SQUIRE SANDERS | LEGAL COUNSEL WORLDWIDE

INTERNATIONAL TRADE & TECHNOLOGY TRANSFER (IT^3) UPDATE

Squire, Sanders & Dempsey L.L.P.

Fall 2009

Global Markets Need Global Counsel

With 32 offices in 15 countries, Squire, Sanders & Dempsey L.L.P. is the first choice for international trade legal advice. Squire, Sanders & Dempsey L.L.P. has an exceptional depth of experience in successfully dealing with the full spectrum of complex trade issues in the United States and in Europe, Asia, Latin America and the Middle East. Our lawyers assist clients with:

- Export controls, sanctions and technology transfer
- Customs and trade remedies
- Market access
- International government contracting
- Investment in the US defense and critical infrastructure industrial base by entities outside the United States

www.ssd.com

Stepped Up Trade Regulation Enforcement Against Non-US Persons: A Growing Trend or a Flash in the Pan?

Non-US citizens living and doing business outside the Untied States and business entities located and organized in other countries often find it difficult to understand how their wholly non-US sales and other commercial transactions could possibly be subject to US export controls and economic sanctions programs. The fact is US export controls and economic sanctions programs have broad application outside the United States. Transactions involving dual-use items controlled under the Export Administration Regulations (EAR) and defense articles subject to the International Traffic in Arms Regulations (ITAR) can require approvals from the Department of Commerce or the Department of State if, for example, US-origin goods are re-exported from one foreign country to another foreign country, even if the subject transaction is conducted entirely by non-US persons operating outside the United States. Foreign-made products also may be subject to such approvals if they contain US content or are derived from US technology. Similarly, US country-specific economic sanctions administered by the Treasury Department's Office of Foreign Assets Control (OFAC) can apply to non-US companies and persons. For example, OFAC's Iranian Transactions Regulations prohibit re-exports to Iran by non-US persons of US-origin goods and services, and the Cuban Assets Control Regulations, which generally prohibit trade and other dealings with Cuba and Cuban nationals, expressly apply to the non-US subsidiaries of US companies.

Non-US companies violating US trade restrictions might also question how, as a practical matter, the United States can enforce its export control and economic sanctions regulations against them. Indeed, the difficulty in obtaining jurisdiction over non-US persons generally has meant that the "penalty" for such violations has been to add the foreign person to a denied parties list, such as OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List). US persons are prohibited from having dealings with any person or entity on the SDN List, thus potentially imposing an economic hardship on the SDN.

Based on the following examples, efforts by US agencies and courts to move more directly against non-US companies involved in activities considered noncompliant with US export controls and economic sanctions programs appear to be growing.

- The Department of Commerce Bureau of Industry and Security's (BIS) Major Cases List reports that on July 17, 2008 a France-based company, Cryostar SAS, formerly known as Cryostar France, was sentenced in the US District for the District of Columbia to a US$500,000 criminal fine and two years of probation for its involvement in a conspiracy to illegally export US-origin cryogenic submersible pumps to Iran. On April 10, 2008 Cryostar pled guilty to three felony counts charging one count of conspiracy, one count of export without an export license and one count of attempted export without an export license. The conspirators, Cryostar France, a US company and another France-based company, developed a plan to conceal the export of cryogenic pumps to Iran. The US company would sell and export the pumps to Cryostar France, which would then resell the pumps to another company from France, with the ultimate and intended destination being the 9th and 10th Olefin Petrochemical Complexes in Iran.
- Qioptiq S.a.r.l., a Luxembourg-based optics company, entered into a consent agreement with the State Department's Directorate of Defense Trade Controls (DDTC) this past December agreeing to pay US$25 million in fines and remedial compliance measures to settle 163 alleged violations of the ITAR. The violations involved unauthorized exports and re-exports of military-grade night vision components and technical data without required licenses from the DDTC, which were committed by certain Thales High Technology Optic Group companies and their predecessors prior to Qioptiq's acquisition from Thales France in December 2005. The

DDTC has long said that it considers an acquiring company to be strictly liable for export violations committed by the acquired company. Some of the unauthorized transfers and retransfers of technical data arose in connection with a technical assistance agreement (TAA) between US-based Thales Optem Inc. and Singapore-based Thales Electro-Optics Pte Limited. First, the US company started exporting technical data to the Singapore company prior to the execution of the TAA. Second, the US company exported enhanced night vision goggle (ENVG) technical data of ITT Night Vision, which was outside the scope of technical data to be transferred under the TAA. Moreover, the US company concealed the ENVG exports by marking the technical data as SNVG (special night vision goggle). An email to the Singapore company uncovered by the DDTC stating that the SNVG label was a "decoy" bolstered the DDTC's charge of misrepresentation and omission of facts regarding these transactions allegedly made under the TAA.

