The Export Practitioner

Timely News and Analysis of Export Regulations

MARCH 2016

VOLUME 30
NUMBER 3

In this issue

Lessons from Japan's Export Control System

ALSO INSIDE

The Export Practitioner

March 2016
Volume 30
Number 3

Publisher
Martin Kalin

Managing Editor
Meredith Gilston

Associate Editor
Melissa Apter

Editor, Japanese Edition
Megumi Senda

The Export Practitioner
Is published monthly by
Gilston-Kalin Communications, LLC
P.O. Box 5325,
Rockville, MD 20848-5325

Editorial
(301) 460-3060

Circulation
(301) 460-3060
FAX: (301) 460-3086

WWW.EXPORTPRAC.COM

AT A GLANCE

DEPARTMENTS

Postmaster: Send Address Changes to the Above Address. Annual Subscription: Domestic $699, International $699

Lessons from Japan's Approach to Export Controls

By Jason E. Prince and Steven W. Pelak*

Although Japan's pacifist Constitution limits the Japanese Self-Defense Force's ability to engage in military intervention abroad, Japan has long played a leadership role in another area of international peace and security: export controls. For nearly three decades, the Japanese government has focused on developing one of the Asia-Pacific's most robust legal systems for preventing foreign nations and terrorist organizations from obtaining military and dual-use items and technology.

Demonstrating Japan's current leadership role in the export control arena, the Japanese Ministry of Economy, Trade and Industry (METI), the Japanese Ministry of Foreign Affairs (MOFA), and the Tokyo-based Center for Information on Security Trade Control (CISTEC) co-hosted the 23rd Asian Export Control Seminar in Tokyo Feb. 23-25, 2016.

Participants in this invitation-only event included more than 120 representatives from roughly 20 Asian countries and administrative regions (including China, South Korea and Taiwan), the U.S., the European Union, Australia, Turkey, United Arab Emirates, Mexico, the Wassenaar Arrangement, the United Nations (UN) Security Council 1540 Committee, and the World Customs Organization. Most of the seminar participants were high-ranking government officials within their countries' respective export control agencies.

Due to North Korea's January 2016 nuclear bomb test and February 2016 long-range rocket test, this year's Asian Export Control Seminar assumed a heightened sense of urgency. Indeed, several speakers and panelists pointed to North Korea's activities as a principal reason why Asian and other countries must redouble their collective efforts to safeguard military and dual-use hardware and technology.

For example, three members of the Panel of Experts established pursuant to Resolution 1874—a 2009 UN Security Council resolution that imposed certain sanctions on North Korea—presented on the elaborate global web of intermediaries, shell companies, falsified cargo manifest documents, aliases and transshipments the North Koreans have recently used to obtain unmanned aerial vehicle components, missile transport vehicles, and weapons of mass destruction (WMD).

This article provides an overview of Japan's export control system and its role in ensuring peace and security in the Asia Pacific region. In particular, this article focuses on Japan's internal compliance program (ICP) approach to export controls, which incentivizes exporters to establish and register with METI an ICP that satisfies specified criteria. This article concludes by suggesting some lessons companies and government officials in the U.S. and elsewhere may learn from Japan's ICP approach.

> Japan's internal compliance program (ICP) approach... incentivizes exporters

Overview of Japan's Export Control System

While under the Allied Occupation in 1949, the Japanese government enacted the Foreign Exchange and Foreign Trade Control Act, which essentially still serves as the country's primary export control law. At that time, Japan also formed METI, which continues to administer Japan's export control system. Three years later, in 1952, Japan joined the Coordination Committee for Multilateral Export Controls (COCOM), an organization through which the United States and other Western-bloc countries sought to maintain their military edge over the Soviet Union.

However, export controls did not become a major focus for the Japanese government until 1987. That was the year in which the U.S. revealed a Japanese company, Toshiba Machinery, and a Norwegian company, Kongsberg Vaapenfabrikk, had exported milling machines and numerical-control computers and software to the Soviet Union between 1982 and 1984. These illegal exports, which enabled the Soviet Union to manufacture quieter submarine propellers which were difficult to detect, provoked public outrage in the U.S. and in other allied nations.

In response to what is known in Japan as the "Toshiba Machinery Incident," the Japanese government enacted sweeping amendments to the Foreign Exchange and Foreign Trade Control Act in 1987. Among other things, these amendments significantly increased the penalties and fines for violating the Act's export control provisions and also called for Japanese companies to create ICPs that satisfied

certain criteria.

Two years later, in 1989, Japan's government and industry collaborated to found CISTEC, a nonprofit, non-governmental research and analysis organization geared toward serving as a bridge between government, industry and academia in the area of export controls.

Over time, Japan has developed a complicated export control regime that involves not only the Foreign Exchange and Foreign Trade Control Act, but also a complex web of cabinet orders and ministerial ordinances, notifications, and guidance.

Japan is currently a member of all of the existing international export control regimes. As a result, the fundamental components of Japan's export control system are similar to those of the United States and many other countries, consisting of export classification numbers, control lists, licenses, license exemptions, brokering controls, transshipment controls, special controls for countries of serious concern (currently Iran, North Korea and Russia), and penalties and fines for noncompliance.

Japanese companies may now export defense equipment and technology in 11 specified cases

One of the more noteworthy recent developments in Japanese export controls took place in April 2014 when the cabinet of Prime Minister Shinzo Abe repealed the "Three Principles on Arms Export and Their Related Policy Guidelines." These former guidelines, adopted in 1967 and supplemented in 1976, essentially prohibited Japanese companies' export of defense equipment and technology—even to Japan's allies.

Seeking primarily to counter China and North Korea's growing military presence in the Asia-Pacific region, the Abe Cabinet has eased certain post-World War II restrictions on Japan's military involvement. Accordingly, under the Abe Cabinet's new "Three Principles on Transfer of Defense Equipment and Technology," Japanese companies may now export defense equipment and technology in 11 specified cases that will contribute to global peace and serve Japan's security interests.

Japanese Internal Compliance Programs

As mentioned above, one of the cornerstones of Japan's post-1987 export control system is its emphasis on companies' implementation of internal compliance programs or ICPs. Technically, Japanese law merely encourages companies to adopt written ICPs and submit them to METI for review.

However, written ICPs became closer to mandatory when METI's new "Export Compliance Standard" took effect in April 2010. Under this Standard, each exporter of controlled goods or technology—including individuals, companies and universities—is legally obligated to establish a compliance system that includes at least the following elements:

Organization: An organizational structure that addresses export control, with clearly defined roles and responsibilities and the designation of a specific person who is ultimately responsible for ensuring compliance.

Procedures: Procedures that address the classification of items, transaction screening (e.g., end-user and end-use verification), and shipment controls (e.g., confirmation that goods match their shipping documents).

Monitoring: Ongoing export control compliance monitoring through internal audits, training of relevant personnel, appropriate recordkeeping, the prompt reporting of violations to METI, and the adoption of remedial measures.

The elements of the Export Compliance Standard closely resemble the elements Japanese law has long encouraged exporters to include in their written ICPs. Thus, an exporter's best means to ensure compliance with the mandatory Export Compliance Standard is typically to submit a written ICP to METI for review.

If the written ICP is satisfactory, METI will register it. Exporters with registered ICPs may then choose to allow METI to publish their names on METI's website, such that the public knows their ICP has received METI's stamp of approval. According to CISTEC, METI has thus far registered roughly 1,500 ICPs, and approximately 600 companies have chosen to publish their names on METI's website.

Each year, METI also issues a compliance checklist to all exporters that have registered an ICP. Exporters answer the approximately 40 questions in the checklist to assess their ongoing compliance and then return the completed checklist to METI.

Notably, only exporters that have registered their ICP and submitted their completed annual compliance checklist to METI are eligible for "special bulk licenses" that allow multiple exports of controlled items in a streamlined fashion. In other words, METI provides exporters with an added business incentive to develop and maintain a robust ICP.

