery shipments in Peru.

Customs Penalty Regime for Clerical Errors: Peru's Customs Penalty Regime enforces high, fixed fines of \$360 per air waybill for high-value shipments lacking comprehensive advance documentation. Importers lack a reasonable 48-hour post-arrival grace period to adjust discrepancies, creating an overly punitive environment for minor, non-fraudulent clerical errors. NFTC recommends that USTR press Peru under bilateral trade discussions to establish a mandatory administrative safe harbor and implement automated prescreening tools, allowing operators to amend documentation without facing crippling financial penalties.

Services Barriers

Data Localization: In January 2020, Peru’s Digital Trust Framework (Decree 007) raised significant industry concerns by giving preferential treatment to domestic data storage and service providers. The decree introduced potential trade barriers, including the creation of a whitelist for cross-border data transfers (even though the Peruvian Data Protection Law does not include such restrictions), the establishment of mandatory domestic cybersecurity certifications for private companies, and the creation of a national data center for hosting data provided by public sector entities. While an April 2025 draft regulation has addressed some concerns, making cybersecurity certifications voluntary for the private sector and limiting other measures to critical industries, significant issues persist. The draft fails to clearly define key terms like “internet intermediaries”, creating legal uncertainty and potential enforcement risks, for a wide range of US digital service providers, who could be inadvertently captured by obligations not intended for them. Critically, it has not clarified the original decree's provisions on cross-border data

flows or data localization mandates, leaving businesses facing continued regulatory uncertainty in Peru.

Absence of a Public-Sector Cloud Procurement Framework Agreement: Peruvian law requires the government to establish a framework agreement (acuerdo marco) for cloud services, yet none has been implemented. Article 32 of the Regulation of Emergency Decree No. 006-2020 (which created the National Digital Transformation System) mandates that the Presidency of the Council of Ministers, through the Secretariat of Government and Digital Transformation and in coordination with the central procurement agency Perú Compras, drive the implementation of framework agreements (Catálogos Electrónicos de Acuerdos Marco) for cloud services. Despite this legal obligation, the cloud procurement vehicle has still not been created. As a result, public sector entities lack a standardized, efficient mechanism to acquire cloud services and must rely on general procurement procedures that are ill-suited to the pay-per-use, continuously evolving nature of cloud offerings, creating lengthy processes, legal uncertainty, and a market access barrier for U.S. cloud service providers. Peru should fulfill this existing legal mandate by finalizing and launching the electronic framework agreement (Catálogo Electrónico de Acuerdo Marco) for public cloud, with product structures and pricing rules adapted to cloud services and technology-neutral participation for qualified providers.

Network Usage Fees / Net Neutrality: In August 2026, OSIPTEL, Peru's telecommunications regulator, launched an early consultation (Supporting Document No. 06-2026/DPRC) on potential amendments to its 2016 Net Neutrality Regulation (Resolution No. 165-2016-CD/OSIPTEL). The supporting document explicitly references Korea's "sender-party-network-pays" model and invites comment on whether mandatory network usage fees, or "fair share" schemes, should require content and application providers (CAPs) to compensate ISPs for user-generated traffic. Notably, OSIPTEL's own ex-post evaluation of the Regulation (2016–2024), cited in the same document, found no adverse impact on network investment, deployment, or service quality, undermining the case for such mechanisms. A mandatory fee regime would also be hard to reconcile with the Regulation's Principle of Equity (Article 5.3), which requires non-discriminatory treatment of all traffic and services. U.S. industry has flagged that this could conflict with Articles 14.2 and 14.3 of the U.S.-Peru Trade Promotion Agreement (as well as Articles 13.4 and 13.5 of the CPTPP), which guarantee non-discriminatory access to telecommunications networks and the free cross-border flow of information. OSIPTEL received comments from industry associations, and other stakeholders by the September 24, 2026, deadline; a draft regulation is expected to follow.

Intermediary Liability: Peru remains out of compliance with key provisions under the U.S.-Peru Trade Promotion Agreement (PTPA). Article 16.11, para. 29 of the PTPA requires certain protections for online intermediaries against copyright infringement claims arising out of user activities. USTR cited this discrepancy in its inclusion of Peru in the 2018 Special 301 Report, and we support its inclusion in the 2026 NTE report.

Electronic Payment Systems: There is a governance risk arising from the BCRP's dual role. The BCRP is simultaneously assuming the role of regulator and supervisor of the payments ecosystem, while developing and operating Tapp, the new retail instant payments infrastructure. This concentration of functions creates a potential conflict of interest and departs from the principles of competitive neutrality that support open markets and private investment. Experience in other jurisdictions shows that when the same authority acts as both regulator and operator, it is particularly difficult to preserve effective neutrality and avoid regulatory bias, even when there is an intention to maintain a level playing field.

Although Tapp is presented as complementary infrastructure, in practice the BCRP's regulatory decisions have the ability to favor the system it operates, affecting competitive conditions for other participants.

Industry believes it is essential to ensure a clear separation between regulatory and operational functions, aligned with international governance practices for payment systems.

Peru has an opportunity to build a modern and inclusive instant payments system, but this requires that all technologies and business models be able to compete under equal conditions. Industry is concerned that Tapp's current design favors account-to-account (A2A) transfers, excluding payment credentials and other solutions currently used by millions of Peruvian consumers.

Interoperability should be genuinely open and technologically neutral, allowing the participation of all players that meet objective and transparent requirements. Excluding certain models or technologies could reduce competition, limit innovation, and discourage future investment in Peru's payments ecosystem.

Peru has a unique opportunity to consolidate a modern, interoperable, and inclusive payments ecosystem. However, to attract investment, promote innovation, and ensure sustainable benefits for consumers and merchants, it will be essential to preserve competitive neutrality, ensure appropriate governance of Tapp, and maintain a level playing field for all market participants.

Industry appreciates the U.S. government's efforts and engagement to address these issues.

The Philippines

Import Policies

Pre-Border Technical Verification and E-invoice Submission: Background: Issued in late May 2024, Administrative Order No. 23-2024 implements pre-border technical verification and cross-border electronic invoicing for commodities bound for export to the Philippines. As defined in the AO, pre-border technical verification involves the testing and inspection of commodities by accredited Testing, Inspection, and Certification (TIC) companies prior to export. Cross-border electronic invoicing requires registered foreign exporters to create export invoices on a single electronic platform managed by the Philippine government.

Technical Barriers to Trade

Internet Transactions Act of 2023. The Philippines' E-Commerce Bureau (ECB) of the Department of Trade and Industry (DTI) distributed communications to online marketplaces regarding their obligations under Republic Act No. 11967, also known as the Internet Transactions Act of 2023 (ITA). The transitory period for compliance of ITA ended on June 20, 2025. Specific obligations include requiring online merchants to submit necessary information, maintaining updated lists of merchants, prohibiting the sale of regulated goods without permits, providing effective consumer redress mechanisms, and clearly indicating merchant information in product listings. The DTI emphasizes that failure to comply may result in penalties.

Inconsistent Incentive Regimes: Various laws in the Philippines impose inconsistent and burdensome regulatory requirements on businesses operating in its Special Economic Zones. Specifically, the Business Process Outsourcing (BPO) and related services industries are often subjected to the same obligations as export manufacturing firms, ignoring the fundamental operational differences between them. This regulatory mismatch, coupled with outdated and uncompetitive incentive packages, creates regulatory risk and uncertainty for foreign investors, making the Philippines a less attractive investment

destination compared to other outsourcing locations.

Government Procurement

Government Procurement: The government procurement system in the Philippines generally favors Philippine nationals or Filipino controlled enterprises for procurement contracts. [Republic Act No. 9184 or the Government Procurement Reform Act](#), specifies a minimum Filipino ownership requirement of at least 60 percent in the procurement of goods, consulting services, and infrastructure projects. Domestic goods are also given preferential treatment over imported products in the bid evaluation process. The New Government Procurement Act (NGPA), which became law in 2024, looks to enhance the existing procurement systems implemented by the 21-year-old Republic Act (RA) No. 9184. The law states that preference and priority are given to Philippine products. As per Section 79, "The procuring Entity shall award the domestic bidder if the bid is not more than twenty-five (25%) in excess of the lowest foreign bid. The margin of preference provided herein shall be subject to a periodic review and adjustment by the GPPB, as may be necessary." However, domestic preference can be waived if specific conditions are met, such as if the priority and preference will result in inconsistencies with obligations under international agreements.

While the NGPA introduced more flexible and fit-for-purpose procurement mechanisms that could better support recurring and consumption-based services, such as cloud computing services, these mechanisms have yet to be widely adopted, as many procuring entities remain unfamiliar with their application and opt to continue with traditional procurement and budgeting practices. This implementation gap currently limits the practical benefits of the NGPA and creates uncertainty for cloud service providers and government users seeking to structure scalable, multi-year or pay-as-you-go arrangements.

The government has taken initial steps to improve market access by classifying cloud services as Common-Use Supplies and Equipment and making them available through the PS-DBM eMarketplace. As part of the onboarding process, U.S. CSPs are required to furnish a Certificate of Reciprocity confirming that Philippine companies may compete, with limited exceptions, on an equal basis with U.S. suppliers in U.S. government procurement.

Services Barriers

Data localization: The Philippines is facing increased pressure for data localization, driven by the Department of Information and Communications Technology (DICT), local telcos, and local conglomerate investments in data centers. While proponents argue it enhances national security and the digital economy, the Business Process Outsourcing (BPO) industry and the Joint Foreign Chambers of Commerce strongly oppose it, warning of increased compliance costs and barriers to innovation. Primary beneficiaries of the localization push include local firms and Chinese Cloud Service Providers (CSPs) like Huawei and AliCloud, while U.S. CSPs face growing restrictions. Furthermore, a mandated Securities and Exchange Commission (SEC) license for foreign providers continues to act as a de facto localization hurdle for public sector contracts.

Recent regulatory milestones have formalized this shift:

- **Konektadong Pinoy Act (2025):** Also known as the Open Access in Data Transmission Act, this law liberalized the market by removing outdated legislative franchise requirements. However, a late provision granted the DICT broad authority to safeguard local data for national security. This has raised concerns among foreign businesses that the implementation could introduce mandatory

data localization or overly broad security vetting.

- Executive Order No. 119 (July 2026): established a strict government data classification and residency framework. It mandates that "Top Secret" and "Secret" government data must remain within Philippine territory. Additionally, "Confidential" data can only be stored offshore with strict approvals and safeguards established by the newly created Joint Oversight Committee for Data Classification (JOC-DC).

These developments, alongside circulating drafts of broader data sovereignty regulations, signal a continued trajectory toward strict localization, which will likely impose onerous new compliance requirements on foreign digital service providers.

Taxation of Cross-Border Services: The taxation of cross-border services remains a key concern for foreign investors in the Philippines. The Bureau of Internal Revenue's (BIR) Revenue Memorandum Circular (RMC) No. 5 – 2024 subjected certain cross-border service transactions, including non-resident digital services, to both a 25% final withholding tax and a 12% value-added tax, and presented inconsistencies with the double taxation treaty between the U.S. and the Philippines. Following industry calls for further policy clarity, RMC No. 24-2026 later stressed that income derived from services is generally sourced where the services are performed and that cross-border services are not automatically subject to taxation in the Philippines. While the issuance provided some certainty for foreign service providers, concerns remain that future interpretations of tax rules could broaden the scope of taxation for cross-border transactions and present duplicative tax burdens.