- On January 9, 2009 Lloyds TSB Bank plc entered into a deferred prosecution agreement with the Department of Justice (DOJ) in which Lloyds agreed to pay US$350 million for violating OFAC's trade sanctions against Iran and Sudan. The bank's actions that triggered the case involved "stripping" information from US dollar payment instructions, so-called SWIFT messages, that would have revealed to US banks that US dollar payments originated by Lloyds were for certain of its Iran- and Sudan-based customers. This conduct, according to the charges, resulted in willful exportation of services from the United States to Iran and Sudan prohibited by US economic sanctions regulations. Although none of Lloyds' US branches were involved, the DOJ viewed Lloyds' use of US banks to service its customers in Iran and Sudan as constituting an export of services from the United States by Lloyds.

Free ITAR HANDBOOK Download From Squire Sanders' International Transaction Regulations, Export Controls & Customs Practice

Squire Sanders offers a global solution to address the regulation of imports, exports and cross-border transactions. To guide our clients through this complex system, we have created an ITAR Handbook, including the complete ITAR, a primer on the ITAR and government personnel phonebook, available at no charge on our **International Transaction Regulations, Export Controls & Customs** page at ssd.com/international_trade.

One-Year Review of the Revised Encryption Regulations in Practice

Last year BIS, in an "interim rule," amended the rules governing the export and reexport of encryption items in the EAR. The revisions were more form than substance in that the majority of the changes focused on restructuring and simplifying the encryption rules, particularly License Exception ENC, which is now organized by whether a review, waiting period or reporting is required.

However, BIS eased, although only to a limited extent, the restrictions on encryption exports by removing the notification requirements for low strength encryption items, increasing the symmetric key length thresholds for exemption from the 30-day waiting period, adding to the list of countries that receive favorable treatment under License Exception ENC and adding new exclusions to the reporting and review requirements. The chart on page 6 provides a summary of License Exception ENC as revised by last year's interim rule.

Self-Classification as 5x992 and Using License Exception ENC

Prior to analyzing whether License Exception ENC is applicable to one's export, one should first analyze whether a self-classification exclusion applies. The following encryption items can be self-classified (i.e., without review) as

5A992, 5D992 or 5E992 and exported under the designation of No License Required (NLR): (1) items with limited cryptographic functionality[1]; (2) items with key lengths not exceeding 56, 512 or 112 bits for symmetric, asymmetric and elliptic curve algorithms, respectively[2]; or (3) mass market items with a symmetric key length that does not exceed 64 bits[3]. The interim rule eliminated the notification requirements for exports classified as 5A992, 5D992 or 5E992.

Exporters may also be able to rely on another license exception rather than using License Exception ENC, such as one of the following: LVS for shipments of limited value (§ 740.3); TMP for certain temporary exports (§ 740.9); RPL for replacement parts (§ 740.10); GOV for US government use (§ 740.11); TSU for unrestricted technology and software (§ 740.13); and BAG for temporary exports used in travel (§ 740.14). Some of these license exceptions may be less restrictive than License Exception ENC (e.g., immediate authorization of an export rather than a 30-day waiting period or the avoidance of License Exception ENC's reporting requirements).

However, if the product cannot be self-classified under one of the three criteria discussed above, the exporter may still be able to rely on one of the self-classification provisions of License Exception ENC, which are set forth in the chart on page 6. An exporter may also rely on the "internal development or production of new products" or "US subsidiaries" provisions to avoid filing a review. If none of these authorizations applies, then the exporter will have to file an encryption review request for mass market encryption or License Exception ENC and rely on the license exceptions contained in § 740.17(b) of the EAR. Under the new regulations, exports pending mass market review may no be longer exported as 5A992, 5B992 or 5D992. Rather they must be exported as 5A002, 5B002 or 5D002 using License Exception ENC.

