Managing global telecom supply chains

What telecommunications companies need to know about trade control laws

Maintaining a global supply chain brings its share of commercial, financial, and regulatory risks. Increasingly, telecommunications companies with global operations and suppliers are finding that U.S. trade control laws affect their operations. For instance, telecommunications companies can inadvertently breach export control or economic sanctions laws when critical suppliers are designated on U.S. or non-U.S. government restricted parties lists, engage in prohibited transactions with sanctioned countries, or re-export U.S. origin items to prohibited destinations, end users, or end uses. In an interconnected world, even companies that primarily provide products and services within the U.S. can be exposed under trade control laws if they have a global supply chain. This article highlights the three areas of U.S. trade control laws that can affect the operations of U.S. telecommunications companies: export controls, economic sanctions, and anti-boycott restrictions. With U.S. and non-U.S. trade control laws constantly evolving as U.S. foreign and national security policies react to global developments, U.S. telecommunications companies need to remain alert to potential risks in their global activities and implement robust compliance programs to be prepared for sudden shifts in U.S. policy and/or legal requirements.

U.S. export controls laws

U.S. export controls laws govern how U.S. companies may export and re-export items to specified destinations and end-users around the world. These rules apply to dealings with third parties, as well as intra-company transfers. The export, re-export, and transfer of certain U.S. origin commodities, software, and technology requires authorization by the U.S. government and other procedures, even for transfers to U.S. company's own affiliates and suppliers outside the United States. While most commercial telecommunications items are not highly controlled, there are certain items that require prior authorization. Therefore, it is critical for telecommunications companies to understand how their commodities, software, and technology are controlled. Major companies in the global supply chain for telecommunications and computer networking equipment have been targeted by export enforcement agencies, raising legal risks for U.S. companies who rely on their products and services.

U.S. commercial and dual-use items are governed by export control rules set forth in the Export Administration Regulations (EAR), which are administered by the Commerce Department's Bureau of Industry and Security (BIS). The list of items controlled by the EAR is extensive, covering commodities and software as well as technology, which includes specific information necessary for the production, development, or use of a commodity or software (e.g., blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering specifications, and documentation such as manuals, written instructions, or recorded on devices such as a disk, tape, or read-only memories). Technical collaboration and testing data is also controlled

by the EAR. The EAR applies to U.S. origin items wherever they are located, items that transit the U.S., and non-U.S. origin items that contain greater than a de minimis amount of controlled U.S. origin content. Product-based controls will depend on an item or technology's Export Classification Control Number (ECCN) as determined by review of the Commerce Control List (CCL) in the EAR. Items that are not specifically listed on the CCL, including many telecommunications products, are classified in the "basket" category of EAR99 and are subject to minimal export controls limiting their transfer to sanctioned countries or restricted parties. However, certain telecommunications equipment, software and technology are specifically listed on the CCL and may require export licenses to transfer across borders:

- Certain advanced electronics, such as analogue to digital converters and semiconductor manufacturing equipment, are specifically listed on the CCL because their export implicates national security concerns. Depending on the final destinations of these goods and services, exports of these items – and technology for their development or production – require a license from the Commerce Department
- Certain telecommunications devices that are specially designed to withstand electromagnetic pulse effects or hardened against radiation are controlled and requires export licenses for certain countries
- Certain devices primarily useful for the surreptitious interception of wire, oral, or electronic communications are controlled and require export licenses for certain countries
- Encryption devices, software, source code and technology, especially those employing algorithms that exceed 64-bit in key length, are subject to export controls, and exports of such items may require notification or prior authorization

The release of controlled U.S. origin technology or source code to foreign persons in the U.S. counts as a "deemed export," even if it happens inside the U.S.. Accordingly, software patches or transfers of technical data may need a license, depending on the controls on the underlying technology and who is on the other side of the transaction. An oral exchange of information or visual inspection of an item or data may count as a "deemed export" under Commerce Department regulations.

The EAR also imposes controls on certain end uses or end users, regardless of the level of control of the item at issue; therefore, companies have to be alert to who will receive their items and why. For instance, items may not be exported or re-exported for illicit uses, such as when a company has reason to know that they will be used in nuclear, missile, chemical, and/or biological weapons activities.