Services Barriers - Telecommunications

Telecommunications: Under the amended Public Services Act (PSA) which took effect in April 2022, public services engaged in the provision of telecommunications services are considered critical infrastructure. Foreign nationals may only own more than 50 percent of public services engaged in the operation and management of critical infrastructure, subject to reciprocity requirements i.e. if the country of the foreign national allows reciprocal rights to Filipinos, as defined by foreign law, treaty, or international agreement. Reciprocity may be satisfied by according rights of similar value in other economic sectors.

The Philippines allocates and manages spectrum through the Radio Control Law of 1931 (RA 3846 and its amendment, RA 584), Executive Order No. 546 1979, and the Public Telecommunications Policy Act of 1995 (RA 7925). These laws and directives provide the country's legal framework for spectrum enfranchisement, operation, and permitting in line with International Telecommunication Union requirements, and general provisions on the allocation and assignment of radio spectrum. While RA 7925 requires the conduct of open tenders in allocating spectrum, no public bidding has ever been carried out to allocate spectrum (e.g., spectrum auctions). Evaluation of applications typically involves submission by an applicant of a letter of request to the National Telecommunications Commission for its spectrum needs. This model is inherently non-transparent, constituting an administrative approach by which applicants are chosen based on the government's prioritization of certain criteria (like financial or technical capacity).

Qatar

Import Policies

VAT: The planned introduction of a 5% VAT may increase operational costs for U.S. exporters. Additionally, logistical challenges still affect supply chain efficiency.

Intellectual Property Protection

Patent Term Extensions & Data Exclusivity Protections: While Qatar has made good progress in IP protection, There is no provision for patent term extensions, and data exclusivity protections are limited. Enforcement mechanisms are underdeveloped, and judicial processes can be slow and opaque.

Services Barriers

Electronic Payment Services: The Qatar Central Bank (QCB) is expanding its domestic payment scheme, Himyan, and has approached U.S. payment networks to explore co-badging options. We urge USTR to encourage a level playing field for U.S. companies.

Russia

Import Policies

Faced with budget constraints, the Ministry of Health is exploring various mechanisms to limit the inclusion of drugs in official lists—such as restricting eligibility to specific clinical indications or patient groups rather than broad INN categories—and to drive price reductions beyond the scope of the current IRP methodology (e.g., through competition between different INNs). However, the draft amendments to the relevant legislation (Government Decree No. 871) have not been published; decision-making authority rests with the government, and communication with the industry remains limited, which hinders dialogue.

Government Procurement

Localization Barriers & Procurement Restrictions: In late 2024, the government introduced new rules requiring localized production of API in order to be eligible for government tenders and pricing advantages. For example, local manufacturers offering to supply medicines from Essential Drug List (EDL) containing locally produced substances would receive a 15% price advantage in state procurement auctions. On top of that, the new rules creating regulatory standards for defining API were approved in 2026. The effective date of the SDL rule has been postponed, as further details are still under development; the definition of 'locally produced API' remains one of the most critical elements

Intellectual Property Protection

Inadequate IP Protection: Russia's pharmaceutical IP environment continues to involve active litigation and uncertainty regarding the practical enforcement of patent rights. Recent industry analysis indicates that pharmaceutical patent disputes have increased in recent years and are increasingly associated not only with patent validity challenges, but also with market entry by follow-on products prior to patent expiry. At the same time, the legislative framework in the area of intellectual property continues to evolve; however, law enforcement practice in certain areas remains insufficiently developed, including with respect to the application of interim measures and the criteria for compulsory licensing.

A further relevant area concerns the practical application of interim measures and compulsory licensing in pharmaceutical patent disputes. While interim relief is formally available, preliminary injunctions appear to remain difficult to secure in practice, including in cases where disputed products may enter public procurement or commercial circulation while litigation is ongoing. Compulsory licensing has also become a more visible element of the IP landscape, including claims related to alleged insufficient use of patented inventions. The development of a more consistent approach involves ongoing dialogue among the Supreme Court, the Constitutional Court, and relevant government authorities, reflecting continued efforts to shape a unified position on these issues.

Possibility of blocking the circulation of drugs that infringe a patent: The Ministry of Economic Development has prepared a draft federal law, the main idea of which is to introduce an prejudicial expedited mechanism for resolving disputes over patent infringement on medicines and to grant the Federal Service for IP (Rospatent): 1) the authority to review complaints from patents holders regarding potential patent infringement in the circulation of medicines 2) the authority to technically block the circulation of medicines in the track & trace system (MDLP) if patent infringement occurred. Status: The draft is undergoing interdepartmental approval (MoIT, FAS, Ministry of Justice, etc.). Although MOH has issued a negative opinion of the draft, this initiative represents an important step in the industry's efforts to further improve the IP protection system.

Compulsory Licensing: Transferring Jurisdiction for CL cases: the Government submitted to the State Duma the bill to transfer consideration of compulsory license cases to the jurisdiction of the Specialized IP Court (SIP) as a court of first instance. Currently, such cases fall under the jurisdiction of arbitration courts. The State Duma is expected to consider the draft law during its autumn session. The likelihood of adoption is high. This initiative is actively supported by industry and is aimed at reducing the number of such cases, ensuring more competent review and more balanced decisions.

Saudi Arabia

Technical Barriers to Trade

SASO Laboratory Testing Requirements: Imported products subject to conformity assessment requirements administered by the Saudi Standards, Metrology and Quality Organization (SASO) may undergo examination, sampling, and laboratory testing as part of the product compliance and certification process. Industry stakeholders have raised concerns regarding increased sampling activity, additional testing costs, shipments and inventory being held pending test results, and extended customs clearance timelines. Management advises that the issue affects multiple customers and industries and is not unique to FedEx. Industry engagement with SASO and Customs authorities is ongoing regarding sampling criteria, testing turnaround times, and opportunities to simplify the process.

GCC - Defence Approval Requirements for Military Shipments: Military products moving into and out of Saudi Arabia are subject to approvals administered by the Ministry of Defense (MOD) and regulatory oversight by the General Authority for Military Industries (GAMI). Saudi Arabia's military industries framework requires licensing and authorization for activities involving controlled defence products, which can increase processing requirements and operational complexity for logistics providers handling military-related shipments across GCC markets.

Government Procurement

Forced Localization Policy (EPP): Foreign companies are required to provide offsets in order to sell to the government. In November 2022, the LCGPA released, without public consultation or private sector input, the Economic Participation Policy (EPP) mandating that foreign companies locally invest 35 percent of the value (based on certain multipliers) of any government tender filled with more than 100 million Saudi Riyal of imported products. In addition, in February 2021, the Ministry of Investment announced that multinational companies must establish their Regional Headquarters in Saudi Arabia to be eligible to participate in government tenders. This requirement was endorsed by a royal decree in December 2022. As a result, U.S. pharmaceutical companies do not receive reciprocal access to the Saudi market.

Other Procurement Challenges: Frequent renegotiation of tenders, combined with the lack of clear timelines, have resulted in an unpredictable government procurement system. The creation of the Local Content and Government Procurement Authority (LCGPA) to identify lists of products that must be procured from local manufacturers, combined with up to 30 percent price preferences for medicines made with locally manufactured active pharmaceutical ingredients (API), serve to discriminate against foreign manufacturers and increase uncertainty in the Saudi market.

Intellectual Property Protection

IP Challenges: The Kingdom does not have a notification system for innovator companies and the current system of reliance on third-party agents does not have sufficient oversight and does not prevent patent violations. Additionally, the SFDA and SAIP introduced the "Approach of Dealing with Patents when registering generic drugs" in January 2023 – which includes a major verification loophole as a free-to-operate (FTO) document is enough to register generics. The Kingdom should add an additional step to this approach that guarantees verification of FTO, while also implementing a more robust IP mechanism that includes a notification system, quality control measures, elimination of conflict of interest, and a reliable dispute resolution system.

Services Barriers

Cross-Border Transfers of Personal Data: Saudi Arabia's Personal Data Protection Law (PDPL) allows companies to transfer personal data out of the Kingdom if they use one of three approved safeguards: standard contractual clauses (SCCs), binding common rules for transfers within a corporate group, or a certificate of accreditation. SDAIA set these safeguards out in its September 2024 Regulation on Personal Data Transfer Outside the Kingdom. While this is an improvement on the original law, which required prior SDAIA approval for most transfers, there is an outstanding concern relating to the terms of the SCCs. Companies cannot change them, and any change makes them invalid. They also require the company receiving the data outside Saudi Arabia to comply with and enforce binding decisions made under Saudi law. As a result, a U.S. parent company that receives data from its Saudi subsidiary becomes directly subject to Saudi regulatory decisions. Companies must also carry out a risk assessment before each regular or large-scale transfer of sensitive data. Together, these requirements raise compliance costs for routine data flows within a company.

The Saudi Data and Artificial Intelligence Authority's (SDAIA) is currently seeking feedback on Saudi Arabia's Personal Data Protection Law (PDPL) Implementing Regulations (open until 5 November 2026). The proposed changes appear to introduce a default requirement to store personal data within Saudi Arabia, while still permitting cross-border transfers only under certain conditions. The most effective solution to provide long-term legal certainty and promote digital trade is for the U.S. Government to advocate for the United States to be recognized on Saudi Arabia's forthcoming list of "adequate"

countries for data transfers.

Data Localization: Saudi Arabia's 2019 Regulations on the Use of Information and Communication Technologies in Government Entities require government entities, state-owned enterprises and operators of Critical National Infrastructure (CNI) to host their data inside the Kingdom. This covers many sectors, from financial services and aviation to oil and gas. Sector regulators can also add their own localization rules on top of this.

In 2024, the National Cybersecurity Authority (NCA) issued updated Essential Cybersecurity Controls (ECC-2:2024) and Cloud Cybersecurity Controls (CCC-2:2024). The updates removed explicit requirements for cloud providers to deliver storage, processing, disaster recovery, monitoring and support from within the Kingdom. However, this did not loosen localization requirements. Instead, the NCA moved responsibility for data localization to the National Data Management Office (NDMO). Entities must now consult the NDMO before making any decision on where data is hosted. Without clear NDMO rules, U.S. cloud providers and their customers have no dependable way to know which workloads can be served from outside Saudi Arabia. The result is a case-by-case approval process that in practice favors in-country hosting.

In addition, ECC-2:2024 requires every cybersecurity position in an in-scope organization to be filled by a full-time, qualified Saudi national. Previously this applied only to senior roles. CCC-2:2024 separately requires cloud providers to fill cybersecurity roles in their Saudi data centers with Saudi nationals. These rules stop U.S. cloud providers from staffing their security teams with experienced specialists from their global workforce, which raises costs and operational risk.

Artificial Intelligence: Saudi Arabia has thus far adopted a generally “light-touch” AI regulatory approach, favoring guidelines over specific laws. A key exception is the draft Global AI Hub Law, which aims to create sovereign data zones to promote international data flow, but the effectiveness of which is limited by a lack of clarity on security standards, legal conflict resolution, and government intervention rules – resulting industry uncertainty in the ability to enhance cross-border management and R&D capabilities. Industry seeks clearer safeguards, predictable data transfer pathways, and alignment with international frameworks.

Digital Content Platform Regulation: Saudi Arabia's Communications, Space and Technology Commission (CST) adopted the Regulations for Providing Digital Content Platform Services in 2023, with compliance requirements taking effect in October 2024. The framework requires digital content platform service providers, including international services, to apply for the relevant regulatory authorization. Implementation remains ongoing, including with respect to applications submitted by international service providers. At this stage, U.S. industry continues to monitor implementation of the framework and its practical implications for international digital services.