Modifications to Previously Reviewed Encryption Items

The interim rule moves language from the interpretation section in Part 770 of the EAR to a new note in § 740.17(b) and also into the text of § 742.15(b) in order to highlight that a new product review may be required when a change has occurred in the encryption product. These sections point out that any change made to "the cryptographic functionality (e.g., algorithms) or other technical characteristics affecting mass market eligibility (e.g., performance enhancements to provide network infrastructure services, or customizations to end-user specifications) of the originally reviewed product" will cause the modified product to be treated as a new product for the purpose of the regulations and thus will require a new review request. However, if the change involves only a name change, an update of the encryption software components (e.g., an update to a third-party encryption library) where the product is otherwise unchanged, or the subsequent bundling, patches, upgrades or releases of a product, the modified product will not require a new review.

If the only modification to a previously reviewed product is a key length increase, then a new review is not required. Key length increases require the exporter only to file (prior to exporting the product) a notification of the key length increase, a certification that no other change to the encryption functionality was made and the CCATS number for the originally reviewed product. However, key length increases to items not previously reviewed but exported under another exclusion (e.g., a mass market item with 64 bits or less symmetric encryption) may require a review request if the increase exceeds a certain key length threshold (e.g., symmetric encryption increased from 64 to 128 bits).

[1] *See* Control Note in 5A002, ECCN 5A002.a.1, and Technical Note to ECCN 5A002.a.1. Items with limited cryptography include the following: items that only perform cryptography related to authentication, password protection or digital signature; personalized smart cards; and items specially designed and limited to banking use or money transactions or to perform copyright protection, wireless telephone without end-to-end encryption and client wireless devices. *See id.*
[2] *See* ECCN 5A002.a.1.a–b.
[3] *See* Cryptography Note to Category 5, Part 2.

New Regulations in Practice – Ancillary Cryptography

BIS added a new review requirement exclusion for items performing ancillary cryptography, which was apparently intended to reduce the volume of requests, that has broad appeal to exporters but has created some uncertainty in its application.

Ancillary cryptography is the use of cryptography by items that are "not primarily useful for" computing, communications, networking or information security. Examples of items that perform ancillary cryptography include commodities and software that are "specially designed and limited to": piracy and theft prevention for software and music; video games; household utilities and appliances; printing, reproduction, imaging and video recording; business process modeling and automation; industrial manufacturing or mechanical systems; and automotive, aviation and other transportation systems.

Exporters may self-classify items they deem to perform ancillary cryptography. However, determining whether a product performs ancillary cryptography is not always clear. For example, an industrial computer specially designed for industrial manufacturing systems may also be used in other areas not explicitly identified in the regulations, such as power distribution or the control of wastewater systems. The qualifier "specially designed and limited to" provides uncertainty as to whether an industrial computer must be limited to use only in an industrial manufacturing system or whether it may be used in other industrial applications. Moreover, the regulations do not establish whether the list of examples of ancillary cryptography items is exhaustive or provide any guidance as to what other types of items perform ancillary cryptography.

In order to achieve certainty, many manufacturers and exporters have decided to forgo self-classification and file encryption reviews that formally request BIS to determine whether the ancillary cryptography exclusion applies to their product. Other manufacturers have ignored the ancillary cryptography exclusion altogether, finding it easier to submit a traditional mass market review request.

Conclusion

Despite the October 3, 2008 revisions' improvements with respect to the structure and readability of the encryption regulations, the application of the rules retains its complexity.

COPING WITH EXPORT CONTROLS IN MIXED COMMERCIAL AND MILITARY BUSINESS: "TURNING THE ITAR ON ITS EAR"

28 October 2009
8:30 a.m. – 6 p.m.

Companies dealing in both military and dual-use items face complicated export controls issues including determining the appropriate export licensing jurisdiction for their products and technology. Please join us for a one-day workshop on the application of ITAR and EAR to mixed military and dual-use products at the Westin Tysons Corner in Falls Church, Virginia. This event will take place in a collaborative, workshop environment where attendees will gain an understanding of the government's perspective (State and Commerce) and learn from industry leaders and export controls lawyers.

Robert S. Kovac, Managing Director of Defense Trade Controls, US Department of State, Directorate of Defense Trade Controls is providing the keynote address. In addition, there will be a Commodity Jurisdiction Panel Discussion with government officials from the Departments of Commerce, State and Defense.

The cost of attendance is US$199.

Registration is available at the event website, http://www.regonline.com/Checkin.asp?EventId=762704.