The Commerce Department also imposes restrictions on who may receive U.S. exports. The Department of Commerce adds entities or individuals to the Entity List, Denied Persons List

and the Unverified List when the U.S. government determines they pose a significant risk to U.S. national security or foreign policy interests, or pose a significant risk of diversion. If an international business partner is listed, engaging in certain transactions with these partners immediately may become violations of U.S. law. Companies generally may not export or re-export to such restricted parties without an export license from the Commerce Department.

For instance, when a foreign company is listed on the Entity List, the Commerce Department may specify that licenses are only necessary for exports of specific items controlled under the EAR. More often, though, all exports of items subject to the EAR to the listed entities will need a license—a requirement that can reach farther than one might expect. If a company knows there is a listed entity in their supply chain that will receive their products or technology, they will need to get a license for the export. If companies continue to export or re-export controlled items to listed entities without a license, they risk criminal and/or civil penalties.

Telecommunications companies with supply-chain relationships with the U.S. subsidiaries of foreign companies need to be particularly cautious about how those U.S. subsidiaries relate to their foreign parent. If the foreign parent is listed on the Entity List or the product is subject to export controls, companies should understand the

flow of technology and items between the U.S. subsidiary and the foreign parent to confirm there are no potential export control violations as part of the intracompany supply chain and ensure no prohibited foreign persons are involved at any stage of the U.S. subsidiaries' operations (e.g., a listed foreign parent has employees working in U.S. laboratories or manufacturing facilities run by its U.S. subsidiaries).

There are also certain circumstances that the Commerce Department identifies as "red flags" requiring additional investigation and due diligence. Under the EAR's Know Your Customer Guidelines, if a buyer or business partner is reluctant to offer information about the end use of an item or is evasive about whether the product is for domestic use, export, or re-export, a company is required to take additional steps to confirm their reliability before proceeding with the transaction. Other red flags include counterparties willing to pay cash when the terms of the sale call for financing, vague delivery dates, out-of-the-way destinations, and abnormal shipping routes. The current complete list of circumstances that should be viewed as "red flags" is available on BIS' website.

U.S. economic sanctions laws

U.S. economic sanctions laws prohibit U.S. companies from engaging in transactions and dealings with certain countries, entities and individuals for foreign policy reasons. However, because of the special role of the internet and mobile devices in promoting free speech and democratic values, the U.S. government permits telecommunications companies to engage in certain limited activities with sanctioned country markets.

There are currently six countries or regions subject to comprehensive U.S. sanctions: the Crimea region, Cuba, Iran, North Korea, Sudan, and Syria. More than twenty other U.S. sanctions regimes administered by the Treasury Department's Office of Foreign Assets Control (OFAC) impose targeted prohibitions on transactions with certain countries, sectors, or persons. Under the comprehensive sanctions regimes, U.S. persons are broadly prohibited from transacting or dealing, directly or indirectly, with a sanctioned country and nationals of such country. The U.S. government provides for a series of exceptions or general licenses for certain limited activities that are in the interest of U.S. foreign policy, including humanitarian or democracy-promoting activities. Some sanctions regimes, like the Cuba embargo, have exceptions and general licenses that allow for more substantial U.S. involvement in the local market. Others, like the sanctions on Iran or Crimea, limit exceptions to narrow humanitarian and communications needs.

Each program is different, creating its own pitfalls and potential opportunities. Companies seeking to directly engage in sanctioned markets must ensure their proposed activities strictly adhere to the bounds of the relevant licenses, or they risk civil or criminal penalties.

There are also certain individuals and entities with which U.S. companies may not transact. The Treasury Department maintains a list identifying certain persons and entities because they are affiliated with sanctioned countries or because they acted against U.S. interests in some way, such as supporting terrorism or violating human rights. U.S. persons risk criminal and/or civil penalties if they transact with Specially Designated Nationals (SDNs), Foreign Sanctions Evaders (FSEs), or Sectoral Sanctions Identifications List (SSIL) designees without a license from OFAC. SDNs, FSEs, and SSIL designees may be located in any country in the world, not just sanctioned countries. In addition to persons and entities expressly identified on these lists, entities owned 50% or more by persons and entities on the lists are also subject to restriction, making it imperative for U.S. companies to fully understand who their customers and business partners are.