Media Regulation: In 2023, Saudi Arabia's General Authority of Media Regulation (GMedia) consulted on a proposed Media Law intended to consolidate and modernize the country's media regulatory framework, including digital media activities. The proposed law has not been formally adopted, and the existing Audiovisual Media Law remains in force. As Saudi Arabia continues to develop its media regulatory framework, U.S. industry encourages transparency, meaningful stakeholder consultation, and proportionate, risk-based requirements that reflect the nature and functionality of different digital media services.

Content Moderation: The regulatory environment is becoming increasingly stringent for content creators

and platforms alike, and point to a heightened level of content moderation oversight and responsibility placed on digital platforms and users within Saudi Arabia:

- The SDAIA issued Deepfake Guidelines in September 2024, requiring platforms to disable and prevent the spread of misleading deepfake content, even if user-generated, with potential penalties for non-compliance and an emphasis on proactive detection.
- An amendment to the Telecommunications and Information Technology Act, proposed by the Ministry of Communications and Information Technology (MCIT) in July 2024, could force social media companies to implement internet filtering and prohibit circumvention, with severe penalties including significant fines of up to SAR25 million (US\$6.6 million), service suspension, and license revocation for non-compliance.

South Africa

Services Barriers

Data Localization: South Africa's National Data and Cloud Computing Policy, published in May 2024 by the Department of Communications and Digital Technologies (DCDT), contains data sovereignty provisions. The Policy states that "data that incorporates content pertaining to the protection and preservation of national security and sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of the Republic." The scope of covered data remains unclear.

Additionally, the Public Procurement Act was signed into law in 2024, but has yet to be brought into effect. Implementing regulations are being drafted, which will bring the new framework into effect. Currently, the procurement regime is not streamlined and is largely hardware-driven, without nuanced and context specific procurement frameworks for other industries including cloud. RFPs are issued with limited participation to specific vendors, which is an issue that is currently being investigated by the South African Competition Commission.

News Media-Related Digital Service Taxes: The South African government is advancing new regulations to force revenue transfer from online platforms through two key initiatives. A draft White Paper on Audio and Audiovisual Media Services proposes introducing a licensing fee for platforms and considering local content quotas. Separately, a February 2025 provisional report from the South Africa Competition Commission on its Media and Digital Platforms Market Inquiry recommends more drastic measures, including a 1% copyright levy, mandatory payments to publishers for news links, and a 5-10% digital advertising levy. Overall, the report significantly distorts the business model of online news and the role digital services play in the online information ecosystem. Given the focus of the report and in anticipation of the release of the finalized proposed remedies, industry remains concerned and urges the U.S. government to continue to push back on the report and future action.

Online VAT: South Africa currently levies a 15% VAT on the online selling of content, including films and television programming. As of 2019, income on services provided to South African businesses by foreign businesses is also subject to VAT.

Electronic Payment Systems: Foreign payment system operators were required to localize domestic processing infrastructure to comply with the amendments of the Payment Association of South Africa (PASA) Payment Clearing House (PCH) System Operator Criteria (focusing on domestic processing)

effective from August 1, 2025. The policy requires that, for domestic transactions, payment service operators must authorize, clear and settle transactions through infrastructure that is established and maintained in South Africa. In 2025 the South African Reserve Bank (SARB) announced its intention to establish a domestic scheme. This will impact international schemes, who have made significant investments in localizing infrastructure, and NFTC urges USTR to work to assure a level playing field for U.S. companies.

Regulation of New Audiovisual Services under the Broadcasting Regime: Since 2020, the South African government has been considering overhauling the regulatory framework governing audiovisual media services. In particular, the government is considering whether, and how, to extend the regulatory regime for broadcasting to other audiovisual media services. The government published draft White Papers in 2020, 2023, and 2025. In particular, the White Papers suggest that the government intends to apply licensing/registration requirements on SVOD players which may result in several obligations including compliance with broad-based economic empowerment laws which include local shareholding requirements, a local content quota or a levy (quantum yet to be determined), discoverability obligations and the establishment of a new ombudsman without a clear mandate, risking mandate duplication with existing regulators such as the Film and Publication Board. These rules would undermine and unreasonably burden U.S. streaming services operating in South Africa.

Switzerland

Government Procurement

Public Procurement: RFIs for public and cantonal IT tenders increasingly use the CLOUD Act as a justification to exclude U.S. cloud providers from participating, despite Switzerland's commitments under the WTO GPA.

Services Barriers

Surveillance Law: In January 2025, the Swiss Federal Council opened a consultation on a partial revision of the Telecommunications Surveillance Ordinances (VÜPF), aiming to clarify cooperation duties for telecommunications and communications service providers, and to adapt regulations to technological developments. The revision seeks to introduce a three-tier obligation system for "derived communications service providers" (including cloud providers) based on user volume (starting at 5,000 users) and revenue thresholds (CHF 100M+ for full obligations), and requires expanded data retention, user identification capabilities, and technical surveillance interfaces that undermine encryption protections. The proposal has faced overwhelming rejection in public consultation from all major political parties and industry associations, with prominent Swiss startups threatening to exit due to privacy concerns and disproportionate compliance burdens. Despite this, the Federal Government remains intent on introducing these new requirements. For U.S. cloud providers, the proposed revision could significantly impact Swiss operations, potentially requiring substantial compliance infrastructure, expanded data retention capabilities and weakened encryption.

Taiwan

Services Barriers

Restrictive Use of Public Cloud for Generative AI: Taiwan's National Science and Technology Council

(NSTC) has issued an administrative ruling restricting government agencies from using public cloud-based generative AI services. While intended to protect sensitive information, the ruling creates significant market access barriers for global cloud service providers (CSPs) and their AI offerings.

The ruling's core requirement mandates on-premises deployment for the use of generative AI by government agencies, explicitly prohibiting public cloud-based AI services for government data processing. This creates a de facto data localization requirement and restricts the use of public cloud through technical specifications. Such requirements contradict global best practices where hybrid and public cloud solutions often provide superior offering of generative AI and security measures.

While the ruling aims to ensure data sovereignty and control, it imposes restrictive requirements including mandatory on-premises deployment, physical system isolation, and local data control. These create substantial barriers through increased infrastructure costs, reduced access to advanced AI technologies, and limited scalability. The requirements effectively prevent government agencies from leveraging global AI innovations and cloud-based solutions that could enhance public services.

These restrictions raise concerns regarding Taiwan's international trade commitments and digital transformation objectives. They potentially violate WTO Technical Barriers to Trade (TBT) Agreement principles and create inconsistencies with Taiwan's open government procurement commitments. We recommend revising the ruling to align with international best practices while maintaining secure use of generative AI through 1) adopting a risk-based approach rather than blanket restrictions, 2) recognizing international standards and certifications, and 3) allowing secure cloud-based generative AI services with appropriate safeguards.

Intermediary Liability: Taiwan's approach to intermediary liability is creating a significant trade barrier by systematically eroding safe harbor protections, a practice that deviates from established democratic norms. Rather than implementing a clear and predictable legal framework, the government is pursuing a sectoral approach that imposes "strict liability" on platforms for user-generated content. This trend forces digital services to pre-screen and censor content, creating an untenable operating environment and undermining free expression. The enforcement of the Tobacco Hazard Prevention Act is a stark example of this flawed liability model. While the government aims to regulate illicit sponsored user content, the Act's critical flaw is its failure to assign liability to the content creator—the party actually engaged in advertising. Instead, it improperly holds the intermediary platform legally responsible, defining sponsored posts as commercial "advertisements" and mandating that platforms pre-screen all user content against an ever-expanding list of keywords. This results in severe, repeated fines for platforms over content they did not create.

This pattern of governance ignores the fundamental distinction between paid advertising and user-generated content, compelling platforms to build extensive, preventative censorship systems. This not only constitutes a significant non-tariff barrier to trade but also normalizes speech-filtering mechanisms inconsistent with a free and open internet, undermines the free flow of information online which, in some instances, is essential to U.S. business interests (including for training AI models), and hinders the development of a vibrant digital public sphere. We urge the U.S. government to press Taiwan to adopt a coherent intermediary liability framework with clear safe harbor provisions that correctly assign liability to the originator of illegal content, not the intermediary.

Data Localization: A recent initiative by Taiwan's Personal Data Protection Committee Preparatory Office to develop a unique, domestic set of Standard Contractual Clauses (SCCs) for cross-border data transfers represents a significant concern for U.S. and other foreign investors. This plan risks creating a

bespoke data transfer mechanism that is incompatible with established international standards, thereby generating pervasive legal uncertainty and substantial compliance burdens. A fragmented Taiwanese SCC framework will not facilitate secure data flows; instead, it would fragment the digital economy, compelling multinational companies that rely on globally integrated systems to adopt costly and duplicative contractual arrangements. ITI urges the U.S. government to encourage Taiwan to adopt flexible cross-border data transfer mechanisms. Prescriptive SCCs or templates should not be a pre-requisite for cross-border transfers so long as the parties have contractual arrangements or overarching policies in place that contractually obligate the transferee to adhere to a standard of protection comparable to the transferor's home country's standard. Adopting a flexible, risk-based approach will allow data controllers to operate in a safe, efficient, and internationally interoperable manner across jurisdictions, supporting U.S. investment and sustainable digital trade.

News Media-Related Digital Services Taxes: Legislators in Taiwan have introduced proposals to the Legislative Yuan to initiate a mandatory news bargaining code, with the legislative process advancing without industry or public consultation. The opposition parties have designated the bill as a priority, creating a significant risk of enactment of a law imposing mandatory revenue transfers from digital services providers to local news businesses. This legislative push ignores substantial, proactive digital investments and voluntary support from platforms to help foster a sustainable news ecosystem in Taiwan, including multi-year co-prosperity funds and ongoing digital skills training designed to support the transformation of local news organizations. Industry remains concerned that the proposed law would constitute a discriminatory trade barrier and urges the U.S. government to continue to oppose its enactment.

Services Barriers - Telecommunications

National Communications Commission: Since 2021, Taiwan's National Communications Commission ("NCC") has mandated firewalls, switches, and routers deployed in critical telecommunications infrastructure to undergo re-certification at two designated laboratories located in Taiwan, regardless of any existing certifications from foreign laboratories (e.g., U.S.-based laboratories that are already recognized by the Taiwan government). The local testing in the two designated testing facilities – one of which is affiliated with the Ministry of Digital Affairs ("MODA") and the other a private laboratory named "Onward Security" – are mandatory under MODA regulations. Furthermore, each firmware update requires additional re-certification in both Taiwanese laboratories.

Taiwan's Bureau of Standards, Metrology and Inspection (BSMI) regulates safety, health, and environmental standards for imported products. Under its recent draft regulation on "Relevant Inspection Regulations for Information Products, Audiovisual Equipment, and Ten Other Categories of Goods Subject to Mandatory Inspection", BSMI has proposed new

requirements that would require U.S. companies to re-certify products and rely on local laboratories for cybersecurity testing. These duplicative rules would significantly increase compliance costs, delay time-to-market, and create unnecessary barriers for U.S. exporters.

Such dual certification requirements, coupled with the mandatory re-testing of firmware updates, creates significant trade barriers by requiring redundant and unnecessary testing. U.S. companies already invest heavily to meet internationally recognized standards, and BSMI should accept certifications from accredited global testing laboratories instead of mandating re-testing in Taiwan. Unless addressed, these measures risk discouraging investment and limiting the competitiveness of U.S. technology products in Taiwan's market.