Summary of License Exception ENC

Authority (§ 740.17)	Description of License Exception[1]	Review Required	Waiting Period	Reporting Required
(a)(1)[2]	Exports to **private sector end-users** located anywhere (except E:1 countries) that are headquartered in a country listed in Supplement No. 3 to Part 740 of the EAR (Supp. 3 Country), but only if such exports are used for **internal development** or the **manufacture of new products** by the end-user.	No	N/A	No
(a)(2)[2]	Exports to **US subsidiaries** or **employees of a US subsidiary** located anywhere (except E:1 countries) but only for **internal company** use, which includes the development of new products.	No	N/A	No
(b)(1)(i)[3]	• Encryption commodities and software to **private companies** located in **Supp. 3 Countries**. • Encryption commodities and software to **private companies and government end-users headquartered** in **Supp. 3 Countries,** wherever located (except E:1 countries).	Yes	No	Yes[4]
(b)(1)(ii)(A)	Encryption commodities and software, with key lengths not exceeding **80 bits (symmetric), 1024 bits (asymmetric)** and **160 bits (elliptic curve),** to private companies or government end-users headquartered or located in **non-Supp. 3 Countries** (except E:1 countries). Items that provide an open cryptographic interface are not authorized by this provision.	Yes	No	Yes[4]
(b)(1)(ii)(B)	Source code to non-government end-users located anywhere (except E:1 countries).	Yes	No	
(b)(2)	The following encryption items are only authorized for export to government end-users headquartered in a Supp. 3 Country or to private companies located anywhere, except E:1 countries, after the 30-day waiting period: • Certain network infrastructure software; • Encryption source code that is not publicly available; • Encryption items that are customized for a government end-use or end-user, where the cryptographic functionality has been modified to customer specification or is user-accessible and easily modified by the user, that provide functions necessary for quantum cryptography, or that have been modified for computers classified under ECCN 4A003; and • Cryptanalytic items.	Yes	Yes (30 days)	Yes
(b)(3)	If the product is (i) ***not listed in § 740.17(b)(2)*** and (ii) pending a mass market review or not a mass market item, then it may be exported to government or non-government end-users located anywhere (except E:1 countries) after the 30-day waiting period using License Exception ENC.	Yes	Yes (30 days)	Yes
(b)(4)(i)[5]	***Short Range Wireless Items*** – items with a nominal operating range not exceeding 100 meters.	No	N/A	No
(b)(4)(ii)[5]	***Foreign products*** developed with or incorporating previously reviewed and authorized US-origin encryption source code, components or toolkits, provided that the cryptographic functionality has not been changed.	No	N/A	Y/N[6]
(b)(4)(iii)[5]	***Wireless Personal Area Networks*** – Devices limited to a nominal operating range of 30 meters or less, such as hands-free headsets and wireless video game controllers.	No	N/A	No
(b)(4)(iv)[5]	***Ancillary Cryptography*** (see discussion above)	No	N/A	No

[1] License Exception ENC does not authorize exports to countries listed in Country Group E:1 of Supplement No. 1 to part 740 of the EAR ("E:1 countries").

[2] Any product that incorporates or is manufactured from an item exported using § 740.17(a) of the EAR is automatically subject to the EAR, even if such incorporation is minimal (i.e., the *de minimis* and foreign direct product rules do not apply to such products incorporating or manufactured from items exported under § 740.17(a)).

[3] Export or re-export of items that provide an "open cryptographic interface" is authorized under § 740.17(b)(1)(i) but not under the other sections of paragraph (b).

[4] Exports made under these provisions are subject to the reporting requirements until classified as 5A992, 5B992 or 5D992.

[5] These items may be self-classified as 5x002 or 5x992, as appropriate. If 5x002, then it may be exported using License Exception ENC. If 5x992, then it may be exported using NLR.

[6] Items exported under this exception are subject to the reporting requirements if the foreign item has entered the United States.

Money, Money – Who's Got the Money?

When the economic going gets tough, multinational companies might be tempted to cut costs by cutting back on steps needed to comply with the Foreign Corrupt Practices Act (FCPA).

But the DOJ is on record that it and the Securities and Exchange Commission (SEC) don't expect to cut back on FCPA investigations and prosecutions. In 2008 the DOJ and SEC collected more than US$924 million in penalties for FCPA violations. And lead DOJ Prosecutor Mark Mendelsohn recently – and pointedly – noted that even though the global economic crisis presents "a grave challenge in the fight against foreign bribery ... companies need to be especially vigilant in this economic climate not to cut back. Our law enforcement efforts are not going to be scaled back, and so it would be, I think, a grave mistake for a company to take that path."

Instituting policies and procedures that implement the US Federal Sentencing Guidelines for an Effective Compliance and Ethics Program and practicing effective due diligence are two bedrock fundamentals of FCPA compliance and risk mitigation.