METI works closely with CISTEC to ensure each Japanese exporter has the tools and information necessary to create a tailor-made ICP. For example, CISTEC has posted on its website six different model ICPs that take into account the

various types of exporters (e.g., manufacturers, trading companies), enabling each exporter to select a model that best fits its organizational structure and risk profile. Moreover, Japan's recent Asian Export Control Seminar—which METI and CISTEC co-hosted—devoted an entire panel discussion to highlighting the key components and benefits of ICPs.

Considerations Arising from Japan's ICP Approach

Although it may not make sense to incorporate Japan's ICP system into the export control regimes of every country, Japan's approach provides a useful vehicle for exporters, regulators, and policy makers in the United States and elsewhere to reflect on certain key components of export controls. For example, Japan's ICP system offers at least three key considerations or lessons:

> METI can provide companies with review and feedback before a violation occurs

1. All exporters would be well-advised to study the basic export control compliance program elements Japan prescribes in its ICP laws and its Export Compliance Standard. These basic elements—which cover key aspects of organizational structure, control procedures and monitoring—serve as a solid starting point for the development of a compliance program that will withstand scrutiny under nearly any country's export control regime.

2. In the U.S. and certain other countries, regulators and enforcement officials typically review and provide feedback on a company's export control program only after the company has potentially violated the law and is the target of an enforcement action. At that point, the damage to national security may have already occurred.

   In contrast, under Japanese law, METI can readily provide companies with such review and feedback before a violation occurs, when companies still have the chance to adjust their compliance programs in a way that might prevent certain types of violations. Moreover, by working closely with CISTEC, METI has helped to shape the six different compliance program templates CISTEC makes available to Japanese companies on its website.

   Whether through a formal ICP system like Japan's or other more informal mechanisms, companies and export control regulators stand to benefit from communicating with each other about compliance program best practices in contexts other than enforcement actions or consent agreements.

3. Under any export control regime, companies have an obvious incentive to implement robust, tailor-made compliance programs. Indeed, such a compliance program is one of the most important tools for avoiding violations and the penalties, jail time and reputational damage that potentially follow.

   Yet, Japan demonstrates that export control regimes can also use such tools as streamlined licensing procedures or positive recognition on a regulator's website to incentivize companies to establish and maintain a healthy compliance program. The publication of companies' names on the regulator's website also provides a deterrence to procurement agents of adversary nations. Policy makers in the United States and elsewhere, with appropriate input from industry, should explore these sorts of positive incentives when seeking to reform existing export control laws rather than devoting inordinate time and expense to frequent revisions to control lists.

As explained above, Japan has devoted the past three decades to bolstering its own export control program and engaging in outreach to its Asia-Pacific neighbors to help them do the same. Amid growing tensions in the Asia-Pacific region fueled in part by North Korea's recent provocations, there has perhaps never been a better time to examine the state of export controls in Asia and to learn what countries like Japan are doing to keep military and dual-use items and technology out of the wrong hands.

** Jason Prince (jeprince@hollandhart.com) and Steven Pelak (swpelak@hollandhart.com) are partners in Holland & Hart LLP's International Trade Compliance Group. Mr. Prince previously served as Deputy Press Secretary to Nobuteru Ishihara, Japan's current Economy Minister, and he also attended the Japanese government's 23rd Asian Export Control Seminar as an invited observer. Mr. Pelak served as the U.S. Department of Justice's first National Coordinator of Export Control/Embargo Enforcement from 2007 until 2013.*

FORMER SOLDIER PLEADS GUILTY TO ILLEGAL NIGHT-VISION EXPORTS

Former Army soldier Hunter Perry pleaded guilty Feb. 12, 2016, in Louisville U.S. District Court to violating the Arms Export Control Act (AECA) by exporting defense articles, including night-vision equipment, to the United Kingdom (UK), Poland and Japan without State licenses.

Exported items included a D-760 night vision scope, a PAS-23 mini-thermal scope, PVS-15 night vision binocular and PAS-13 thermal scope, which were all controlled on the U.S. Munitions List.

Payments for this equipment were made through PayPal accounts associated with eBay and through bank wire transfers, the criminal information noted. Perry "would and did falsely state on shipping documents that he was exporting equipment other than defense articles in order to escape detection," the information added. Sentencing is set for May 18.

HALLIBURTON SUBSIDIARIES SETTLE OFAC CUBA CHARGES

Two Cayman Island subsidiaries of Halliburton Energy Services, Inc., agreed to pay more than $300,000 to settle charges of providing goods and services to an oil project in Angola of which a Cuban company was a partner.

Halliburton Atlantic Limited (HAL) agreed Feb. 25, 2016, to pay Treasury's Office of Foreign Assets Control (OFAC) $304,706 to settle charges of violating Cuba sanctions in 2011. HAL and its affiliate Halliburton Overseas Limited (HOL) allegedly exported goods and services in support of oil and gas exploration and drilling activities in the Cabinda Onshore South Block oil concession in Angola.

Cuba Petroleo, the state-owned Cuban oil company also known as Cupet, held a 5 percent interest in the Concession, OFAC said. "HAL issued 19 invoices to the Consortium operator, a company with headquarters in Angola, related to these goods and services, and HOL primarily performed the services which were invoiced," OFAC charged.

"HAL and HOL should have known that a Cuban entity belonged to the Consortium because the Consortium operator provided HAL with documents that showed that Cupet was a member, and there were other contemporaneous documents that stated Cupet held an interest in the Consortium, including a news article and a notice in an Angolan government registry," the agency said.

Other documents stated Cupet held an interest in the Consortium

Halliburton's sanctions compliance program was inadequate because it did not include a procedure to screen all of the Consortium members, OFAC added. HAL voluntarily self-disclosed the violation.

The company "cooperated fully with OFAC to expeditiously resolve this matter and believes it took reasonable steps to comply with all applicable regulations," Halliburton spokesperson Emily Mir wrote in an email to The Export Practitioner. "Halliburton has a longstanding, comprehensive trade compliance program to support global compliance with U.S. economic sanctions," she wrote.

QUALCOMM PAYS $7.5 MILLION TO SETTLE SEC BRIBERY CHARGES

Mobile technology company Qualcomm Inc. agreed March 1, 2016, to pay the Securities and Exchange Commission (SEC) a $7.5 million civil penalty to settle charges of violating the Foreign Corrupt Practices Act (FCPA) by hiring relatives of Chinese telecom officials to win contracts.

"From 2002 through 2012, Qualcomm provided things of value to foreign officials – including high-ranking employees of state owned enterprises (SOEs) and government ministers – to try to influence these decision makers to favor and/or promote Qualcomm-developed technology in an evolving international telecommunications market, thereby providing Qualcomm with a business advantage," the SEC order noted.

Specifically, Qualcomm "provided or offered full-time employment and paid internships to family members and other referrals of foreign officials at [state-owned firms] – often at the request of these foreign officials. Qualcomm referred to some of these individuals as 'must place' or 'special' hires," the SEC charged.

"In several areas of its business operations,

including hiring, hospitality planning, and business development, Qualcomm lacked an adequate oversight process to determine whether things of value that it provided to foreign officials were made with the intent to induce those officials to provide a business benefit to Qualcomm," it said.

Qualcomm provided or offered full-time employment and paid internships to family members

Justice recently closed its investigation on these matters without taking any action, the company said. "Qualcomm is pleased to have put this matter behind us. We remain committed to ethical conduct and compliance with all laws and regulations, and will continue to be vigilant about FCPA compliance," Don Rosenberg, Qualcomm's executive VP and general counsel, said in a statement.

BARCLAYS PAYS $2.5 MILLION TO SETTLE ZIMBABWE SANCTIONS

In case that highlights the risk of doing business in a country with a "significant presence" of blocked entities, Barclays Bank Plc agreed Feb. 8, 2016, to pay Treasury's Office of Foreign Assets Control (OFAC) $2,485,890 to settle charges of violating Zimbabwe sanctions from July 2008 to September 2013. Barclays did not voluntarily self-disclose the apparent violations.

Barclays allegedly processed 159 transactions for corporate customers of Barclays Bank of Zimbabwe Limited (BBZ) that were owned, 50 percent or more, directly or indirectly, by Industrial Development Corporation of Zimbabwe (IDCZ), a company on the Specially Designated National (SDN) list.