Tanzania

Services Barriers

Digital Services Tax and other digitally focused taxes: Tanzania adopted a 2% DST as part of its 2022-2023 Budget and issued regulations on July 1, 2022. The DST applies to the gross revenues of non-resident persons from providing digital services to individuals in Tanzania. The rate was increased to 3% beginning July 1, 2026. In addition, the Finance Act of 2026 and its implementing regulations applied a new excise duty to certain services supplied to Tanzanian customers by non-resident suppliers. Rates range from 7% for pay-TV and video on demand (VOD) services to 17% for electronic communication services.

Thailand

Technical Barriers to Trade

Pricing: National Drug Committee sets price ceilings for essential drugs, limiting pricing flexibility. Price negotiation required for public reimbursement listing, especially via the National List of Essential Medicines (NLEM). Private pricing remains largely unregulated, but under public scrutiny and consumer protection lens (e.g., Consumer Protection Board).

Government Procurement

Maximum Procurement Price: Thailand's Ministry of Public Health and the National Drug System Development Committee oversee the Maximum Procurement Price (MPP) system for pharmaceuticals. While intended to control public spending, the MPP process lacks transparency and predictability, especially when combined with preferential treatment for domestic suppliers. This has created barriers for foreign companies and delayed patient access to innovative medicines: only 21% of new global medicines since 2014 have launched in Thailand, with an average delay of 36 months.

The 2017 Public Procurement Act introduced a Reference Price Subcommittee to standardize pricing, but its implementation remains slow. **NFTC urges expedited formation and inclusion of private sector stakeholders to improve transparency and collaboration.**

The Oncology Prior-authorization System under the Civil Servants Medical Benefit Scheme (CSMBS) was designed to reduce out-of-pocket costs for high-cost cancer drugs. However, recent tiered revisions have made reimbursement inconsistent and unclear, with some newly approved drugs deemed non-reimbursable. Patients may face financial barriers or limited treatment options due to opaque criteria and budget constraints. To ensure equitable access, stakeholders recommend transparent OCPA procedures, outcome-based evaluations, and flexible financial models to balance innovation, affordability, and public health needs.

State-Owned Enterprises / Procurement

Preferential Procurement: Thailand Government Pharmaceutical Organization (GPO), a Thai State-owned enterprise that manufactures pharmaceutical products in Thailand, benefits from preferential procurement privileges. Per Ministerial Regulation B.E.2560 (2017), government hospitals must procure

at least 60 percent of their medicines budget from the NLEM. Specific procurement methods are required if the product on the NLEM is manufactured by the GPO or the Thai Red Cross Society. Purchases from other suppliers are permitted only when the GPO or the Thai Red Cross Society is unable to produce and distribute the product. In addition to these procurement preferences, under the Drug Act B.E. 2510 (1967), the GPO is not required to obtain FDA approval prior to launching medicines on the Thai market. There is no such exemption for private sector manufacturers or sellers, all of whom must obtain appropriate market authorization from the Thai FDA prior to selling their products in the Thai market. Further procurement privileges are also being extended to local vaccine producers under National Vaccine Committee Regulations on “Vaccine Procurement in Government Sector” that went into effect on August 14, 2020.

Services Barriers

Data Localization: In 2025, Thailand’s Digital Government Development Agency (DGA) introduced draft guidelines – the Government Cloud Usage Guidelines and the Cloud Data Classification Guidelines – to support the national “Go Cloud First” policy. Despite the policy’s aim for greater cloud adoption, the guidelines impose significant data localization requirements, mandating that most government and regulated data be stored in Thailand. Cross-border transfers are subject to narrow exceptions requiring DGA approval and a local data center being built in Thailand. Furthermore, the policy stipulates that the most sensitive government data (in the “Secret” and “Top Secret” categories) can only be handled by a state-owned enterprise. Furthermore, there are requirements that providers comply with domestic procurement rules, achieve government-mandated certifications, and demonstrate conformity with Thai security standards, which will raise compliance costs and exclude providers that rely on global or regional data management models. These data localization and sovereignty requirements effectively limit participation by U.S. and other foreign cloud services providers from participating in public sector projects. These measures not only restrict competition but also risk fragmenting the digital ecosystem by forcing data silos and limiting the scalability of international services, creating significant market access barriers for U.S. cloud services providers.

Postal Parity: Current Thai law restricts any other carriers for transporting documents other than Thai Post, the state-owned postal operators. Express carriers are regularly fined by Thai Post for transporting documents to recipients in Thailand, which is necessary in some cases to meet their chain of custody obligations. Yet Thai Post is allowed to carry small parcels which are also carried by Express carriers.

Logistics Regulation: ETDA is proposing a logistics regulation that will require all e-commerce marketplaces to provide both customers and sellers with at least three logistics carrier options for deliveries. ETDA is aiming to implement the Logistics Regulation by December 2025. The draft, however, has not been shared publicly, and we understand that a call for public comments can be expected soon. Five local logistics carriers had been consulted behind closed doors by ETDA.

Platform Economy Act : Thailand is drafting ex-ante digital platform framework legislation to regulate digital services, adopting concepts from the EU's Digital Services Act (DSA) and Digital Markets Act (DMA). Under this proposed law, cloud services could be classified as 'intermediaries' and may become subject to 'gatekeeper' obligations. During the previous administration, development of the law was paused due to concerns about potential impacts on digital innovation and possible creation of trade barriers. However, with the recent change in government, the initiative has been revived. The new administration announced its intention to pursue this legislation in its policy statement in late September 2025. e government, as of today, is still working on the draft.

Digital Platform Fair Competition Draft Rule. The Trade Competition Commission of Thailand (TCCT) finalized its Guidelines on the Consideration of Unfair Trade Practices and Conduct Constituting Monopoly, Reducing Competition, or Restricting Competition in Multi-Sided Platform Businesses in the Category of Digital Platforms for the Sale of Goods or Services (E-commerce), were published in the Government Gazette on March 24, 2026 and took effect March 25, 2026. The guidelines provide the first detailed framework for how the TCCT will interpret and enforce the substantive provisions under the Trade Competition Act against digital platforms, which have a unique network effect and require complex competition analysis. This development will profoundly impact the operations of e-commerce platforms, sellers, and associated service providers in Thailand. Affected digital platforms have highlighted issues such as proportional algorithmic transparency (aligned with international practice), allowing legitimate operational requirements (e.g., logistics/payment solutions) where justified, and flexibility in designing transparent and non-discriminatory fee structures.

Digital Platform Services (DPS) Decree: The DPS decree, which came into force in 2022, is a regulation that aims to enhance consumer protection in digital transactions. Initially designed to regulate electronic intermediary services that facilitate connections between users for commercial transactions, the decree primarily targeted platforms such as e-commerce marketplaces, ride-hailing services, and food delivery applications. The Electronic Transaction Development Agency (ETDA) is the owner of this regulation.

However, the implementation of this regulatory framework has evolved beyond its original scope, with ETDA extending registration requirements to a broader range of digital service providers. This expansion now encompasses social media platforms, video conferencing services, and cloud service providers - entities that arguably fall outside the decree's intended purview. This broadened interpretation of the regulation's scope has raised questions about the true objectives of the registration scheme and its effectiveness in achieving its stated consumer protection goals.

The registration requirements impose significant obligations on digital service providers, including annual reporting of user statistics and gross revenue disclosure. These extensive reporting requirements, particularly those related to financial data, suggest potential agendas beyond consumer protection, possibly laying out the groundwork for future digital taxation initiatives. Moreover, the regulatory burden appears redundant given the existence of multiple consumer protection frameworks already governing digital commerce, raising concerns about regulatory overlap and unnecessary administrative complexity.

Total Take Rate (TTR) Disclosure Guideline: ETDA issued a voluntary guideline (Announcement No. THPD 3/2569, September 2026) directing marketplace platforms to disclose a consolidated "Total Take Rate" combining all platform fees, with advance notice required before fee changes take effect and a calculator tool to be made available to sellers. The guideline is voluntary for now, but ETDA has indicated it may be codified as a binding requirement under a forthcoming Digital Platform Services Law if industry compliance is deemed insufficient. Industry has urged that any future codification include objective, bright-line criteria for distinguishing "additional service" fees from "basic" fees, a quantified trigger for mandatory fee-increase warnings rather than an undefined "significant impact" standard, and a reasonable phase-in period before mandatory compliance.

Advertiser Identity Verification: Under Electronic Transactions Commission (ETC) Notification No. 2 on Prevention of Technology Crime for Online Social Media (published in the Royal Gazette May 5, 2026; mandatory from November 1, 2026), social media platforms must verify the identity of every advertiser before an ad is published — using either a government-issued reference standard or a certified digital verification system — and retain the advertiser's identity and contact information for at least 90

days after the advertising relationship ends, with annual re-verification required. The requirement currently applies to social media advertising specifically rather than e-commerce marketplaces generally, but is a precedent worth monitoring for extension.

High-Impact Marketplaces: High-Impact Marketplaces. Thailand's Electronic Transactions Development Agency (ETDA) designated digital platforms as "High-Impact Marketplaces" under Section 20 of the Royal Decree on the Operation of Digital Platform Service Business, B.E. 2565. The Royal Gazette initially designated 19 platforms on July 9, 2025, effective July 10, 2025; ETDA subsequently expanded the list, and additional requirements — including seller verification, monitoring of regulated products, notice-and-takedown procedures, and reporting — took effect December 31, 2025, with 21 platforms now covered. The list continues to be reviewed and expanded, creating ongoing regulatory uncertainty for affected platforms.

AI Act: Thailand's draft AI Act introduces sovereignty requirements for AI services: invoking national strategic autonomy, regulators can dictate the contract terms of AI and data processing services supplied to government and critical infrastructure, require those services to be processed inside Thailand, and obtain court orders to access providers' technical documentation and training data. Foreign providers of high-risk systems must also establish an in-country presence, and providers and deployers face joint liability for AI-related damage regardless of fault — stricter than any regime in the region and in key respects stricter than the EU. The combined effect favors domestic providers. Companion legislation would impose governance and transparency obligations on AI-driven platform functions such as product recommendation, search ranking, and chatbots, including a local-liaison requirement for offshore AI providers. The draft remains under discussion.

Content Moderation: Thailand has enacted two laws that raise significant industry concerns regarding government overreach and surveillance. Under the Computer Crime Act, the Ministry of Digital Economy and Society established an Anti-Fake News Center to combat what is considered “false and misleading” in violation of the Act, and leveraged this to expand oversight of content and identify millions of posts. Similarly, the controversial Cybersecurity Act grants officials broad authority to search and seize data and equipment in what are vaguely defined as "national emergencies," enabling potential government surveillance.

Türkiye

Import Policies

Market access delays (Pharmaceuticals): Long licensing processes delay product entry into the Turkish market. The Turkish Drug and Medical Device Agency (TITCK) prioritizes Good Manufacturing Practices (GMP) audit procedures and allows marketing authorization applications to advance in parallel with GMP process. However, these procedures have not diminished the delays in MA approvals. While “highly innovative designated products” receive preferential reviews, products without this designation face increased delays in GMP inspections. For the GMP inspections that are carried out by the FDA and/or EMA, the Turkish authority should not carry out GMP inspections for the same imported products with approved and accredited certificates. Instead, it should recognize FDA or EMA approvals and there should not be an additional GMP audit by Turkish authority.