FCPA compliance is a must if you engage in international business. Operating a compliance and ethics program that meets the Guidelines' expectations should be every organization's baseline objective. For an organization to demonstrate it has an effective program, the Guidelines require the organization to exercise due diligence to prevent and detect criminal activity and to promote an organizational culture that encourages ethical behavior and a commitment to lawful conduct. The Guidelines provide that a program minimally requires the following seven characteristics:

1. The organization must "establish standards and procedures to prevent and detect criminal conduct."
2. The organization's governing authority must be knowledgeable about and reasonably supervise the program. Individuals with operational responsibility for the program must report periodically to high-level personnel and, as appropriate, to the governing authority or an appropriate subgroup of the governing authority (e.g., the audit committee) on the program's effectiveness.
3. The organization must use reasonable efforts to not empower substantial authority in any individual whom it "knew, or should have known…engaged in illegal activities or other conduct inconsistent with an effective" program.
4. The organization must "take reasonable steps to communicate periodically and in a practical manner its standards and procedures" to the governing authority, officers and employees, and, as appropriate, agents and other third parties.
5. The organization must take reasonable steps to guarantee that the program is followed, including monitoring and auditing to discover unlawful behavior, to evaluate from time to time the program's effectiveness and to publicize a system that may include methods of communication that provide for anonymity, thus enabling employees and third parties to "report or seek guidance regarding potential or actual criminal conduct without fear of retaliation."
6. The organization must promote and consistently enforce the program through appropriate performance incentives and commensurate disciplinary measures.
7. "After criminal conduct has been detected," the organization must "take reasonable steps to respond appropriately…and to prevent further similar criminal conduct."

Finally, in addition to these seven elements, the Guidelines require that the organization "periodically assess the risk of criminal conduct" and take "steps to design, implement or modify each requirement" to reduce the risk of unlawful conduct.

The DOJ and SEC have stressed the need to conduct due diligence on anyone acting on behalf of an entity subject to the FCPA. The government has backed up these words by bringing enforcement actions against companies, their officers and employees, and third parties where the lack of due diligence contributed to FCPA violations. While common law agency will ultimately govern, the acts of employees, officers and directors, joint-venture partners, targets acquired in a merger and third parties all can impute FCPA liability to an entity for which they act.

There is no one right way to conduct due diligence. Due diligence is a potpourri of tasks that include FCPA-tailored risk and awareness application materials; interviews; background checks; using a forensic accountant to review books and records to evaluate high risk transactions; and visiting the office of and documenting the services provided by third parties. If any red flags appear during due diligence, they must be investigated until you are reasonably satisfied you do not have an FCPA concern. Finally, due diligence must be documented.

The government has suggested that FCPA due diligence is not a one-size-fits-all undertaking. For example, degrees of diligence may reasonably vary from industry to industry and location to location. Similarly, the timing (e.g., before and during) may also vary.

Once you have satisfied your due diligence, you need to implement the next steps in mitigating potential FCPA exposure. Suggested courses of action include providing your third-party agents with a copy of your antibribery code of conduct. Require them to read it and execute an acknowledgment that they will abide by it. Include in this acknowledgment FCPA-specific representations and warranties attesting to past compliance and covenants promising future compliance. If possible, negotiate as part of your third-party contracts the right to inspect and audit the books and records of your agent. Be certain to include termination rights.

In the high stakes and high risk world of international business, it's all about mitigating exposure. Proactively meeting the Guidelines' mandates and adhering to the due diligence best practices discussed above are your best tools to avoid sleepless nights due to an FCPA nightmare.

Recent Enforcement Actions and Updates

Directorate of Defense Trade Controls (DDTC) – US Department of State

- **Air Shunt Instruments, Inc. Agrees to Settle Charges of Unauthorized Export of Defense Articles and Technical Data.** Air Shunt Instruments, Inc. has entered into a consent agreement with the DDTC to settle charges relating to unauthorized exports of defense articles and technical data and misrepresentations and omissions of material facts on an export control document. Based in California, Air Shunt supplies replacement parts and components for military aircraft to the Department of Defense and aerospace industry. According to the DDTC charging document, between September 2003 and January 2004, the company was involved in three separate sales of defense articles to Dubai and Thailand, each without a proper DDTC license. In addition, the company indicated in shipping documents that no license was required for the subject merchandise.