Special considerations for telecommunications companies

Telecommunications companies may be eligible for certain licenses set forth in OFAC's sanctions regulations. A number of the sanctioned countries have governments that repress freedom of expression and civil liberties, and the U.S. government sees foreign policy benefits to expanding personal communications with these countries in the hope of spurring democratic development. General licenses allow specified transactions for internet or telecommunications purposes under all the territorial sanctions regimes except North Korea. For example, even though most U.S. persons are prohibited from engaging in virtually any transaction with Iran, General License D-1 authorizes certain services, software, and hardware incident to personal communications, provided that such services and items are not intended for use by the Government of Iran or persons whose property or interests in property are blocked. Specifically, General License D-1 authorizes the export of certain fee-based services such as instant messaging, chat and email, social networking, sharing of photos and movies, web browsing, and blogging, certain fee-based software necessary to enable such services, and certain other software and hardware including mobile phones, consumer modems, WiFi access points, laptops, tablets, anti-virus software, anti-censorship tools and related software, and Virtual Private Network (VPN) client software—provided that such hardware and software have been designated under specified categories of the EAR's CCL. U.S. companies utilizing General License D-1 must strictly adhere to the terms of the license.

Similarly, as part of President Obama's new policy direction for Cuba, OFAC has authorized certain telecommunications services, including data, telephone, internet connectivity, radio, television, and news wire feeds, provided to individuals in Cuba, so long as such individuals are not prohibited Cuban government officials or prohibited members of the Cuban Communist Party. This general license authorizes transactions

to establish facilities for the purpose of establishing commercial telecommunications services between Cuba and third countries, as well as authorizing U.S. companies to provide certain internet-based services to Cuba, including certain web hosting, software design, business consulting, information technology management services, and installation and repair services.

As discussed above, general licenses for the provision of telecommunications services exist for other countries and regions, such as Sudan and Crimea. Each region comes with a slightly different set of rules. Some general licenses allow exports of social media applications but not devices; others allow exports but not marketing. Importantly, the general licenses still prohibit transactions with persons on the Treasury Department restricted party lists, such as SDNs and FSEs—the same persons who are sometimes key players in the local telecommunications sector.

Telecommunications companies seeking to take advantage of the general licenses should:

1. Carefully review the general license terms to confirm the specific requirements for compliance under that specific program.
2. Fully vet all of their counterparties to ensure no prohibited persons or entities are involved.
3. If a general license does not cover the proposed activity or if there is some question about whether an activity will expand beyond the scope of a general license, companies may apply for a specific license.

Licensing under U.S. sanctions regimes is usually controlled by OFAC. OFAC will often seek input on requests from the U.S. State Department, which will take into account whether the proposed activity promotes U.S. foreign policy goals like democracy promotion.

U.S. anti-boycott laws

Under U.S. anti-boycott laws, which are implemented both by the Commerce Department and the Internal Revenue Service, U.S. companies may not agree to cooperate with international boycotts that the United States does not support, such as the boycott of Israel by the Arab League. For example, U.S. companies may not enter into contracts, whether oral or written, that prohibit shipments on vessels that call at Israeli ports or certify that goods are not of Israeli origin. Other prohibited terms include agreeing not to do business with a distributor with Jewish employees or confirming that a company has no Israeli operations or Jewish board members. Boycott-related requests may appear as provisions in a proposed bid invitation, contract, purchase order, letter of credit or other agreement. Even agreeing to comply with the laws of a boycotting country can violate U.S. anti-boycott laws.

Companies that receive requests for such commitments may be required to report the request to the U.S. government under certain circumstances, even if they do not respond to the request. While receipt of boycott-related language or requests will not necessarily prohibit a transaction from progressing, additional steps like amending the contract or reporting to the U.S. government may be required to process the transaction.

In sum, especially when doing business in the Middle East, U.S. companies must be aware of and sensitive to boycott-related requests from customers, suppliers and other business partners.

Conclusion

As supply chains and product development become more and more globalized, telecommunications companies, including those that are focused on the U.S. market, are increasingly subject to a range of trade control laws that affect their operations and activities. Given the complexity of the export control, economic sanctions and anti-boycott laws, it is critical that telecommunications companies consider their trade control risks and implement robust compliance programs to manage these risks.

Ajay Kuntamukkala
Partner, Washington, D.C.
T +1 202 637 5552
ajay.kuntamukkala@hoganlovells.com

Stephenie Gosnell Handler
Associate, Washington, D.C.
T +1 202 637 5540
stephenie.gosnellhandler@hoganlovells.com