OFAC designated IDCZ in July 2008. At the time, BBZ maintained U.S. Dollar (USD)-denominated customer relationships for three corporate customers that were owned, 50 percent or more, directly or indirectly, by IDCZ and were also therefore blocked pursuant to OFAC guidance.

"Neither BBZ nor Barclays UK identified these customers as blocked persons at that time due to the aforementioned issues, however, and continued to process USD transactions for or on their behalf to or through the United States in apparent violation" of Zimbabwe sanctions, OFAC said.

"Although Barclays NY conducted an investigation that confirmed this information, the bank failed to properly upload identifying information for the blocked person into its sanctions screening filter in a timely or accurate manner and subsequently processed three additional transactions involving the same party between November2012 and September 2013–all of which were blocked by other U.S. financial institutions," OFAC said.

"Barclays is pleased to have resolved this matter with OFAC. As the notice states, OFAC considers the matter to have been a non-egregious case. Barclays continues to maintain a robust sanctions compliance program across its global operations and has implemented specific controls designed to ensure that payments of the type that gave rise to this matter do not occur again," company spokesperson Andrew Smith wrote in an email to The Export Practitioner.

Five days earlier, OFAC removed Agricultural Development Bank of Zimbabwe (Agribank) and Infrastructure Development Bank of Zimbabwe (IDBZ) from the SDN list. At same time, it removed Zimbabwe General License 1, which it had issued in April 2013 authorizing all transactions involving those two banks (see *The Export Practitioner*, May 2013, page 26).

"Following today's removal of Agribank and IDBZ from the List of Specially Designated Nationals and Blocked Persons, a license is no longer required to engage in transactions with those entities," OFAC noted.

N.C. MAN INDICTED FOR ATTEMPTED GUN EXPORTS

A North Carolina man was indicted after an elaborate scheme to smuggle firearms in household appliances. Richmond Akoto Attah of Charlotte, N.C., was indicted Feb. 16, 2016, in Charlotte U.S. District Court on charges of illegally attempting to export munitions to Ghana.

Attah allegedly hid 27 firearms, including nine millimeter and .40 caliber semi-automatic pistols and .38 caliber and .357 revolvers, inside a washing machine and dryer. He also is charged with hiding 3,500 rounds of ammunition inside a barrel, then attempting to ship the containers from Charlotte to Ghana.

In December 2015, "the container with the hidden firearms and ammunition left Charlotte and was driven to the port in Savannah, Georgia; where it was dropped off for shipment to Ghana and interdicted by U.S. customs officers," the indictment noted. The firearms were designated under Category I of the U.S. Munitions List, and the ammunition under Category III.

Attah remains in federal custody. "The government's forecast of evidence is strong and suggests the Defendant also repeatedly made false statements to customs, ATF (when purchasing firearms), and probation officials. While a naturalized US citizen, the Defendant has significant ties to Ghana and has traveled there several times in recent years. Defendant is both a danger and a risk of flight," the detention order notes.

ANOTHER PHARMACEUTICAL FIRM SETTLES SEC BRIBERY CHARGES

Yet another global healthcare company has settled charges of bribing Chinese healthcare providers (HCPs) to increase sales. SciClone Pharmaceuticals agreed Feb. 4, 2016, to pay a total of $12.8 million to settle Securities and Exchange Commission (SEC) charges of violating the Foreign Corrupt Practices Act (FCPA).

Pharmaceutical company Bristol-Myers Squibb (BMS) agreed in October to pay more than $14 million to settle similar charges (see *The Export Practitioner*, November 2015, page 12). Two months prior, infant formula supplier Mead Johnson Nutrition Company agreed to pay SEC $12 million for the same kind of violations.

"Although SciClone has local distributor relationships in China, its sales and marketing activities there are conducted through SPIL [a Hong Kong subsidiary]. Sales representatives in China regularly reported to senior management of SPIL on their efforts to increase sales," the SEC order noted.

"In these reports, sales representatives openly referred to instances in which they provided weekend trips, vacations, gifts, expensive meals, foreign language classes, and entertainment to HCPs in order to obtain an increase in prescriptions from those HCPs. As described by one sales manager, this was 'luring them with the promise of profit,'" it said.

"The related transactions were falsely recorded in SciClone's books and records as legitimate business expenses, such as sponsorships, travel and entertainment, conferences, honoraria, and promotion expenses. During this period, SciClone also failed to devise and maintain a sufficient system of internal accounting controls and lacked an effective anti-corruption compliance program," the SEC added.

SciClone also failed to maintain a sufficient system of internal accounting controls

SciClone agreed to pay a civil penalty of $2.5 million, disgorgement of $9.4 million and prejudgment interest of $900,000. As part of the agreement, the company neither admitted nor denied any wrongdoing. In a press release, the company said the Justice Department (DOJ) "has also completed its related investigation and has declined to pursue any action."

"We are very pleased to have reached a final settlement with the SEC and DOJ that is in line with our previous expectations and brings this matter to conclusion. We believe that we have established an industry-leading compliance program, including a commitment to constant improvement, which is a key business asset," SciClone CEO Friedhelm Blobel said in a statement.

FRENCH FIRM SETTLES OFAC CUBA SANCTION CHARGES

A French company that provides services and equipment to the oil and gas industry settled charges of violating Cuba sanctions. CGG Services S.A., formerly known as CGG Veritas S.A. (CGG France), agreed Feb. 22, 2016, to pay Treasury's Office of Foreign Assets Control (OFAC) $614,250 to settle the charges.

The company and a U.S. affiliate allegedly exported spare parts and other equipment to three vessels – the M/V Amadeus, M/V Veritas Vantage, and M/V Princess – while they operated in Cuba's territorial waters in 2010 and 2011. CGG France did not voluntarily self-disclose the violations, the agency noted.

In addition, Veritas Geoservices, a Venezuelan CGG subsidiary, allegedly engaged in five transactions involving "the processing of data from seismic surveys conducted in Cuba's

Exclusive Economic Zone benefiting a Cuban company," OFAC said.

Veritas Geoservices "acted with reckless disregard for U.S. sanctions requirements by performing data processing related to seismic surveys conducted in Cuban waters without determining if there was a Cuban interest in the data," it said.

The company has adjusted its procedures to minimize the risk of future violations

CGG France took some steps to avoid OFAC violations as part of its compliance program, including removing U.S. personnel and equipment for one of the vessels prior to it entering Cuba's territorial waters; and the company has adjusted its supply procedures to minimize the risk of future sanctions violations, OFAC noted.

CGG provides "leading geological, geophysical and reservoir capabilities to its broad base of customers primarily from the global oil and gas industry," its website notes.

POPCORN MAKER GETS PROBATION FOR EXPORT-IMPORT BANK FRAUD

The owner of a Louisville, Ky., popcorn maker was sentenced Feb. 1, 2016, to three years' probation and $110,678.74 in restitution for defaulting on a loan insured by the Export-Import Bank (Ex-Im). Kermit W. Highfield, owner of Preston Farms Popcorn, LLC, pleaded guilty in November in Louisville U.S. District Court to bank fraud (see *The Export Practitioner*, December 2015, page 8).

Highfield admitted he diverted payments in 2013 that should have been deposited into the secured loan account to meet operating expenses. "Preston Farms had customers pay money into an account that secured loans through the Import Export Bank [sic]. These funds were to be deposited into this trust account to pay the loans for Preston Farms upon receipt," Highfield admitted in a sentencing memo filed in court.

"The Government agrees that this crime is not one where the defendant used stolen money to live a lifestyle beyond his means with luxurious and expensive purchases for himself. Rather, the diversion and use of the funds merely extended the life of Preston Farms Popcorn, LLC, and delayed the inevitable failure of Mr. Highfield's business," he wrote.