Intellectual Property Protection

Inadequate Regulatory Data Protection and patent enforcement (Pharmaceuticals): According to Türkiye's Industrial Property Law, which was passed by the Turkish Parliament in 2016, the RDP term begins with first marketing authorization of the original product in any of the EU-Türkiye Customs Union Area Member States. As a result, the effective RDP term is reduced significantly to 6 years in Türkiye – and considering the marketing authorization process timeline of approximately 2-3 years, the life without generics is approximately 3 years for originator/innovator products.

Services Barriers

Data Localization: Presidential Circular 2019/12 on Information and Communication Security Measures requires critical public data to be stored in Turkey and effectively blocks public sector organizations from using U.S. cloud services. Strict data localization requirements are also applied to the financial services industry, where the Banking Regulation and Supervision Agency (BDDK), under Banking Law No. 5411, requires banks' primary and secondary information systems to be hosted in Turkey. The Central Bank of Turkey, under Law No. 6493, also requires payment system IT infrastructure and backups to remain in Turkey. The Capital Markets Board (SPK), under Communiqué VII-128.10, similarly requires systems to be hosted in-country, permitting external cloud only for order matching with same day data repatriation. While Turkey liberalized cross-border transfers of personal data under Law No. 6698 in 2024, the sector-specific requirements above were not aligned with that reform. Meanwhile, the Turkish Data Protection Law (DPL) permits the transfers of personal information to jurisdictions deemed adequate, subject to the explicit consent of the data subject or after obtaining permission from the data protection authority (KVKK). However, Türkiye has not yet decided on countries deemed adequate for international transfers. The adequacy decision has been postponed several times since 2021; with the latest timeline for the announcement being Q4 2024. Certification rules for regulated industry and government cloud use under the 2025 Cybersecurity Law No. 7545 remain under development, prolonging uncertainty for US cloud and AI providers.

Cybersecurity Law: The implementation of Türkiye's Cybersecurity Law (No. 7545) is expected to introduce new accreditation, certification, and compliance requirements for technology systems. Following the designation of Finance as a critical infrastructure sector in May 2026, financial institutions and payment ecosystem participants are likely to face heightened cybersecurity oversight, with the full scope of obligations pending secondary legislation.

Data Localization: A 2019 Presidential Circular on Information and Communication Security Measures introduced localization requirements on government workloads deemed "strategic". In 2020, the Digital Transformation Office published Guidelines clarifying that the scope of the localization requirements included critical information and data; however, the loosely defined residency obligations under the Presidential Circular remain a regulatory challenge as the legislation overrides the DTO Guidelines. Strict data localization also applies in the financial services sector, where the Banking Regulation and Supervision Agency require primary and secondary information systems to be hosted in Türkiye. The Central Bank of Türkiye implements similar restrictions on cloud outsourcing and prohibits the use of cloud for certain workloads. The Turkish Data Protection Law (DPL) permits the transfers of personal information to jurisdictions deemed adequate, subject to the explicit consent of the data subject or after obtaining permission from the data protection authority (KVKK). However, Türkiye has not yet decided on countries deemed adequate for international transfers. The adequacy decision has been postponed several times since 2021; with the latest timeline for the announcement being Q4 2024.

Level-playing field and localization: Türkiye continues to contemplate extraterritorial authority over U.S. electronic payment services companies and their clients domiciled outside of Türkiye. Specifically,

Türkiye is considering regulation of inbound cross-border payments originating from the EU, and such regulation would be more burdensome and restrictive on U.S. EPS providers and their clients, than it is on domestic companies. In order to promote local payment facilitators, the Finance Ministry and Central Bank continue to scrutinize Visa rules prohibiting Turkish acquirers from providing acquiring services to a merchant located in a jurisdiction where it does not have a license to operate, and misrepresenting the location of the foreign merchant as if it was based in Türkiye. Under current Turkish regulation (Article 19 of the Payment Services Regulation), payment services involving a foreign party must reflect genuine cross-border activity and require appropriate authorization for cooperation with foreign entities. However, local Payment Facilitators (PayFacs) have developed models that enable foreign merchants to appear as if they are locally established and subsequently route cross-border transactions through local acquiring infrastructure, effectively treating them as domestic. This practice undermines U.S. companies' Turkish and global operations in several ways. First, it contradicts international card scheme rules. Second, it opens companies up to legal and compliance risks. Third, this treatment has introduced further burdens, as the Turkish Competition Authority (TCA) is investigating U.S. electronic payment service suppliers over the dispute in this practice. This treatment provides uniquely difficult conditions for U.S. companies compared to domestic competitors and warrants engagement from USG to ensure U.S. EPS companies can follow international best practices when serving the Turkish market.

Competition / Ex Ante Rules: Türkiye proposed an amendment to its competition law that largely mirrors the EU's Digital Markets Act. The draft law imposes significant obligations on large digital platforms, which are disproportionately U.S. companies, including mandatory interoperability, a ban on self-preferencing, and restrictions on using data across different services. The draft law also includes severe penalties, such as fines of up to 20% of annual turnover and potential five-year bans on mergers and acquisitions. While the draft law is currently on hold pending trade negotiations with the U.S., certain obligations included in the draft law were, however, adopted in the Regulation of E-Commerce Law, which took effect January 1, 2024. The law prohibits e-commerce intermediary service providers from selling their own trademarked goods on their platform. It imposes additional obligations on larger providers, with those with an annual net transaction volume greater than ₺10 billion (US\$538.3 million) prohibited from using data collected to compete with other providers, and those with an annual net transaction volume greater than ₺60 billion (US\$3.3 billion) prohibited from expanding into industries such as payments, transportation, and delivery as separate business models. Moreover, it imposes new taxes on companies based on their revenues, while providing relief for Turkish-headquartered e-commerce companies. These excessive regulatory requirements, *de facto* preference for Turkish companies, and pressures for localization represent clear barriers for U.S. companies.

Digital Services Tax: Türkiye continues to administer its DST that USTR has previously determined to be discriminatory in a Section 301 investigation initiated in 2020. USTR has previously found that the Turkish DST “is discriminatory against U.S. companies, “contravenes prevailing international tax principles”, and “burdens or restricts U.S. commerce” in its 2021 report on this barrier. The tax undermines U.S. exports, threatens American jobs, and raids the U.S. tax base. Türkiye’s 7.5% DST went into effect on March 1, 2020. The rate of the tax decreased to 5% on January 1, 2026, with a further reduction to 2.5% scheduled for January 2027. The global revenue threshold for this tax is ₺750 million, with a local threshold of ₺20 million. The tax applies to revenue generated from the following services, all of which are sectors where American companies are world leaders: (1) digital advertising, (2) online streaming and sales of audio and audiovisual content, and (3) social networking services. The tax disproportionately impacts U.S. companies. By maintaining this discriminatory tax, Türkiye is promoting unfair treatment of US companies in the market, to the detriment of American exports, tech leadership, and for consumers and businesses in the Turkish market that partner effectively with US tech companies. NFTC encourages USTR to continue working with Türkiye to address the discrimination against U.S. companies under Türkiye’s DST.

Additionally, in 2024, Türkiye amended Law No. 6563, which would impose burdensome withholding tax requirements for non-resident companies that operate e-commerce platforms, depending on how the law is implemented. There is significant uncertainty in the scope and base of the tax, and industry urges vigilance to ensure companies can operate with fair access in the market. The new requirements took effect on January 1, 2025.

VOD Levy Proposal: In July 2026, Türkiye introduced a legislative proposal that would have required U.S. streaming companies to pay 2% of their local revenue as a levy to the Ministry of Culture and Tourism's fund to support the cinema and film industry. The proposal covered only streaming and internet platform services under RTUK license and not linear TV, targeting the predominantly U.S. companies that are successful in streaming and carving out the domestic competitors that dominate traditional TV. If approved, the levy would have undermined Türkiye's DST rate reduction, which was a positive development. The government did not enact the levy in July 2026, but we have heard that the ministry of Culture and Tourism plans to resurrect the proposal in Q4 2026.

Content Moderation: Türkiye has established a highly restrictive and punitive environment for internet services, actively using censorship and legislation that economically harms U.S. companies. A key step was the July 2020 passage of Law No. 7253 (amending the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications), which grants the government sweeping powers over social media. This law compels platforms with over one million daily users to appoint a local representative, respond to takedown requests within hours, and store the data of Turkish users domestically. Authorities moved quickly to enforce these rules, imposing fines, advertising bans, and bandwidth restrictions on non-compliant firms.

The government further intensified its control with Law No. 7418 (Amendment of Press Law, and Certain Laws) in October 2022, which criminalizes the spread of "disinformation" with prison sentences of up to three years. This law requires platforms to disclose algorithms and user data to the government upon request and threatens penalties including fines of up to 3% of global revenue and bandwidth throttling up to 90%. The law also extended the authority of the Information Technologies and Communications Authority (ICTA) over messaging (OTT) services, empowering it to demand detailed user activity data. Failure to comply could result in fines rising to ₺30 million (US\$1.6 million), throttled service up to a 95% restriction on the usual bandwidth capacity, or outright service blockage. Subsequent regulations in April 2023 solidified these obligations, holding platforms responsible for user-generated content and imposing a comprehensive set of duties on all social network providers, regardless of size. These measures negatively impact U.S. companies by imposing steep financial penalties, significant operational burdens like mandatory data localization, and severe legal risks, including liability for user content and the forced disclosure of proprietary algorithms and user data.

Furthermore, Radio and TV Supreme Board (RTUK) leverages Law No: 6112 more often to order content takedowns to VODs services on the basis of vague terms such as cultural and moral appropriateness, which makes operating environments challenging especially for U.S. companies.

OTT Regulation: In March 2025, Türkiye's Information and Communication Technologies Authority (ICTA) proposed sweeping regulations that would subject over-the-top (OTT) communication providers to the same burdensome regime as legacy telecommunications firms. The draft rules mandate that OTTs with over one million monthly users must incorporate locally as a Turkish company, obtain authorization under telecom law, and contribute to a universal service fund for infrastructure they do not use. Additionally, providers would face vague "national security" obligations that could lead to surveillance, and the government reserves broad power to impose severe penalties, including fines, service throttling,

or outright blocking. These requirements, particularly the forced local incorporation, create significant market access barriers for U.S. and foreign companies, undermining the cross-border model of the internet, stifling innovation, and tilting the market in favor of domestic incumbents.

Additional E-Commerce Regulations: A new set of e-commerce regulations in the Law on Amending the Law on Regulation of Electronic Commerce took effect in 2023. Firms that facilitate sales equaling or topping ten billion Turkish lira net (\$538.3 million) annually and over one hundred thousand executed transactions will be required to obtain a license to operate in the country and renew that license when the Ministry of Commerce dictates. Further, the law requires a restriction on e-commerce providers selling goods of their own brand or brands with which they have economic associations. E-commerce providers will also be subject to obligations to take down illegal content and ads, ensuring information is correct, obtaining consent before using brands for promotions, and refraining from anticompetitive practices. For firms with a net transaction of over 60 billion liras (\$3.3 billion), there are a host of other restrictions regarding banking, transportation, and delivery.