  Under a July 2009 Consent Agreement, Air Shunt agreed to pay a US$100,000 civil penalty and implement remedial measures to strengthen its internal export control compliance procedures. The parties agreed that the US$100,000 fine could be applied against costs of improving its compliance program; US$70,000 for pre-consent agreement remedial compliance measures; and US$30,000 for consent agreement-authorized remedial compliance measures. In addition, Air Shunt has agreed to be subject to on-site reviews by the DDTC and 12- and 24-month audits by an outside consultant with export control experience.

- **Two Sentenced in Conspiracy to Export Controlled Aircraft Parts to Iran.** Judge Patricia A. Seitz of the US District Court for the Southern District of Florida sentenced Traian Bujduveanu to 35 months of imprisonment and three years of supervised release for his role in a conspiracy to export military and dual-use aircraft parts to Iran. Bujduveanu, a Romanian national and naturalized US citizen, pleaded guilty in April 2009 to charges of conspiracy to export goods to Iran in violation of the US embargo and to export defense articles without authorization. According to his plea, Bujduveanu used his corporation, Orion Aviation, to sell controlled aircraft parts to co-conspirators Hassan Keshari and his corporation Kesh Air International, which were each sentenced in May 2009. Bujduveanu falsified shipping documents to export the goods to Keshari's customers in Iran by way of a freight forwarder in Dubai. The merchandise illegally exported included parts for the F-14 fighter jet, Cobra AH-1 Attack Helicopter and CH-53A Military Helicopter – each part of Iran's military fleet.

Bureau of Industry and Security (BIS) – US Department of Commerce

- **Semiconductor Technologies Manufacturer Settles Charges of Export Violations and False Statements.** In August 2009 RF Micro Devices, Inc. (RFMD) agreed to settle charges of unauthorized exports of controlled spread-spectrum modems to China. Spread-spectrum modems create wide bandwidth communications links resistant to interference, jamming and detection, and are controlled for national security reasons (and classified under ECCN 5A001). RFMD voluntarily disclosed the unlicensed exports to BIS and was ultimately alleged to have participated in 14 unlicensed exports and 13 instances of making false or misleading statements in connection with the submission of related shipper's export declarations. The company has agreed to pay a US$190,000 civil penalty to settle the allegations. In addition, an RFMD manager responsible for export control compliance has agreed to settle allegations she made false and misleading statements to BIS agents during their investigation of the company. She allegedly told a BIS investigator that an outside consultant advised the company that its products were not export-controlled to any region where they were being marketed and sold; in fact, she repeatedly had been advised that the products may have required export licenses. For her part, the RFMD manager agreed to pay a civil penalty of US$15,000.

- **Unlawful Export Conspirator Sentenced.** In March 2009 Joseph Piquet was found guilty of seven counts of export control violations arising from his role in a conspiracy to export high-tech military electronics to Hong Kong and the People's Republic of China. The electronics included high-power amplifiers used in early warning radar and missile target acquisition systems and certain dual-use, low noise amplifiers. According to testimony during his trial, Piquet conspired with others to purchase and export the controlled items by submitting false End Use Certificates to manufacturers to conceal intended end uses and destinations. A US District Court judge in the Southern District of Florida sentenced Piquet to 60 months imprisonment.

- **Gulf International Bank Agrees to US$50,000 Penalty for Antiboycott Violations.** The New York branch office of Gulf International Bank, which is based in Bahrain, has agreed with BIS to settle allegations of violations of the antiboycott provisions of the EAR. The BIS Office of Antiboycott Compliance alleged eight instances of antiboycott violations by the bank between 2002 and 2004. Each violation related to the sale and transfer of goods from the United States to Syria and involved providing information about a person's business relationship with another company that is believed to be boycotted by Syria. BIS also alleged 17 instances of the bank failing to report its receipt of prohibited requests to engage in activities related to a foreign boycott and one instance of failing to maintain required records relating to such requests.

Office of Foreign Assets Control (OFAC) – US Department of Treasury

- **DHL Agrees to US$9.4 Million Settlement With OFAC and BIS.** OFAC and BIS have entered a joint settlement agreement with DPWN Holdings (USA), Inc. and DHL Express (USA), Inc. regarding allegations that the carrier aided and abetted unlawful exports to embargoed countries Syria, Iran and Sudan and failed to comply with record-keeping obligations related to such exports. BIS alleged eight occurrences of aiding and abetting unlawful exports to Syria in 2004 and 90 instances of failing to retain air waybills and other export control documents, as required under the EAR. OFAC likewise identified record-keeping violations, and other violations of OFAC regulations in connection with thousands of shipments to Iran and Sudan between 2002 and 2006. Under the joint settlement agreement, DHL will pay a US$9.4 million civil penalty and engage an expert in export control laws and sanctions programs to conduct a comprehensive audit of transactions involving Iran, Sudan and Syria occurring between March 2007 and December 2009. In addition, the company will commission full-year 2010 and 2011 audits.