SOFTWARE FIRM PAYS $28 MILLION TO SETTLE BRIBERY CHARGES

Massachusetts software company PTC Inc. agreed Feb. 16, 2016, to pay more than $28 million to settle charges of violating the Foreign Corrupt Practices Act (FCPA) with the Securities and Exchange Commission (SEC) and Justice. From at least 2006 into 2011, two wholly owned PTC subsidiaries in China provided nearly $1.5 million in improper payments to Chinese government officials who were employed by Chinese state-owned entities (SOEs) that were PTC customers, the SEC order said. These payments were made to obtain or retain business from the SOEs.

"Specifically, PTC-China provided non-business travel, primarily sightseeing and tourist activities, as well as improper gifts and entertainment, to the Chinese government officials. PTC earned approximately $11.85 million in profits from sales contracts with SOEs whose officials received the improper payments," SEC noted.

Under the settlement, PTC also entered into a nonprosecution agreement (NPA) with Justice, paying a $14.54 million criminal penalty. PTC China admitted that the cost of these recreational trips was routinely hidden within the price of PTC China's software sales to the Chinese state-owned entities whose employees went on the trips, Justice said.

"PTC China routinely engaged the services of local 'business partners,' Chinese companies that helped PTC China find prospective contracts, assisted PTC China in the sales process with Chinese SOEs, and provided additional services to PTC China's customers that had been outsourced by PTC China, including information technology services," the NPA noted.

"PTC China failed to conduct meaningful due diligence of its Chinese business partners, notably with respect to corruption risks or anti-corruption controls of these Chinese business partners," it added. "Some of the overseas travel expenses paid for by the business partners were tracked by PTC China sales staff on spreadsheets that they maintained separately from PTC China's electronic accounting records to help

PTC China better understand the composition of, and negotiate, fees with the Chinese business partners," the NPA said.

"The company is pleased to have resolved this matter," PTC said in a statement. The settlement pertained to "expenditures by certain former employees and business partners in China," it added. "PTC has implemented extensive remedial measures related to these matters, including the termination of the responsible employees and business partners, the establishment of an entirely new leadership team in China, the establishment of a dedicated compliance function, and other enhancements to compliance programs," the PTC statement said.

MIDDLE EAST SUBSIDIARY GETS SLAP ON WRIST FROM OFAC

The Middle East subsidiary of an international consumer products company received a Finding of Violation from Treasury's Office of Foreign Assets Control (OFAC) Feb. 4, 2016, for alleged violations of Sudan sanctions in 2010.

Johnson and Johnson (Middle East) Inc. (JJME), a wholly owned subsidiary of Johnson & Johnson, allegedly coordinated and supervised five shipments of consumer hygiene products worth $227,818 from Johnson and Johnson (Egypt) S.A.E. (JJE) to Khartoum, Sudan.

"Following a November 2009 restructuring, JJME became directly involved in the business planning and supervision of JJE, including JJE's transactions with Sudan," OFAC said. "Prior to August 2010, this General Manager was unfamiliar with U.S. sanctions and received no training on compliance with OFAC regulations despite being responsible for sales in the Middle East and North Africa, including Sudan," it added.

"JJME acted with reckless disregard for U.S. sanctions requirements when it made two exports to Sudan after being made aware that it might be subject to restrictions under U.S. sanctions," OFAC noted. The company "did not properly take into consideration the implications of OFAC regulations when it restructured its consumer business and placed a U.S. company in charge of sales to Sudan," the agency added.

"This enforcement action highlights the need for U.S. companies, particularly large, sophisticated entities dealing primarily in international transactions, to ensure that their employees are properly trained on OFAC regulations, especially managers who oversee sales to regions that pose a particularly high risk for violations of the sanctions programs administered by OFAC," the agency said.

Harm to sanctions programs was limited because the exports were consumer hygiene products

OFAC considered the following mitigating factors: JJME took remedial action including conducting an internal investigation of the violations and instituting additional compliance training; and the harm to sanctions programs objectives was limited because the products exported, while not authorized by OFAC, were consumer hygiene products.

In addition, JJME has no prior OFAC sanctions history, including no penalty notice or Finding of Violation in the five years preceding the violations; and JJME cooperated with OFAC's investigation, including by providing detailed and well-organized information, it said.

AIRLINE CEO SETTLES CHARGES OF BRIBERY IN UNION DISPUTE

Ignacio Cueto Plaza, CEO of South America-based LAN Airlines, agreed Feb. 4, 2016, to pay $75,000 to settle Securities and Exchange Commission (SEC) charges of violating the Foreign Corrupt Practices Act (FCPA) by authorizing improper payments to a consultant in connection with a union dispute in Argentina.

In 2006 and 2007, Cueto allegedly authorized $1.15 million in payments in connection with LAN's attempts to settle disputes on wages and other work conditions between a LAN subsidiary, LAN Argentina S.A., and its employees, SEC charged.

"At the time, Cueto understood that it was possible the consultant would pass some portion of the $1.15 million to union officials in Argentina. The payments were made pursuant to an unsigned consulting agreement that purported to provide services that Cueto understood would not occur," the SEC order noted.

Specificially the contract "falsely stated that the consultant would undertake a study of

existing air routes in Argentina and the regional market as a basis for the payment. The draft contract was never signed by the parties. Cueto knew that the consultant would not perform a study," it said.

"Cueto approved the payments to get the unions to abandon their threats to enforce the single-function rule and to get them to accept a wage increase lower than the amount asked for in negotiations," it said. "In 2006, LAN did not have a policy requiring that due diligence be performed on consultants, and neither Cueto nor LAN conducted any due diligence on the consultant or any of his related entities" the SEC order added.

Neither Cueto nor LAN conducted any due diligence on the consultant

"Cueto authorized subordinates to make the payments that were improperly booked in the Company's books and records, which circumvented LAN's internal accounting controls," it added.

DUTCH TELECOM FIRM SETTLES CHARGES OF UZBEK BRIBERY

Amsterdam-based telecommunications firm VimpelCom Limited and its subsidiary in Uzbekistan, Unitel LLC, agreed Feb. 18, 2016, to settle charges of conspiracy to violate the Foreign Corrupt Practices Act (FCPA) by making corrupt payments to Uzbek government officials from 2004 through 2012.

In the criminal case, Unitel pleaded guilty in Manhattan U.S. District Court to conspiracy to violate the FCPA, and VimpelCom entered into a deferred prosecution agreement (DPA) for conspiracy to violate the anti-bribery and books and records provisions of the FCPA, and a separate count of violating the internal controls provisions of the FCPA.

The companies were charged with making more than $114 million in corrupt payments to officials in the government of Uzbekistan and instrumentalities thereof "to affect or influence acts and decisions of Uzbek government officials or instrumentalities in order to assist the telecom companies in entering and operating in the Uzbek telecommunications market, including by influencing government officials at the Uzbek Agency for Communications and Information," the criminal complaint said.

"The corruption proceeds were laundered through a complex series of monetary transactions, including through bank accounts in Switzerland and the transfer of funds into and out of correspondent banking accounts at financial institutions in the United States," the complaint noted.

Under the DPA, VimpelCom agreed to pay a criminal penalty of $230.1 million to the United States, including $40 million in criminal forfeiture. Under a separate settlement with the Securities and Exchange Commission (SEC), VimpelCom agreed to a total of $375 million in disgorgement of profits and prejudgment interest, to be divided between the SEC and the Dutch Public Prosecution Service (Openbaar Ministrie, or OM). VimpelCom also agreed to pay OM a criminal penalty of $230.2 million, which Justice agreed to credit as part of its agreement with the company.

"These cases combine a landmark FCPA resolution for corporate bribery with one of the largest forfeiture actions we have ever brought to recover bribe proceeds from a corrupt government official," said Assistant Attorney General Leslie Caldwell said in a statement.

"Resolving this has been a top priority for VimpelCom. While this has been a very challenging experience for our business and our employees, we are pleased to have now reached settlements with the authorities. The wrong-doing, which we deeply regret, is unacceptable," VimpelCom CEO Jean-Yves Charlier said in a statement. "We have taken, and will continue to take, strong measures to embed a culture of integrity across the group. We have significantly strengthened our internal controls and compliance program," Charlier added.