Electronic Payment Services: Türkiye continues to contemplate extraterritorial authority over U.S. electronic payment services companies and their clients domiciled outside of Türkiye. Specifically, Türkiye is considering regulation of inbound cross-border payments originating from the EU, and such regulation would be more burdensome and restrictive on U.S. EPS providers and their clients, than it is on domestic companies. In order to promote local payment facilitators, the Finance Ministry and Central Bank continue to scrutinize the rules of U.S. EPS providers' that prohibit Turkish acquirers from providing acquiring services to a merchant located in a jurisdiction where it does not have a license to operate, and misrepresenting the location of the foreign merchant as if it was based in Türkiye. Under current Turkish regulation (Article 19 of the Payment Services Regulation), payment services involving a foreign party must reflect genuine cross-border activity and require appropriate authorization for cooperation with foreign entities. However, local Payment Facilitators (PayFacs) have developed models that enable foreign merchants to appear as if they are locally established and subsequently route cross-border transactions through local acquiring infrastructure, effectively treating them as domestic. This practice undermines U.S. companies' Turkish and global operations in several ways. First, it contradicts international card scheme rules. Second, it opens companies up to legal and compliance risks. Third, this treatment has introduced further burdens, as the Turkish Competition Authority (TCA) is investigating U.S. electronic payment service suppliers over the dispute in this practice. This treatment provides uniquely difficult conditions for U.S. companies compared to domestic competitors and warrants engagement from USG to ensure U.S. EPS companies can follow international best practices when serving the Turkish market.

Domestic card processing restrictions/TROY: On Sep. 6, 2026, the Government enacted its 2027-2029 Medium-Term Programme, which identified digital transformation, technology development and international investment attraction among its economic policy priorities. Among those priorities was to expand the use of the domestic card scheme TROY (Türkiye'nin Ödeme Yöntemi, or "Türkiye's Payment Method") and to finalize the infrastructure for the Digital Turkish Lira. Specifically, the Programme commits to work "to be carried out to increase the prevalence of the use of TROY." Although TROY began as an independently run association led by the domestic banks, the Central Bank now owns 51% of the conglomerate, and recent government actions have continued to put U.S. companies at a disadvantage in Türkiye, particularly for domestic processing. On Jan. 15, 2025, President Erdogan signed Presidential Circular No. 2025/1, titled "Use of Cards Issued by Card System Organizations Established and Licensed to Operate in Türkiye." The decree dictated that state-owned banks would issue cards linked to payment networks established and licensed to operate in Türkiye when providing new cards or replacing existing ones, unless a customer specifically requests otherwise. TROY is the only supplier licensed for domestic processing in Türkiye, thus providing less favorable treatment for U.S. companies, which are relegated to

only operating cross-border transactions. Further, all government payments were subsequently processed through TROY, including: personnel salary payments; retirement benefit payments; advance payments made via cards; social assistance payments; scholarship and student loan payments Incentive and support payments made to farmers, tradespeople, and professional groups; payments made via public transport, meal, identity, and student cards; and other payments made to beneficiaries under bank protocols and other payments covered by such protocols. These actions have resulted in TROY expanding significantly, inorganically, and undermining U.S. companies' presence in the market. Industry urges USG to engage Türkiye through available fora to promote interoperability and allow U.S. companies the ability to compete fairly.

Turkish Digital Lira: The Central Bank of the Republic of Türkiye continues work on the Digital Turkish Lira initiative, including pilot programs and cooperation with selected ecosystem participants. Industry encourages U.S. government monitoring of developments to ensure future participation opportunities are transparent, market-based, and available on a non-discriminatory basis to qualified domestic and international stakeholders.

Ukraine

Services Barriers

Cloud Law, Public Procurement Law, Public Electronic Registers Law, Information Protection Law, Law on Protection of Personal Data, National Bank of Ukraine Regulations: In 2022, Ukraine's Martial Law temporarily allowed U.S. cloud providers to serve the public sector. Once lifted, outdated legislation will re-impose pre-war barriers. In addition, under Cabinet of Ministers Resolution No. 154, cloud providers must register with the Government by December 2026. However, the process demands documentation impossible for global providers due to the nature of their business model and global infrastructure (e.g., proof of ownership of all infrastructure assets, software, and hardware). To date, only local Ukrainian companies have been able to register. A reform of the Ukrainian Cloud Law before the registration deadline would enable U.S. providers to register. A draft is pending in Parliament, but its outcome remains uncertain. Additional barriers include insufficient recognition of international security certifications, mandatory Ukrainian-law-only contracts, restrictions on foreign cloud providers processing public-sector personal data, post-martial-law data repatriation obligations, and a lack of regulatory predictability — with requirements changing multiple times in recent years, creating a chilling effect on long-term investment.

United Arab Emirates

Services Barriers

Data Localization and Sovereignty Requirements: The UAE Cyber Security Council mandates cloud services providers that serve the public sector and certain regulated industries to be solely subject to UAE law; not be subject to foreign jurisdiction and foreign laws; and physically localize data centers as well as engineering, security, maintenance, and support operations and respective personnel in the UAE. Similar localization requirements are now imposed on data processing for financial services and the healthcare sector: the UAE Central Bank's outsourcing guidelines ban financial services institutions—not including subsidiaries of foreign banks—from storing and processing personal data outside the country; and the UAE 2019 Health Law also obligates processors to conduct activities for health data within the UAE. Further, the Abu Dhabi Healthcare Information and Cyber Security Standard disallows hosting

information sharing systems on cloud services. The UAE Government's approach to data sovereignty for CSPs serving public sector and regulated industries has evolved with the publication of the National Cloud Security Policy by the UAE Cyber Security Council (CSC) in September 2025. The new policy allows foreign CSPs with infrastructure in the UAE to serve most government and regulated workloads, except for Secret and Top Secret classified data which must be hosted in fully sovereign infrastructure (e.g. Gov Cloud) with more stringent controls, including exclusive UAE jurisdiction, UAE-based Hardware Security Modules (HSMs), and denial by default of all foreign access requests. While this framework provides clearer pathways for foreign CSPs to serve government customers, informal preferences remain for local technology champions like G42, and ongoing data and infrastructure localization requirements continue to undermine U.S. providers from serving the private sector and regulated customers and serve as a barrier to market entry.

Security Approval Requirements for Aviation and Military Products - Under Federal Decree-Law No. 17 of 2019 on Weapons, Ammunition, Explosives, Military Materiel and Hazardous Substances and Federal Decree-Law No. 43 of 2021 on Goods Subject to Non-Proliferation, as further implemented through Cabinet Decision No. 97 of 2024, certain aviation-related, military, and strategic goods are subject to licensing and security approval requirements administered by competent UAE authorities, including the Executive Office for Control and Non-Proliferation (EOCNP). These requirements may result in additional administrative and compliance obligations, approval-related charges, and delays in the movement of affected shipments within the UAE, increasing operational costs and reducing supply chain flexibility for logistics providers.

Emiratization Requirements: Under the UAE's Emiratization programme, private-sector employers are required to meet prescribed Emirati employment targets, with larger companies expected to achieve a 10% Emirati workforce representation target by the end of 2026. Companies that fail to meet these targets may face financial penalties and other administrative consequences. These workforce localization requirements continue to increase recruitment, workforce planning, and compliance challenges for employers operating in the UAE, while increasing employment costs and limiting workforce flexibility.

Media Regulation: The UAE has introduced a new federal media regulatory framework under Federal Decree-Law No. 55 of 2023 on Media Regulation and Cabinet Resolution No. 68 of 2024 implementing the law, supplemented by further licensing, fee, and enforcement measures. The framework extends to electronic and digital media activities, while additional requirements affecting digital platforms continue to develop. U.S. industry welcomes the emerging risk-based approach reflected in more recent digital regulation and encourages this approach to continue as implementation develops, with greater clarity and proportionate differentiation among digital services based on their nature, functionality and risk profile, alongside continued stakeholder engagement.

The United Kingdom

Import Policies

UK CBAM: The United Kingdom is developing its own Carbon Border Adjustment Mechanism (CBAM), closely modeled on the European Union's system but with differences in pricing and scope. Announced in December 2023, the UK CBAM will apply to imports of carbon-intensive goods with implementation set for 2027. Unlike the EU's certificate-based model, the UK version imposes a levy directly on the importer, calculated to reflect the gap between the carbon price paid in the country of origin and the price that would have applied under the UK Emissions Trading Scheme (ETS) had the good been produced domestically — aiming to prevent carbon leakage. Because compliance liability

falls on the UK/EU importer rather than the foreign exporter, U.S. companies exporting into both markets will not bear the filing obligations directly, but they will face growing pressure from importer customers to supply accurate product-level emissions data — and differing calculation methods and reporting timelines between the two regimes will add complexity to that task. As details are still being finalized, the compliance burden for exporters may continue to shift.

Technical Barriers to Trade

Excessive revenue clawbacks (Medicines): UK revenue clawbacks on branded medicines have increased dramatically over the past several years, further reducing spending on already devalued medicines. While the UK commitment to cap the VPAG newer medicines rebate at 15% as part of the US-UK arrangement on pharmaceutical pricing is a step in the right direction, this remains much higher than peer countries. The UK Government should work with industry in the upcoming 2027 negotiation to ensure that clawback rates decline further, with the aim of full elimination in any future scheme. This should be monitored under the US-UK arrangement, considering the UK's commitment to invest 0.6% of GDP in innovative medicines by 2036.

Biased health technology assessment: Recent changes under the US-UK arrangement on pharmaceutical pricing to increase the NICE cost-effectiveness threshold to £25,000-35,000 per QALY, and introduce a new value set, are a welcome step in the right direction, with 10 new medicines approved in the first four months. The UK's pricing and HTA framework continues to rely on outdated cost-effectiveness thresholds and other cost-containment measures that limit the value placed on innovative medicines and slow patient access to new therapies. While the recent U.S.-UK pharmaceutical arrangement and related VPAG reforms, including modest increases to NICE thresholds and a temporary cap on clawback rates, are important first steps, further reforms are needed to ensure UK patients can access innovative medicines more quickly and that the UK more appropriately rewards pharmaceutical innovation. However, the United Kingdom still uses low and outdated monetary thresholds per life year gained from clinically proven treatments, which – despite the recent change – do not fully account for inflation since 1999 (depreciating a life year by more than 47% over the past 25 years). This means access to new medicines is still often restricted to a only a small subset of the population for which the regulator deems the product to be safe and effective, and access is denied completely for many treatments: just 33% of new medicines approved in Europe were made fully available to UK patients between 2021-24.¹³ The UK Government should ensure that the cost-effectiveness threshold is reviewed and updated annually to ensure it keeps pace with inflation, and enables the UK's commitment to invest 0.6% of GDP in innovative medicines by 2036. In addition, there has not yet been any change in the threshold used to assess centrally procured vaccines – this should be immediately updated in line with NICE's recent change to £25,000-35,000 per QALY.

Intellectual Property Protection

SPC Term Calculation: Following the UK's exit from the EU, one of industry's key IP incentives, the term of the supplementary protection certificate (SPC), has been linked to the date at which a medicine is granted marketing authorization (MA) in the UK or EEA/EU, whichever is first. This means that the term of some UK SPCs will be determined by decisions taken by the European medicines regulator, rather than the post-Brexit UK regulator (MHRA). This is inconsistent with other updates to post-Brexit pharmaceutical legislation in the UK which puts decision making solely in the power of UK authorities. It also means that if a company is granted MA in the EU prior to the UK, the term of protection in the UK is

¹³ <https://www.efpia.eu/media/mnfdwzax/efpia-patients-wait-indicator-2025.pdf>

calculated from a date before the company can sell the medicine in the UK market, reducing the effective duration of IP protection in the UK below that in European countries. The UK regulation on SPCs should be minimally amended to remove the reference to EU marketing authorization, so that only the UK MA is used in the calculation of the SPC term in the UK.

