SEC Issues Disclosure Guidance on Risks to Intellectual Property and Technology Associated With International Business Operations

January 6, 2020

On December 19, the staff of the Securities and Exchange Commission released **interpretive guidance** for companies to consider on an ongoing basis with respect to risks to intellectual property and technology arising from international operations. This guidance expands on earlier cybersecurity risk **guidance** by focusing on business conducted outside the United States, particularly in jurisdictions that may not have comparable levels of protection for corporate assets such as intellectual property, trademarks, trade secrets, know-how and customer information and records. The new guidance does not create a line-item disclosure requirement, but instead indicates that the disclosures of these risks should be assessed in light of overall materiality. According to the SEC staff, disclosure may be needed in various places in a company's periodic reports, including in MD&A, the business section, legal proceedings, disclosure controls and procedures, and financial statements.

Sources of Risk

The guidance identifies both direct and indirect sources of risks of theft of, or compromises to, technology, data and intellectual property. Direct sources of risks include cyber intrusion and corporate espionage by private parties and foreign actors, including state actors.

Indirect risks could arise from reverse engineering by joint venture partners or others, and infringement of patents or theft of know-how or trade secrets. In addition, the SEC notes that companies may be required to compromise protection of, or yield rights to, technology, data or intellectual property in order to conduct business in one or more foreign jurisdictions through agreements with foreign entities or due to legal or administrative requirements imposed by foreign jurisdictions. This could impede the company's ability to compete currently and in the future. The guidance provides several examples of what it terms indirect intrusion:

- Patent license agreements pursuant to which a foreign licensee retains rights to improvements on the relevant technology, including the ability to sever such improvements and receive a separate patent, and the right to continued use of technology or intellectual property after the patent or license term of use expires.
- Foreign ownership restrictions, such as joint venture requirements and foreign investment restrictions that potentially compromise control over a company's technology and proprietary information.
- Use of unusual or idiosyncratic terms favoring foreign entities, including those associated with a foreign government, in technology license agreements, such as access and license provisions, as direct or indirect conditions to conducting business in the foreign jurisdiction.
- Regulatory requirements that restrict the ability of companies to conduct business, unless they agree to store data locally, use local services or technology in connection with their international operations, or comply with local licensing or administrative approvals that involve the sharing of intellectual property.

Assessing and Disclosing Risk

In assessing risks related to the potential theft or compromise of technology, data or intellectual property, the guidance encourages companies to focus on how realization of these risks may impact their business,

financial condition and results of operations, and any effects on reputation, stock price and long-term value. The SEC emphasized that in instances where a company's technology, data or intellectual property has already been materially compromised, its disclosure obligations would not be satisfied by statements that an intrusion could or might hypothetically occur.

The guidance suggests the following questions to consider:

- Is there a heightened risk to the company's technology or intellectual property because it has or expects to maintain significant assets or earn a material amount of revenue abroad?
- Does the company operate in an industry or foreign jurisdiction that has caused, or may cause, it to be particularly susceptible to the theft of technology or intellectual property or the forced transfer of technology? Does the company believe that its products have been, or may be, subject to counterfeit and sale, including through e-commerce?
- Has the company directly or indirectly transferred or licensed technology or intellectual property to a foreign entity or government, such as through the creation of a joint venture with a foreign entity? Does the company store technology or intellectual property locally in a foreign jurisdiction? Is the company required to use equipment and services provided by a state actor, including equipment or services that could result in a reduction in protections?
- Has the company entered into a patent or technology license agreement with a foreign entity or government that provides such entity with rights to improvements on the underlying technology and/or rights to continued use of the technology following the licensing term, including in connection with a joint venture?
- Is the company subject to a requirement that foreign parties must be controlling shareholders or hold a majority of shares in a joint venture in which it is involved, or is the company involved in a joint venture that is subject to foreign ownership restrictions or requirements that a foreign party retain certain ownership rights?
- Has the company provided access to its technology or intellectual property to a state actor or regulator in connection with foreign regulatory or licensing procedures, including but not limited to local licensing and administrative procedures?
- Has the company been required to yield rights to technology or intellectual property as a condition to conducting business in or accessing markets located in a foreign jurisdiction?
- Is the company operating in foreign jurisdictions where the ability to enforce rights over intellectual property is limited as a statutory or practical matter?
- Does the company conduct business in a foreign jurisdiction or through a joint venture that may be subject to state secrecy or other laws, such as those limiting or prohibiting the export of data or financial documentation? Is the company able to readily produce data or other information that is housed internationally in response to regulatory requirements or inquiries?
- Have conditions in a foreign jurisdiction caused the company to relocate or consider relocating its operations to a different host nation? Has the company considered related material costs, such as costs to train new employees, establish new facilities and supply chains, and the impact of any related gaps or lags in production, manufacture and/or export of its products?
- Does the company have controls and procedures in place to adequately protect technology and intellectual property from potential compromise or theft? Do these policies and procedures enable the company to identify risks and incidents, analyze the impact on its business, respond expediently, appropriately and effectively when incidents occur and repair any damage caused by such incidents? Are the company's controls and procedures designed to detect:

  - malfeasance by employees, contractors or other insiders who may have access to the company's technology and intellectual property;
  - industrial, corporate or other espionage events;
  - unauthorized intrusions into commercial computer networks; and
  - other forms of theft and cyber-theft of the company's technology and intellectual property?
- What level of risk oversight and management does the board of directors and executive officers have with regard to the company's data, technology and intellectual property and how these assets may be impacted by operations in foreign jurisdictions where they may be subject to additional risks? What knowledge do these individuals have about these risks and what role do they have in responding if and when an issue arises?

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

David R. Bauer		212 450 4995	david.bauer@davispolk.com
Maurice Blanco		212 450 4086	maurice.blanco@davispolk.com
Alan Denenberg		650 752 2004	alan.denenberg@davispolk.com
Marcel Fausten		212 450 4389	marcel.fausten@davispolk.com
Joseph A. Hall		212 450 4565	joseph.hall@davispolk.com
Michael Kaplan		212 450 4111	michael.kaplan@davispolk.com
James C. Lin	+	852 2533 3368	james.lin@davispolk.com
Byron Rooney		212 450 4658	byron.rooney@davispolk.com
Richard D. Truesdell, Jr.		212 450 4674	richard.truesdell@davispolk.com
Elizabeth S. Weinstein		212 450 3889	elizabeth.weinstein@davispolk.com