EXPAT BUSINESSMAN PLEADS GUILTY TO DEFRAUDING EX-IM

The owner of a Florida aircraft brokerage and export business pleaded guilty Feb. 4, 2016, in Tampa U.S. District Court to charges of defrauding the Export-Import (Ex-Im) Bank in 2007.

Martin Slone of Oldsmar, Fla., owner of Woolie Enterprises Inc., admitted to creating false documents claiming that foreign buyers had purchased aircraft and parts for agricultural and passenger services from Woolie.

Slone then reported that the buyers had defaulted on their payments, causing Ex-Im Bank to pay Woolie approximately $197,690. A grand jury returned the original sealed indictment in July 2013, while Slone was residing in Brazil, Justice said.

He originally pleaded not guilty in August 2015, after being arrested at Abu Dhabi International Airport and extradited to the U.S (see *The Export Practitioner*, October 2015, page 10). Sentencing is set for April 7.

HOUSE COMMITTEE BLASTS ADMINISTRATION ON GUN TRANSFERS

During a seemingly benign House Small Business Committee hearing Feb. 11, 2016, on the progress of export control reform, committee members took the opportunity to press the Obama administration on what is left to be done: the transfers of firearms and ammunition from the U.S. Munitions List (USML) to the Commerce Control List (CCL).

The department is committed to finalizing an initial review of the entire USML in 2016

In response to relentless grilling by Rep. Tim Huelskamp (R-Kan.), Deputy Assistant Secretary of State Brian Nilsson argued that the prioritization of transfers was set early on. "The categories that we've been doing have been based on those that provide the best benefit for interoperability with our key allies. We've been systematically working through those," Nilsson told the hearing.

This argument contradicts common wisdom about those transfers. Administration officials previously have acknowledged the proposed rules for those transfers were drafted, but pulled back in 2012 after the mass shootings in Aurora, Colo., and Newtown, Conn.

At the urging of gun industry groups, members of Congress from both parties have urged the Obama administration to complete the reforms (see *The Export Practitioner*, December 2015, page 12).

"At this time, the Department's primary focus, as well as that of our interagency partners, is to finalize the significant number of proposed rule-makings currently in process, which include revisions to USML Categories XII and XIV. Nonetheless, the Department is committed to finalizing an initial review of the entire USML in 2016," wrote Assistant Secretary of State for Legislative Affairs Julia Frifield in a response Feb. 5 to one of these letter-writers, Sen. David Perdue (R-Ga.).

However rational, this explanation fell flat at the House hearing. "I just hammered Obama administration on playing politics & hurting gun & ammo manufacturers," Huelskamp later tweeted, along with a link to the video on his YouTube channel.

Committee Chairman Steve Chabot (R-Ohio) also joined the fray, telling the hearing, "The chair would just note that there's considerable suspicion by many members, that this administration, because it's not particularly considered to be a friend of guns or ammo, that this is sort of 'willful neglect' on their part, at least."

U.S. WILL RENEGOTIATE WASSENAAR CYBER CONTROLS

After months of angry letters, congressional testimony and overwhelming industry opposition, the Obama administration announced it will go back to the table at the Wassenaar Arrangement and renegotiate agreed-upon controls on cybersecurity products.

Specifically, the U.S. will propose to eliminate the controls on technology required for the development of "intrusion software." The administration will also continue discussions, both domestically and with Wassenaar partners, "aimed at resolving the serious scope and implementation issues raised by the cybersecurity community concerning remaining controls on software and hardware tools for the command and delivery of 'intrusion software.' Commerce Secretary Penny Pritzker wrote in a letter to industry groups March 1, 2016.

"Because changes in Wassenaar controls must be approved by all 41 members, we cannot predict the outcome of these discussions and negotiations," she wrote. In any case, the administration commits that it "will not implement domestically any regulations on these specific controls without first giving the public an opportunity to participate through the notice and comment process of a proposed rule," Pritzker added.

Those discussions will start in April and continue over the summer, a senior Commerce official told The Export Practitioner. Talks could go in a number of ways, the official said; either leave the agreed control language as is, remove the controls completely, or amend the text slightly and repropose rule changes. "We heard a lot of good ideas, so we'll see where that goes," he said.

The administration will do a cost-benefit analysis as to "whether the benefits of controlling the export of the purpose-built tools at issue outweigh the harms to effective U.S. cybersecurity operations and research," the official added.

Pritzker was responding to a letter in which the Information Technology Industry Council (ITIC) and 11 other trade associations, including the Chamber of Commerce, American Petroleum Institute, and National Association of Manufacturers, asked her, Secretary of State John Kerry, and Homeland Security Secretary Jeh Johnson to renegotiate the controls.

"While we agree with the laudable goals of the Wassenaar Arrangement, we write today to emphasize the broad range of industries whose cybersecurity efforts would be undermined by the implementation of these provisions in the United States and abroad. Given the cross-border nature of cyber threats, we urge you to pursue a renegotiation of the 2013 Plenary provisions to avoid interference with global cybersecurity efforts," the groups wrote.

Congress and Industry Joined Chorus

Earlier in February, eight members of the House Oversight and Homeland Security committees wrote a letter to Kerry saying "We unambiguously expect that the U.S. Department of State will work to renegotiate the controls at the Wassenaar plenary."

The two committees held a hearing on the issue in January (see *The Export Practitioner*, February 2016, page 11). "According to testimony received at the hearing, addressing this issue through U.S. policy alone would not be enough due to the cross border nature of cyber threats," the letter read. "Furthermore, the language of the Arrangement itself appears to preclude an interpretation that allows for legitimate cybersecurity activities," it noted.

Industry and congressional response to the administration's decision was quick. "Of course, this isn't the end of the road. There is no guarantee that the 40 other nations who participate in the Wassenaar Arrangement will agree, but for now, we are enjoying this important victory," Electronic Frontier Foundation (EFF) wrote in a blog post Feb. 29.

"Today's announcement represents a major victory for cybersecurity here and around the world. While well-intentioned, the Wassenaar Arrangement's 'intrusion software' control was imprecisely drafted, and it has become evident that there is simply no way to interpret the plain language of the text in a way that does not sweep up a multitude of important security products," Congressional Cybersecurity Caucus cochair Rep. Jim Langevin (D-R.I.) said in a statement.

"By adding the removal of the technology control to the agenda at Wassenaar, the Administration is staking out a clear position that the underlying text must be changed. Furthermore, the Administration leaves open the possibility for further alterations to the control pending additional interagency review," wrote Langevin.

There is no guarantee that the 40 other nations who participate in the Wassenaar Arrangement will agree

Langevin and 124 other members wrote to National Security Advisor Susan Rice in December 2015 and heard what they needed to hear in a letter made public by Langevin in February. "The Administration is committed to taking into account the impact that any export control rule relating to cyber technology may have on our national security and adequately considering the burden that such a rule may place on legitimate cybersecurity activities," Special Assistant to the President Caroline Tess, on behalf of Rice, wrote in her response.

"To that end, we have intensified our engagement with experts and stakeholders from the U.S. government and industry on how to mitigate the national security risks posed by the proliferation of cyber tools in a manner consistent with promoting cybersecurity," Tess wrote.

BIS WILL REQUIRE OFFSET REPORTS FOR 600 SERIES

Hearing crickets from industry, Bureau of Industry and Security (BIS) is going forward with its plan to require U.S. defense exporters to report offsets for items moved to Commerce jurisdiction under export control reform.

BIS proposed requiring reporting of offsets involving items controlled in the new "600 series" Export Control Classification Numbers (ECCNs) in December and did not receive a single public comment (see *The Export Practitioner*, January 2016, page 16).

The reporting would be required "regardless of whether the item was added to a 600 series ECCN simultaneously with its removal from the USML or was subject to the EAR prior to its inclusion in a 600 series ECCN," BIS said in the

Federal Register March 1, 2016.

The proposal would exclude "certain submersible and semi-submersible cargo transport vessels and related items that are not on control lists of any of the multilateral export control regimes of which the United States is a member," the agency noted.