Service Barriers

Digital services tax: The UK maintains a 2% DST, applying to worldwide revenue above £500 million and UK revenue above £25 million from "digital services activity" — social media platforms, internet search engines, and online marketplaces. The UK Government has acknowledged that roughly 90% of the tax is paid by 5 digital-services companies, which USTR has previously identified in its Section 301 report as likely all American companies.

Digital Transformation Law (DTL): Vietnam is implementing a comprehensive digital regulation law that closely mirrors the EU's Digital Markets Act and Digital Services Act, but includes additional government-led compliance and data sovereignty elements that will likely disproportionately impact U.S. companies. The draft Digital Transformation Law (DTL) incorporates a wide range of distinct legal frameworks including consumer protection, data privacy, and algorithmic transparency obligations, new digital specific ex ante obligations, and new online safety obligations.

Digital Markets, Competition, and Consumers Act: The Digital Markets, Competition and Consumers Act (DMCCA) is a new competition framework that came into force in January 2025. It is designed to regulate digital markets by designating firms with 'Strategic Market Status' (SMS) and imposing behavioral requirements and 'pro-competition interventions'. The regime empowers the UK Competition and Markets Authority (CMA) to address alleged competition issues in digital markets, particularly focusing on companies with 'substantial and entrenched market power', 'strategic significance', and turnover thresholds of over £25 billion globally or £1 billion in the UK. This framework represents a shift from traditional ex post market investigations to permanent regulatory oversight, enabling the CMA to impose forward-looking conduct requirements on a small set of firms, overwhelmingly U.S. headquartered. These can include regulation of prices and other commercial terms allowing CMA to create transfers to domestic vested interests (including a final offer mechanism similar to the Australian news media bargaining code, but not limited by sector); requiring interoperability and data sharing; which services will be offered to consumers and how and when (e.g. choice screens) and restrictions in other areas such as how complaints are handled and how data is used. The CMA has also published "roadmaps" with potential conduct requirements. These would include many of the potential measures described above including speculative interventions regarding the integration of AI services. The breadth and potential impact of these measures has created considerable uncertainty for the services affected. In October 2025, the CMA made its first SMS designations, confirming both Apple and Google as having SMS across their mobile platforms (operating systems, app distribution, and browsers/browser engines), each for a five-year period. The regime represents a shift from ex post market investigations to permanent regulatory oversight, and the breadth of the CMA's discretion over which firms to designate and which conduct requirements to impose creates ongoing regulatory uncertainty for U.S. technology USTR should encourage the UK to make sensible changes to the regulatory regime, including: making compliance simplifications, undertaking a formal economic assessment and only intervening when it finds clear evidence of economic or competitive harm, base fines and fees on UK turnover (not global).

Online Safety Act: The OSA imposes duties on regulated user-to-user and search services, with the most onerous obligations reserved for the largest "Category 1" services. Following Ofcom's categorization process (final register published mid-2026), Category 1 comprises major social media, search, messaging

and video-sharing services. Online marketplaces were not designated Category 1, with several instead falling into the lighter Category 2B tier. The register is subject to ongoing review, and Ofcom retains discretion to re-categorize services as the market evolves — so continued monitoring is warranted to ensure lower-risk services such as marketplaces are not later drawn into disproportionate obligations.

Vietnam

Import Policies

Import / Export License Requirements for Encrypted ICT Products: Vietnam’s Government Cipher Committee (“GCC”) requires that the import and export of any product containing cryptographic functionality obtain specific permits and licenses. Suppliers importing and exporting IT products with regulated data encryption capabilities (civil cryptography products or “CCP”) must obtain a Cryptography Trading License (“CTL”) and a Cryptography Import License (“CIL”). These requirements are unfair because it takes several months to obtain CTLs and CILs, which is an inordinate amount of time. Detailed information needs to be submitted alongside the application, including detailed product information, defined technical plans, information regarding the equipment’s cryptographic functions, information regarding local personnel, and other material. In seeking to meet these requirements, companies often experience delays and inconsistent/non-transparent approvals or rejections by the GCC. These burdensome requirements, and the routine follow ups that the GCC requires, limit the ability of companies that invest in Vietnam to import critical hardware. A new regulation for cryptographic certification equipment, the Circular 23/2022/TT-BQP of the Ministry of Defense, has introduced further uncertainty.

In addition to the license required for CCP, since April 2024, Vietnam introduced an additional cyber information security licensing requirement for products designed with functions to maintain cyber information security. As such, products previously determined to be exempted from the CCP licensing now require a separate license from the Ministry of Information and Communication. The application process and required documentation are unclear, and initial applications for cyber information security trading license still remain pending approval. The dissolution of the Ministry of Information and Communication in February 2025 further adds to the confusion, as it is unclear if the license authority would be transferred to the Ministry of Public Safety or to the Ministry of Science and Technology. The vacuum of regulatory authority also creates uncertainty about how to obtain the necessary licenses to continue importing to Vietnam.

Prohibition on the Import of Refurbished Products: Vietnam maintains import prohibitions on certain used information technology (“IT”) products. While Decision 18/2016/QĐ-TTg eases import prohibitions on some used IT products, lenient treatment only applies provided that they meet various mandatory technical regulations and standards.

Prohibiting the import of refurbished products violates Vietnam’s international trade commitments. Products and components are essential in order to continue supporting customers with products that are under warranty, especially when such products have reached end-of-sale and components are no longer available as new products. In particular, critical infrastructure customers are unable to obtain replacement parts to service and maintain critical elements of their infrastructure without access to refurbished products.

Authorised Economic Operator: Vietnamese Customs is reported to be requesting that companies applying for the Authorised Economic Operator (AEO) compliance program are being asked to

accommodate onsite visits from a third party as a necessary precondition to be approved for the application. The program fee is reported to be US\$100K. U.S. tech companies have encountered this and engaged USTR to intervene, and were subsequently able to bypass the third party. Membership in a trusted trade program should not be preconditioned on the payment of a significant fee to a third party.

Proposed Postal Regulations as a Market Access Barrier: Vietnam's proposed Postal Law and implementing Decree could impose disproportionate and duplicative requirements on international express delivery providers, including obligations related to risk management, technology integration, data sharing, shipment controls, and X-ray image assessment. The draft also lacks clear distinctions among postal, express delivery, logistics, and freight-forwarding services, potentially subjecting express operators to additional requirements that do not apply to companies conducting similar activities. These measures could overlap with existing customs and aviation security regulations, increase compliance costs, delay time-sensitive shipments, and create an uneven competitive environment. USTR should urge Vietnam to clarify the scope of the proposed regulations, avoid duplicating existing customs and security requirements, ensure equivalent treatment of comparable service providers, and adopt risk-based, technology-neutral, and internationally aligned standards.

Technical Barriers to Trade

Civil Cryptography Trading and Import License Requirements: The Government Cipher Committee (GCC) requires that the importation and exportation of any product containing specific cryptographic functionality obtain specific licenses, i.e., a “Trading License” which is a business license valid for 10 years, and an import/export license for each product. Such licenses take months to obtain, sometimes due to unclear follow-up requests by the GCC. Companies have also experienced inconsistent/non-transparent approval or rejection of their applications. These burdensome requirements, and the required follow-ups by the applicants, limit the ability for companies investing in Vietnam to import/export critical hardware. The new regulation (Circular 23/2022/TT-BQP by Ministry of Defense) for cryptographic certification requirement was passed in 2022, but the Vietnamese government is still working through the enforcement mechanism, which will likely introduce additional burdens, more murky processes, and extended lead times for importers once it comes into force although its degree of complexity is unclear at this time. This will further hinder the ability of U.S. Cloud Service Providers (CSPs) to quickly deploy the latest cloud technologies in Vietnam.

Government Procurement

Government Procurement: Vietnamese government procurement policies favor lowest price bids instead of total cost of ownership and long-term performance factors, creating a challenge for U.S. companies to compete on value in public tenders.

Services Barriers

Electronic Payment Services: Domestic-routing mandate: Vietnam requires domestic card-present transactions involving internationally branded payment cards to be routed through a licensed domestic financial switching provider. Circular 18/2024/TT-NHNN, which took effect in July 2024, maintains the domestic-routing requirement previously established under Circular 28. As a result, international payment networks are unable to process domestic transactions through their global infrastructure and are limited in their ability to compete on the basis of security, innovation, service quality, resilience, and value-added services.

The licensing of MobiFone Digital Payments as an additional financial switching provider is a positive development and means the domestic switching market is no longer served exclusively by a single operator. Nevertheless, the underlying routing requirement remains in place and continues to restrict the ability of payment service providers and financial institutions to determine processing arrangements based on commercial and operational considerations.

The United States should encourage Vietnam to remove mandatory domestic routing requirements and allow financial institutions and payment service providers to choose payment processing arrangements based on commercial, security, operational resilience, and business considerations. Vietnam should pursue interoperability through open technical standards and network connectivity rather than routing mandates and ensure that any routing-related requirements are applied on a transparent, technology-neutral, and non-discriminatory basis.

Cybersecurity Law and Implementing Decrees (In Force): Vietnam's new Law on Cybersecurity (No. 116/2025/QH15), passed December 10, 2025, took effect July 1, 2026, replacing both the 2018 Law on Cybersecurity and the 2015 Law on Network Information Security. It introduces content-takedown and national-security obligations, identity-verification requirements, and rules governing AI-generated content on online platforms. Seven implementing decrees followed, effective August 19, 2026 (Decree 328 effective October 5, 2026). Among those most relevant to cross-border marketplaces: Decree 327/2026/NĐ-CP sets procedures for national-security-related content takedown and blocking; Decree 330/2026/NĐ-CP establishes the administrative sanctions and fine schedule; and Decree 333/2026/NĐ-CP (replacing Decree 53/2022/NĐ-CP) sets out general implementation measures, including local-presence and data-localization procedures.

New E-commerce Law and Implementing Decrees. Vietnam's National Assembly adopted the Law on E-Commerce (No. 122/2025/QH15) on December 10, 2025, and it took effect July 1, 2026. The law mandates that online platforms verify domestic sellers via VNeID and foreign sellers through legal documents, and extends oversight to livestream sales, affiliate marketing, and social media commerce. Implementing Decree No. 248/2026/NĐ-CP details these obligations: foreign e-commerce platforms operating in Vietnam must register and appoint an authorized local representative, maintain an escrow/security deposit arrangement, and comply with transparency and consumer-compensation rules. The law and decree also assign responsibilities to logistics, payments, and infrastructure providers, obliging them to work only with compliant platforms.

Competition Regulation: The Vietnam Competition Commission and Ministry of Industry and Trade are fast-tracking DMA-style provisions into existing competition law — draft text was unveiled in June 2026 and is expected to be pushed through the National Assembly. The proposed amendments function as prohibitions that only apply to technology companies, despite removing explicit "digital platform" terminology.

Domestic Processing Mandate (SBV Circular 18/2024/TT-NHNN): This circular, which replaces previous regulations, codifies and reinforces a discriminatory domestic processing mandate. It requires that all domestic card-present transactions conducted on the networks of U.S. electronic payments companies must be routed through the National Payment Corporation of Vietnam (NAPAS). This mandate limits competition, preventing U.S. companies from using their own global processing infrastructure for domestic transactions, and favors a state-owned entity, undermining the principles of national treatment.