FCPA – US Department of Justice and US Securities and Exchange Commission

- **Valve Company Executives Plead Guilty to Unlawful Payments.** Two former executives of a California-based valve company each pleaded guilty to one count of conspiring to violate the FCPA. Mario Covino, the company's director of worldwide sales, admitted that from March 2003 to August 2007 he caused valve company employees and agents to make approximately US$1 million in payments to vice presidents, managers and purchasing officers of state-owned enterprises (SOEs) – "foreign officials" under the FCPA – to assist in obtaining or retaining business. Richard Morlok, then finance director, admitted that he caused valve company employees and agents to make payments of approximately US$628,000 to officials (e.g., vice presidents, managers and purchasing officers) of numerous SOEs to assist in obtaining or retaining business from 2003 through 2006. Sentencing for both individuals is scheduled for later this year. Each faces a maximum of five years in prison, three years of supervised release and a fine of up to US$250,000, or twice the pecuniary gain or loss resulting from the offense, whichever is greater. Covino and Morlok agreed to cooperate with the DOJ's ongoing investigation. The valve company was referred to as an "unnamed co-conspirator" in the statement of facts attached to the plea agreements. To date, the valve company has not been indicted. However, six individuals that acted on its behalf have been indicted.

- **ITT Corporation Settles SEC Action.** ITT has agreed to settle a civil action by the SEC involving allegations that the company violated the FCPA's books and records and internal controls provisions as a result of improper payments to officials in China by employees or agents of ITT's wholly owned subsidiary in China, Nanjing Goulds Pumps Ltd. (NGP). The SEC alleged that NGP employees or agents paid officials of SOEs in China to influence the design of infrastructure projects so as to require the use of NGP pumps. NGP employees also paid third-party agents to facilitate payments to foreign officials, with the understanding that payments would be made to foreign officials that recommended NGP pumps or directly pay employees of the SOE that purchased the pumps.

  ITT's illicit payments totaled approximately US$200,000 and generated more than US$4 million in improper NGP sales. NGP's books and records disguised these payments as increased commissions, which were consolidated in ITT's financial statements filed with the SEC. ITT also allegedly failed to make or keep books and records in reasonable detail so as to accurately and fairly reflect the illicit payments by NGP and the related disposition of assets. Finally, ITT failed to devise and maintain a system of internal controls sufficient to provide reasonable assurances that: (a) transactions were executed in accordance with management's

authorization; (b) transactions were recorded to maintain accountability of assets; and (c) access to assets was permitted only in accordance with management's authorization.

Without admitting or denying the SEC's allegations, ITT consented to the entry of a final judgment permanently enjoining it from future books and records and internal controls violations. ITT further agreed to disgorge approximately US$1 million in profits and pay a US$250,000 civil penalty.

- **Kellogg Brown & Root LLC (KBR LLC), Kellogg, Brown & Root, Inc. (KBR, Inc.) and Halliburton Company Settle Charges in Nigerian Bribery Scheme.** The DOJ and SEC have brought related enforcement actions against KBR LLC, KBR, Inc. and Halliburton in connection with a decade-long scheme to bribe government officials in Nigeria to obtain contracts concerning natural gas facilities. KBR LLC formed a joint venture with others, which operated through three Portugal-based companies, to bid on and perform natural gas contracts in Nigeria. In response to criminal charges by the DOJ, KBR LLC admitted that prior to the award of the contracts, its former CEO, Albert Stanley, and others met with senior executives in Nigeria's government to request the office holders to designate representatives with whom the joint venture should negotiate government officials' bribes. KBR LLC further admitted to paying more than US$180 million to consultants to be used, at least in part, for Nigerian government officials' bribes.

  KBR LLC pleaded guilty to one count of conspiring with joint venture parties and others to violate the FCPA by authorizing, promising and paying bribes to government officials, including executive branch officials, and four counts of violating the FCPA's antibribery provisions. To settle the DOJ's criminal charges, the company agreed to pay a US$402 million fine and to retain an independent compliance monitor for three years to review the design and implementation of the entity's compliance program and report to the DOJ. Further, KBR LLC agreed to undergo three years of organizational probation and continue to cooperate with the DOJ's ongoing investigation.