Proposal would exclude certain submersible and semi-submersible cargo transport vessels

AGENCIES PROPOSE MORE CHANGES TO CONTROLS ON AIRCRAFT, ENGINES

As part of the agencies' ongoing review of their respective regulations under export control reform, the Bureau of Industry and Security (BIS) and State's Directorate of Defense Trade Controls (DDTC) proposed another round of clarifications Feb. 9, 2016, to U.S. Munitions List categories VIII (aircraft) and XIX (gas turbine engines) and the accompanying 600 series on the Commerce Control List (CCL).

These transfers were the first to go into effect in October 2013, and BIS and DDTC had asked for comments on the anniversary of the implementation. Comments on the latest changes are due by March 25.

Most of the changes were technical, adding a note or clarifying text to the existing regulations or to individual Export Control Classification Numbers (ECCNs). For example, BIS added a "note stating that forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as commodities controlled by the ECCN in which the note appears (or by specified paragraphs in that ECCN) are controlled by that ECCN."

Other changes include clarifying that ECCN 9A610 would expand to control gauges and indicators and mirrors wherever they are located on the aircraft, all types of fluid filters and filter assemblies—not just hydraulic, oil and fuel system filters and filter assemblies, as well as fluid hoses, straight and unbent lines, fittings, couplings, clamps and brackets.

In its proposed rule, DDTC responded to comments about specific definitions, including "attack helicopter," "armed" and "military." In those cases, the agency argued the definitions were "sufficiently clear and understood by the public."

Commenters also argued for the removal of the term "specially designed" in some text. "The Department accepts this edit to the fullest extent possible, but notes that 'specially designed' exists in recognition of the fact that an enumeration of specific technical parameters may prove too complex or unwieldy to produce a useful regulation in some cases," it wrote.

DDTC also proposed revising its regulations to clarify that the Category VIII controls for all paragraphs are applicable "whether manned, unmanned, remotely piloted, or optionally piloted," its notice said. For example, commenters argued that the control in paragraph (a)(13) is "overly broad and captures all optionally piloted aircraft, including aircraft that would otherwise be controlled by the EAR," it wrote.

DDTC said it accepted these comments and deleted the paragraph, while revising paragraph VIII(a) to capture all optionally piloted variants of the aircraft listed in that paragraph.

BIS, DDTC HEED COMMENTS ON NIGHT-VISION TRANSFERS

Responding to overwhelming industry input, the two main export control agencies reproposed parallel rules Feb. 19, 2016, amending night-vision controls under U.S. Munitions List (USML) Category XII and the Commerce Control List (CCL) 600 series.

As predicted, the Bureau of Industry and Security (BIS) and State's Directorate of Defense Trade Controls (DDTC) proposed reverting to the old use of "specially designed" to differentiate between military and commercial thermal-imaging products.

Final rules could be published by June or July 2016, BIS Deputy Assistant Secretary Matthew Borman predicted in January (see *The Export Practitioner*, February 2016, page 11). That has traditionally been the cutoff for regulatory changes in an election year. Comments on the second proposed rules are due April 4.

Rules Define Design Intent, End-User

"In response to a high number of substantive public comments, certain articles will be controlled based on the design intent of the manufacturer," DDTC said in its notice. "This was decided because the Department found that certain articles could be used as components or as end items for the same military application," it added.

"While applying the standard terminology 'specially designed for a defense article' would apply to articles that operate as a component for a higher-level assembly, that terminology would not describe the same articles when used as end items on their own for the same military purpose," DDTC noted.

The State rule also added a new note defining what constitutes a military end-user, specifically "the national armed services, National Guard, national police, government intelligence or reconnaissance organizations, or any person or entity whose actions or functions are intended to support military end uses."

"An item is specially designed for a military end user if it was created for use by a military end user or users. If an item is created for both military and non-military end users, or if the item was created for no specific end user, then it is not specially designed for a military end user," DDTC said in its proposed rule.

"Contemporaneous documents are required to support the design intent; otherwise, use by a military end user will establish that the item was specially designed for a military end user," it noted.

Proposed Changes Aim to Clarify Controls

In addition to clarifying controls on certain products based on design intent, the rules proposing transfers from the USML to the CCL make several other changes to its previous proposed rule from May 2015.

For example, the agencies do not "propose to amend part 742 to create a new worldwide Regional Stability (RS) control for dual-use items but would maintain a new worldwide RS control for certain military technology," BIS wrote.

"All other items described in this proposed rule that are or would be subject to RS controls would generally be subject to an RS Column 1 control, which imposes a license requirement for all destinations except Canada," it added.

On the USML side, the State rule would add more than 50 new paragraphs enumerating the specific items under its jurisdiction, listing such items as fire control systems, laser spot trackers, helmet mounted display (HMD) systems, targeting or target location systems, and infrared imaging systems.

Contemporaneous documents are required to support the design intent

The BIS rule also proposes new revisions to the Export Administration Regulations (EAR) that were not included in the May 2015 proposed rule. "In order to make the EAR more consistent and easier to apply, this proposed rule would revise various parts of the EAR related to certain QRS-11 sensors and to license requirements related to uncooled thermal imaging cameras," BIS said.

In the latest rule, BIS also proposed revising several specific Export Control Classification Numbers (ECCNs), including: 0A987, optical sighting devices for firearms; 2A984, concealed object detection equipment; 6A004, optical equipment and components; 6A005, lasers, components, and optical equipment; 6A007, gravity meters and gravity gradiometers; 6A008, radar systems, equipment, and assemblies; 6A107, gravity meters and gravity gradiometers; 7A001, accelerometers; 7A002, gyros or angular rate sensors; 7A003, inertial measurement equipment or systems; 7A005, Global Navigation Satellite Systems receiving equipment; 7A101, accelerometers; and 7A102, gyros.

Unlike the previous proposals, this proposed rule would create only one set of 600-series ECCNs corresponding to USML Category XII rather than two sets, BIS said. "The May 5 proposed rule included a 6x615 series for military fire control, range finder, and optical items and a 7x611 series for military guidance and control items. In order to simplify controls, this proposed rule would only establish one set of 600 series ECCNs, the 7x611 series, which would correspond to all items proposed for control under USML Category XII," it noted.

The return to "specially designed" caused other domino effects in the BIS rule. "Due to the elimination of the term "permanent encapsulated sensor assembly" as a parameter for determining jurisdiction for focal plane arrays in DDTC's proposed rule, this proposed rule also

does not include the definition for that term in part 772, as proposed in the May 5 proposed rule. This rule also removes references to that term that were proposed to be included in ECCN 6A002," the agency said.

The return to "specially designed" caused other domino effects

"This proposed rule also does not include controls proposed in the May 5 proposed rule for certain maintenance, repair, or overhaul software or technology related to certain dual-use infrared detection commodities. Such controls, which were proposed in new ECCNs 6D994 and 6E994, would exceed those of the Wassenaar Arrangement, and based on public comments, would likely have resulted in extensive license requirements for purely commercial activities, such as civil automotive repair," BIS said.

Industry Approves of Changes

Observers seem hopeful that the proposed regulations will "enable U.S. industry to continue to lead the way in technology development and also compete worldwide," one industry source told The Export Practitioner. "It's not perfect, but it adds significant clarity to a confusing technology area," he noted.

Industry groups, including SPIE, the international society for optics and photonics, also applauded the changes. "The interim rule utilizes the 'specially designed' criteria in many areas, which was a request from industry and SPIE. The 'specially designed' criteria, which is a formal review process finalized in 2012, helps ensure that dual-use technologies are not considered munitions items," explained Jennifer Douris, SPIE Government Affairs Director, in a statement.

Though today's proposed rule is a significant improvement from the previous proposal, companies and universities should still review the proposals carefully for potential impacts, Douris said.

BIS SEES INCREASE IN PROPOSED FY2017 BUDGET

The cliché is wrong. Someone hears the tree falling in the forest, but probably will not do anything about it. President Obama unveiled his $4.15 trillion budget for Fiscal Year (FY) 2017 Feb. 9, 2016, which includes a budget increase for the Bureau of Industry and Security (BIS) to handle increased licensing. Unfortunately, House and Senate budget committees will not hold hearings on the proposal.