Data Localization Requirements: There continue to be policy developments that mark a trend toward

data localization in Vietnam. Any changes mandating that foreign companies store data physically within Vietnam poses a significant threat to the country's economic competitiveness, risks derailing the government's digital transformation agenda, and could significantly diminish the country's position as a regional leader in the digital landscape. Examples include the Cybersecurity Law and (discussed above), and the following:

Data Law and its implementing decrees - Decree 165 and Decree 169: In November 2024, the National Assembly passed the Law on Data (No. 60/2024/QH15) (Data Law). The Law went into force together with its implementing Decrees 165 and 169 on 1 July 2025. The Law and its implementing decrees have duplications with the PDP Law on regulations on personal data governance. The Prime Minister Decision No. 20/2025 dated 1 July 2025 supporting the execution of the Data Law and its Decree introduces new categories of "important data" and "core data" similar to China's Data Security Law that can have chilling effects on foreign investors in Vietnam. The Data Law and Decree 165 impose onerous obligations on individuals and organizations for authenticating and ensuring the accuracy of created data as well as approvals for cross border transfers of core data. They also grant the government sweeping powers to requisition private data under vaguely defined "national interest" or "public interest" grounds, without clear due process safeguards. The Data Law and Decree 169 mandate licensing and regulating data products and services such as data intermediary, data analysis and aggregation products and services, and data exchange services. An implication of such requirements is that offshore enterprises not incorporated or registered in Vietnam would not be allowed to offer any of the above services to Vietnamese customers.

Data-Sector Administrative Sanctions: Decree No. 363/2026/NĐ-CP, effective November 11, 2026, establishes administrative sanctions for data-sector violations, including authority to suspend a platform's cross-border data transfers for a period ranging from three to twelve months — a sanction that would functionally halt in-country operations for an affected platform.

Draft Law on Data Security: Vietnam's Ministry of Public Security has released a Draft Law on Data Security that would establish the country's first standalone legal framework governing data security across the full data lifecycle, complementing the existing Data Law, Cybersecurity Law, and Personal Data Protection Law. As currently drafted, the law would introduce a four-tier data classification system, require real-time in-country backup and pre-approval for cross-border transfers of data classified as "Important" or "Core," and impose administrative penalties of up to 5 percent of global annual revenue for multinational violators. The law is expected to take effect December 1, 2027.

While the draft law is still evolving and said to have incorporated some industry inputs while no published draft is made available, there are still problematic issues caused by the overlapping and duplications with the Data Law, the Personal Data Protection Law, and the AI Law. This results in burdensome obligations for cross border providers, including required approval for cross border data transfers, assessment reports, information provision, logs and incident response cooperation, broad AI training-data requirements. As the leading cloud and AI providers in Vietnam, U.S. companies would bear the brunt. These provisions run counter to commitments under the CPTPP, EU-Vietnam FTA, and US-Vietnam bilateral frameworks.

Personal Data Protection Law: In June 2025, the National Assembly passed the Personal Data Protection Law - PDPL and released the draft implementing decree (draft PDPD) for public comments. The PDPL and draft PDPD regulate personal data processing in specific contexts (e.g., marketing, behavioral and targeted advertising, big data processing, AI, cloud computing, recruitment and employment monitoring, banking and finance, social networks and media services) as well as specific

categories of personal data (e.g., health and insurance data, location data, biometric data, credit data, children's data). The PDPL and the draft PDPD expanded their scopes beyond Decree 13/2023/ND-CP to include personal data of individuals residing in Vietnam, regardless of their nationality. The PDPL and draft PDPD impose onerous obligations on the processing of personal data as well as the transferring of personal data across borders. The PDPL also establishes stringent penalties for non-compliance, including administrative fines of up to 10 times the revenue generated from the unlawful sale of personal data, penalties of up to 5% of annual revenue for unauthorized cross-border data transfers, and fines up to VND3 billion (US\$115,000) for other infractions. These obligations would impede the ability of companies that need to process cross-border data from continuing to offer services to customers in Vietnam.

Electronic ID and Authentication Requirements: Decree No. 320/2026/NĐ-CP, effective September 28, 2026, requires e-commerce accounts to link to the national electronic identification (VNeID) system, creating new technical-integration and seller-onboarding obligations. A broader draft Law on Electronic Identification and Authentication, currently at Ministry of Justice appraisal stage, would amend the E-Commerce Law (No. 122/2025/QH15) and supersede Decree 320 upon passage.

National Digital Transformation Strategy – Domestic Preferences: Under its 2020 National Digital Transformation Strategy, Vietnam is implementing policies to control cross-border platforms and promote domestic industry. The government has issued cloud standards that offer preferential treatment to local providers for public sector projects, a move that is inconsistent with Vietnam's government procurement obligations under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Although technically voluntary, these standards are expected to be widely adopted, creating a significant advantage for Vietnamese firms in cloud computing and digital infrastructure.

Content Moderation: On November 9, 2024, the Vietnamese government issued Decree No. 147/2024/ND-CP on the Management, Provision, and Use of Internet Services and Online Information (Decree 147) replacing Decree No. 72/2013/ND-CP ("Decree No. 72") and imposing stringent requirements on foreign "Regulated Cross-Border Services" (over 100,000 monthly Vietnamese visits or local data center use). Decree 147 requires these entities/services to: appoint a local contact; store user data; remove flagged content within 24 hours; temporarily block content within 48 hours of complaints; and form "cooperation agreements" with Vietnamese press. Additional obligations include content scanning, child protection, and regular reporting. Social networks must verify accounts and restrict features, while app stores must comply with payment laws and remove government-requested apps. Decree 147 also prohibits cross-border online games, requiring foreign publishers to establish local entities and introduces a 16+ age rating. These rules create market entry barriers, expand state surveillance, increase compliance costs, and conflict with data minimization. ITI supports USTR's acknowledgment of these risks in its 2025 NTE report and urges continued U.S. engagement to counter measures undermining digital trade, user rights, and market access.

Law on Artificial Intelligence (In Force): Vietnam enacted the Law on Artificial Intelligence (Law No. 134/2025/QH15), effective March 1, 2026, followed by Decree 142/2026/ND-CP, effective May 1, 2026, and Decision 33/2026/QĐ-TTg (effective August 15, 2026) establishing the list of high-risk AI systems subject to the framework. The law establishes risk-based obligations concerning classification, conformity assessment, documentation, transparency, and oversight. Key concerns for digital platforms include short compliance timelines, broad "high-risk" classifications that may capture general-purpose or assistive AI (such as marketplace recommendation and search-ranking functions), mandatory conformity assessments that could duplicate internationally recognized certifications, and documentation requirements that risk exposing proprietary information.

Digital Services Taxes: The Tax Administration Law, effective July 1, 2020, cross-border e-commerce and other digital services. The Ministry of Finance issued Circular 80 providing guidance on the Law and its Decree 126 in September 2021. The Circular added a requirement for foreign digital service and e-commerce suppliers without a permanent establishment in Vietnam to directly register and pay taxes. If the foreign service providers do not register, service buyers (or commercial banks in case of individual buyers) will withhold tax from their payment to foreign suppliers at deemed tax rates. While the Law allows for certain exemptions under applicable tax treaties, digital suppliers who have sought such exemptions have faced onerous processes coupled with undue administration processing delays. The additional tax burden created by the deemed tax rates (Corporate Income Tax and Value Added Tax) will result in further complications and costs for cross-border service providers and conflict with international taxation rules.

Telecommunications Services: Vietnam permits foreign participation in the telecommunications sector, with varying equity limitations depending on the sub-sector. According to the Law on Telecommunications (Telecom Law) 41/2009/QH12, for domestic companies that provide basic telecommunication services with infrastructure, foreign ownership is generally capped at 49 percent; for companies that supply telecommunications services without infrastructure, foreign ownership is capped at 65 percent. Vietnam allows foreign ownership of up to 70 percent for virtual private network (VPN) services suppliers. Facilities-based operators are required to be state-controlled firms, meaning that the state, through the relevant line ministry, must hold 51 percent or more of equity.

The revised Telecom Law was passed by Vietnam's National Assembly on November 24, 2023, with a "light touch" regime for OTT, data center and cloud services. The Ministry of Information and Telecommunications (MIC) has drafted the Decree implementing the Telecom Law and sought industry's inputs. The final draft is under final review by the Government Office.

Video On Demand (VOD) Services: Vietnam maintains a burdensome and restrictive regime governing the provision of VOD services. It is the only market that requires two separate licenses to operate a VOD service with a full range of content offerings. To provide a full range of content, Vietnam requires streaming services to obtain licenses under both the Cinema Law and the new Press Law and its subsidiary Decree 242/2026/ND-CP (which replaced Decree 71). Under the Cinema Law, VOD services can apply for a license to self-classify scripted ("film") content. However, obtaining and maintaining the required self-classification license has been challenging for U.S. service suppliers. The regulatory regime for "non-film" content (including unscripted reality shows, talk shows, and live events/news) under the Press Law and Decree 242/2026/ND-CP includes very strict licensing requirements, including a joint venture or local presence requirement. Currently all foreign service providers have withdrawn non-film content from Vietnam. This licensing scheme severely hampers the provision of legal VOD services to Vietnamese consumers and indirectly contributes to online infringement.

Draft Circular Amending Consumer Protection Rules: Published for comment by the Ministry of Industry and Trade in September 2026, with the consultation window closing in mid-October 2026, this draft circular (implementing the Law on Protection of Consumer Rights) would maintain a 3-million-annual-active-user threshold for designating a "large digital platform" subject to enhanced obligations, including a short turnaround period for providing algorithm, AI, and seller-verification data to regulators on request, and new requirements to halt supply of recalled products within 24 hours and issue a public recall announcement within 3–5 working days depending on risk tier.

Amended Customs Law: Effective March 1, 2027, e-commerce platforms will be classified as customs declarants and required to connect their systems directly to Vietnam's customs data-processing system,

with automated tools used to assess compliance and risk for cross-border transactions.

Draft Decrees on Platform and Product-Quality Liability: Vietnam is separately developing draft decrees replacing Decree 51/2019/NĐ-CP (technology-transfer and IP-licensing sanctions) and Decree 119/2017/NĐ-CP (product-quality standards and platform liability), the latter of which would explicitly expand liability to digital platform operators for product quality, e-labelling, traceability, and seller data. Industry has urged a notice-and-takedown model over strict or vicarious platform liability, preservation of safe-harbor protection for procedurally compliant platforms, and avoidance of double penalties where product value is already regulated under sector-specific rules.

AI regulation in the banking sector: The State Bank of Vietnam has issued Circular 53/2026/TT-NHNN, establishing a risk-based framework for AI use in banking. The Circular sets relatively low thresholds for classifying automated payment and credit-decision systems as high-risk, which could affect the deployment of emerging U.S. technologies such as agentic commerce, automated payments, and AI-enabled credit solutions. While the removal of automated fraud-blocking systems from the high-risk category is positive, the framework also introduces significant governance, cybersecurity, human-oversight, and third-party requirements.

The United States should monitor implementation of Circular 53 and encourage Vietnam to apply its requirements in a proportionate, risk-based, and technology-neutral manner, with high-risk classifications based on the actual risks and impacts of AI use cases rather than transaction value alone. Implementation should also avoid unnecessary barriers to Vietnamese financial institutions' access to secure, and innovative AI technologies provided by U.S. companies.