  In related actions, the SEC charged KBR, Inc., KBR LLC's parent company, with violating the FCPA's antibribery, books and records, and internal controls provisions, as well as aiding and abetting Halliburton's violations of the books and records and internal controls provisions. The SEC also charged Halliburton, KBR LLC's former parent company, with books and records and internal controls violations of the FCPA. Specifically, with respect to Halliburton, the complaint alleged that the company failed to devise adequate internal controls relating to foreign sales agents and the FCPA, and failed to enforce the internal controls then in place. As a result, Halliburton failed to detect, deter or prevent violations by its subsidiaries.

  KBR, Inc. and Halliburton have agreed to pay US$177 million in disgorgement to settle the SEC's charges. KBR, Inc. is permanently enjoined from violating the antibribery provisions and from aiding and abetting violations of the books and records and internal controls provisions of the FCPA and must retain an independent monitor for three years to review its compliance program. Halliburton is permanently enjoined from violating the FCPA's books and records and internal controls provisions and must retain an independent consultant to review its FCPA compliance program. The combined US$579 million in penalties represents the largest penalty ever paid by US companies in the FCPA's history.

Squire Sanders IT^3 Team Members

*Points of contact for additional information on our IT^3 practice

United States

Washington DC Office
Suite 500
1201 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
Donald T. Bucklin
Sarah C. Carey
Francis E. Fletcher Jr.*
George N. Grammas*
Cathy Kettlewell
Peter Koenig*
Henry W. Lavine
Iain R. McPhie
Barry A. Pupkin
Thomas J. Ramsey
Shanker A. Singham*
Christopher H. Skinner
David M. Spooner*
Ritchie T. Thomas*
Christopher A. Williams

Tysons Corner Office
Robert E. Gregg*
Karen R. Harbaugh*

Columbus Office
Donald W. Hughes

Los Angeles Office
Denis H. Oyakawa

Palo Alto Office
David A. Saltzman

Miami Office
Gregory W. Bates
Rebekah J. Poston

San Francisco Office
Michael Moyle

Europe

Brussels Office
Belgium
B. A. Araujo
Brian N. Hartnett*
Cristiana Spontoni

London Office
United Kingdom
Caroline I. Waite
Carol M. Welu

Frankfurt Office
Germany
Jan Sudmeyer

Moscow Office
Russian Federation
Olga M. Bezrukova
Ivan A. Trifonov

Asia

Beijing Office
People's Republic of China
Sungbo Shim
James M. Zimmerman

Hong Kong Office
Hong Kong SAR, China
Nicholas Chan

Shanghai Office
People's Republic of China
Amy L. Sommers

Tokyo Office
Japan
Yasuhiro Hagihara
Munehiro Matsumoto

Latin America

Rio de Janeiro Office
Brazil
Salim Jorge Saud Neto

Caracas Office
Venezuela
Hernando Diaz-Candia

Santo Domingo Office
Dominican Republic
Daniela Collado
Flavio Dario Espinal

Squire Sanders Public Advocacy, LLC
A wholly owned affiliate of Squire, Sanders and Dempsey L.L.P.

Washington DC
Robert D. Lehman*

NORTH AMERICA
Cincinnati
Cleveland
Columbus
Houston
Los Angeles
Miami
New York
Palo Alto
Phoenix
San Francisco
Tallahassee
Tampa
Tysons Corner
Washington DC
West Palm Beach

LATIN AMERICA
Bogotá+
Buenos Aires+
Caracas
La Paz+
Lima+
Panamá+
Rio de Janeiro
Santiago+
Santo Domingo
São Paulo

EUROPE & MIDDLE EAST
Bratislava
Brussels
Bucharest+
Budapest
Dublin+
Frankfurt
Kyiv
London
Moscow
Prague
Riyadh+
Warsaw

ASIA
Beijing
Hong Kong
Shanghai
Tokyo

+Independent network firm

Subscription Information

Squire Sanders publishes on a number of other topics. To see a list of options and to sign up for a mailing, or to correct or update information, visit **www.ssd.com**.

Have an Article Idea?

Is there a particular subject you'd like to see us address?
Send your article suggestions to George Grammas.

The contents of this newsletter are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations. Counsel should be consulted for legal planning and advice. Reproduction or distribution of this *IT^3 Update* in its entirety is permitted.

©Squire, Sanders & Dempsey L.L.P.
All Rights Reserved
2009