The proposed budget allots $127 million for BIS. That number is $15 million more than the FY2016 enacted level, and "will augment domestic and international efforts to curtail illegal exports while facilitating secure trade with U.S. allies and close partners," according to Commerce's budget brief. The additional monies are meant to support the completion of BIS' export control reform (ECR).

BIS staff levels "are not in line with growth in export license applications and enforcement activities," a preliminary study by outside experts to examine BIS' workforce found. The budget brief also described BIS employees as having "reached the tipping point."

To alleviate this shortfall, BIS requested a $3.305 million increase and 13 full-time equivalents (FTEs), bringing the total Export Administration (EA) request to $64.54 million and 227 FTE.

The additional funding and FTE are needed to evaluate the "tens of thousands" of items specially designed for military applications that are moving from the purview of State to Commerce under the terms of the ECR. Ten FTEs will be dedicated to licensing and other reviews, and three will be analytical staff to support the growing number of Defense Production Act industrial base surveys and assessments.

Export Enforcement (EE) has requested an additional $4.115 million and 2 FTEs: $1.6 million for productivity improvement, $1.702 million for the export control officer and end-use check program, and $.8 million and 2 FTEs to support the Information Triage Unit (ITU) expansion. ITU was established as part of ECR.

Budget Committees Ignore Proposal

Neither chamber of Congress will hold hearings with the Director of the Office of Management and Budget, committee chairmen Rep. Tom Price (R-Ga.) and Sen. Mike Enzi (R-Wyo.) said Feb. 4.

"Rather than spend time on a proposal that, if anything like this Administration's previous budgets, will double down on the same failed policies that have led to the worst economic recovery in modern times, Congress should continue our work on building a budget that balances and that will foster a healthy economy," Price said in a prepared statement.

Committee Democrats took issue with this in a letter to Enzi Feb. 9. "This year, with no unusual circumstances to prevent us from doing our work, we have been provided with no reasonable explanation for the decision not to hold a hearing. Furthermore, this decision runs counter to repeated calls by the majority for regular order in the Senate. Instead, we are faced with overt partisanship when we should be addressing important issues that face our country," the members wrote.

TREASURY, STATE OFFICIALS GRILLED ON IRAN SANCTIONS

The Joint Comprehensive Plan of Action (JCPOA) opens up opportunities for international banks and companies to do legitimate business with Iran, but the U.S primary embargo on Tehran is still in place, Obama administration officials told the House Foreign Affairs Committee Feb. 11, 2016. Officials also refuted claims that European banks and companies are doing business with blocked Iranian entities.

OFAC found no evidence of any European banks doing business with Mahan Air

Despite the assurances, the two-hour long hearing was filled with questions on people and entities subject to sanctions. Rep. Ted Deutch (D-Fla.) queried Acting Director of Treasury's Office of Foreign Assets Control (OFAC) John Smith about the number of individuals on the Specially Designated Nationals (SDN) list subject to secondary sanctions.

"You're saying that of the 400 individuals and entities who were listed in the agreement, 200 of them are still being sanctioned for terrorism and human rights violations?" he wondered.

"I should clarify this," Smith said. "We removed 400 from the list because they were not related to terrorism, human rights abuses, ballistic missiles or others. Two hundred of those were marked by the Treasury Department before as Government of Iran or Iranian financial institution. We still in the United States, our U.S. persons are still obligated to block and do no transactions with anyone that is identified as the Government of Iran or Iranian financial institution." Those 200 persons and entities are on a separate OFAC list for U.S. persons, he added.

Rep. Brad Sherman (D-Calif.) got into a heated exchange with Smith regarding the fact that "zero point zero" European entities have been slapped with secondary sanctions for doing business with the Iran Revolutionary Guard Corps (IRGC). When Smith said, "I have not seen evidence of European actors continuing to do business with the IRGC," Sherman visibly expressed disbelief.

Sherman was further angered when questioning Smith about the U.S. government's work to prevent Mahan Air, a blocked Iranian airline, from landing in European cities. "We're relying on the executive branch to enforce this deal because you are able to monitor what Iran does and here's an example where you have a major airline doing business in dozens of cities and you can't find them doing business with a single bank?" Sherman said.

Smith said OFAC found no evidence of any European banks doing business with Mahan Air. The Iranian airline was designated by Treasury in 2011 for providing "financial, material and technological support" to the IRGC. Mahan Air purchases planes built by Boeing and Airbus through third parties due to U.S. sanctions.

In light of recent reports that European countries have entered into tentative business deals with Iran, Rep. Lois Frankel (D-Fla.) asked Smith and Ambassador Stephen Mull, lead coordinator at State for the implementation of the Iran nuclear deal, how realistic it is that U.S. allies will "snap back" sanctions should Iran cheat.

Mull was confident that Europe would side with the U.S. Noting that "we've been down this road before," Mull said that when "[we say] either you do business with Iran or you do business with us and every single time they choose us."

During a similar line of questioning from Rep. Eliot Engel (D-N.Y.), Smith replied, "I fully expect that Europe is going to continue to be a committed partner with us." Europe has "sacrificed" economic ties with Iran in the past, he added.

House Passes Iran Legislation

In a repeat of a vote vacated in mid-January, the House passed legislation Feb. 2 that would restrict President Obama's ability to lift sanctions on Iran as outlined in the Joint Comprehensive Plan of Action (JCPOA).

The Iran Terror Finance Transparency Act (H.R. 3662) passed with a vote of 246-181. The vote split overwhelmingly along party lines with only three Democrats crossing the aisle to vote with Republicans in favor of passage.

The bill bars the president from removing financial institutions from OFAC's SDN list until the administration certifies to Congress that the institutions have not "knowingly facilitated" transactions or provided financial

services that benefit Iran's Revolutionary Guard, proxy terrorist organizations, or Iranian efforts to produce weapons of mass destruction. The president must also certify that the institution no longer knowingly engages in "illicit or deceptive financial transactions" or activities.

President Obama has promised to veto the legislation, going so far as to issue a Statement of Administration Policy (SAP) from the Office of Management and Budget (OMB) decrying the bill as undermining the JCPOA (see *The Export Practitioner*, February 2016, page 15). The bill was sent to the Senate Banking Committee.

"The President has repeatedly said that violators on the terror and human rights sanctions lists would not gain relief due to the Joint Comprehensive Plan of Action, also known as the Iran Nuclear deal. We agree," Rep. Steve Russell (R-OK), who introduced H.R. 3662, said in a statement.

"All this bill does is ask for justifications from the administration for why more than 50 entities and individuals have been selected to be delisted from these sanctions lists, and certify they are no longer associated with human rights abuse or terror," he said.

VERIFICATION OF IRAN DEAL COULD POSE CHALLENGES, GAO SAYS

While administration officials are hailing the success of the Iran nuclear deal, the International Atomic Energy Agency (IAEA) could face challenges in monitoring and verifying Iran's implementation of the Joint Comprehensive Plan of Action (JCPOA), according to a preliminary Government Accountability Office (GAO) report made public Feb. 23, 2016 (GAO-16-417).

These challenges include "(1) the inherent challenge of detecting undeclared nuclear materials and activities, (2) potential access challenges to sites in Iran, and (3) safeguards resource management challenges," the report said. GAO said it is not making recommendations at this time and expects to issue a final report later this year.

Despite these challenges, the IAEA issued its first quarterly report Feb. 26, hailing Iran's cooperation with agency inspectors. "The Agency continues to verify the non-diversion of declared nuclear material at the nuclear facilities and locations outside facilities where nuclear material is customarily used (LOFs) declared by Iran under its Safeguards Agreement," the agency wrote.

"The Agency has conducted continuous monitoring, including through the use of containment and surveillance measures, and verified that the declared equipment has been used for the production of rotor tubes and bellows to manufacture centrifuges only for the activities specified in the JCPOA," the IAEA reported.

IAEA has improved its capabilities in detecting undeclared activity

Within the challenges, the GAO report found some positives. IAEA "has improved its capabilities in detecting undeclared activity. For example, according to U.S. government officials and national laboratory representatives, IAEA has adapted its inspector training program to focus on potential indicators of undeclared activity, beyond the agency's traditional safeguards focus on nuclear materials accountancy," it said.

Budget constraints might also pose challenges, GAO found. While officials from State and Energy's National Nuclear Security Administration (NNSA) said that they are confident that IAEA would obtain any funding it would need, "IAEA officials expressed concerns about the reliability of sustained extra-budgetary contributions for IAEA JCPOA activities due to possible donor fatigue in the long run, as IAEA will be conducting certain JCPOA verification activities for 10 or more years," the report said.

Opponents of the Iran nuclear deal were quick to respond to the report. "This preliminary report raises real concerns about putting our national security interests into the hands of a multilateral organization that – although doing its best to meet overburdening new requirements – does not have the capacity, in terms of staff and funding, nor the authorities, in terms of compelling Iran to comply, in order to meets its charge of monitoring and verifying Iran's commitment under the JCPOA," said Sen. Robert Menendez (D-N.J.) in a statement.

CUBA WILL GET PRESIDENTIAL VISIT, TRACTORS, SCHEDULED FLIGHTS

Even without Congressional approval, the Obama administration continued the normaliza-

tion of relations with Cuba, culminating with the announcement Feb. 18, 2016, that the president and first lady will travel to the island March 21-22. At the same time, American manufacturing companies and airlines received official blessings to expand their business to Cuba.

The March trip will be the first time an American president has visited Cuba since Calvin Coolidge came into port aboard a U.S. battleship in 1928. "We want to open up more opportunities for U.S. businesses and travelers to engage with Cuba, and we want the Cuban government to open up more opportunities for its people to benefit from that engagement," White House Deputy National Security Advisor Ben Rhodes wrote in a Medium post.

Ultimately, the Obama administration would like to see Congress lift the trade embargo

Ultimately, the Obama administration would like to see Congress lift the trade embargo, but that does not mean the administration takes lightly the Cuban government's human rights abuses, Rhodes wrote.

At the same time, Cleber LLC, owned by Horace Clemmons and Cuban-born Saul Berenthal, announced Feb. 15 it is set to become the first American company since 1959 to set up a manufacturing plant in Cuba. Treasury's Office of Foreign Assets Control (OFAC) gave the Alabama-based partners permission to open a tractor factory in the Mariel economic zone set up by the Cuban government.

The duo expects to get final approval from the Cuban government in March and they'll begin manufacturing small tractors for Cuban farmers, and possibly for export to other Latin American countries, in early 2017.

Commerce Hosts Second Regulatory Dialogue

If that weren't enough, Commerce and Treasury hosted Cuban Minister of Foreign Trade and Investment Rodrigo Malmierca in Washington Feb. 17-18 for the second round of the U.S.-Cuba Regulatory Dialogue.

Commerce Secretary Penny Pritzker traveled to Cuba for the first round of talks in October. During the dialogue, Pritzker urged her Cuban counterpart to ease restrictions so U.S. companies can invest in the island, while Malmierca maintained that the U.S. embargo is the primary obstacle to trade and investment.

Commerce officials are already planning a third round in May, which "may not be at ministerial level, but it will still include high-ranking officials from the relevant Cuban and U.S. government agencies," Tony Christino, director of the Bureau of Industry and Security's (BIS) Foreign Policy Division, said on a conference call Feb. 23.

For the next round, "BIS has put on the table that we want to discuss with the Cubans their regulatory regimes," Christino said. "When a company initiates a transaction, what sort of wickets do they have to go through?" he added. "We're asking them not only to discuss it with us, but we're asking them to make it easily obtainable by anybody interested," Christino noted.

Christino also explained the effect the regulatory dialogue is already having on the administration's Cuba policy. "The major change [in January] was the recognition by the U.S. government, including as a result of the first round of the regulatory dialogue held in Havana… that in order to meet the needs of the Cuban people, we could not ignore the state sector in Cuba," he told the conference call.

"So we wrote a licensing policy that allows for case-by-case review of certain categories of items that are for the use and benefit of the Cuban people but are provided by Cuban state-owned enterprises," Christino said.

Officials Ink Airline Deal

Travel to Cuba will also become significantly easier. Transportation Secretary Anthony Foxx and Assistant Secretary of State for Economic and Business Affairs Charles Rivkin traveled to Cuba Feb. 16 to sign an arrangement that re-establishes scheduled air service between the U.S. and Cuba (see *The Export Practitioner*, January 2016, page 17).

Under the arrangement, each country can operate up to 20 daily roundtrip flights between the U.S. and Havana, up to 10 daily roundtrip flights between the U.S. and Cuba's nine other international airports, for a total of up to 110 daily roundtrip flights. Travelers must still officially fall into one of 12 categories approved

by OFAC.

"Reestablishing a strong and vibrant aviation partnership after 50 years is understandably a complex and challenging task with many legal and logistical obstacles to overcome," Rivkin said in a statement. "In that respect, I thank and commend the representatives of both governments who have worked diligently since the first round of aviation talks last March."

Obama's actions have been met with resistance from both sides of the aisle. Rep. Ileana Ros-Lehtinen (R-Fla.) called Obama's upcoming visit "shameful" and Sen. Robert Menendez (D-N.J.) said, "It is totally unacceptable for the President of the United States to reward a dictatorial regime with an historic visit when human rights abuses endure and democracy continues to be shunned." Following the stop in Cuba, Obama and his wife will travel to Argentina to meet with that country's new president.

WIPO WHISTLEBLOWERS DESCRIBE ILLEGAL TECHNOLOGY TRANSFERS

Former officials at the World Intellectual Property Organization (WIPO) got their day in court Feb. 24, 2016, or at least Congress, to air their complaints against Director-General Francis Gurry. In what one observer called political theater, members of three House Foreign Affairs Committee subcommittees were regaled with stories of illegal technology transfers to North Korea and Iran, secret meetings with Beijing and Moscow and retaliation against whistleblowers.

Of most concern, but not fully resolved, was whether the transfer of high-end computer equipment to Pyongyang, which Gurry authorized, violated United Nations (UN) sanctions or U.S. export control laws.

The equipment, including a HP server, a printer worth $14,000, a 24-terabyte disk array and a SonicWall firewall, was "transferred ostensibly in order to support the North Korean patent office in its efforts to modernize its technology," former WIPO Deputy Director James Pooley explained at the hearing.

The equipment included a HP server, a printer worth $14,000, a 24-terabyte disk array and a SonicWall firewall

When asked if this equipment could be bought legally in the U.S. or on Amazon, Pooley responded, "Yes, I suppose it could have been purchased in the U.S., but you can't buy it to send to North Korea. If you did, you'd go to prison for a long time."

In 2012, the UN Sanctions Committee found that the technical assistance to North Korea and Iran did not violate UN resolutions. UN lawyers "determined that when you parse the Security Council sanctions very carefully, the kind of equipment here was not radiation hardened or otherwise of the sort that would necessarily apply. There are lawyers who might disagree, but that was the finding," Pooley said.

Rep. Brad Sherman (D-Calif.) discarded this report. "What Mr. Gurry did is contrary to the national security interests of the United States, and he obviously did not care whether he was violating UN sanctions. Even as a technical matter, he can come back after the fact and point to some loophole," he said.

STATE DEFENDS STANCE ON GUN BLUEPRINTS APPEAL

In a case that has angered gun owners and free speech groups, the State Department and its Justice lawyers defended its authority under the International Traffic in Arms Regulations (ITAR), filing a brief Feb. 11, 2016, in *Defense Distributed v. U.S. Department of State* in the U.S. Fifth Circuit Court.

This case does not involve university lectures or discussions of matters of theoretical interest at a dinner party

The lawsuit got a boost in December when conservative lawmakers and free-speech groups, including the Electronic Frontier Foundation and Cato Institute, filed amicus briefs in support of the plaintiff (see *The Export Practitioner*, January 2016, page 20).

In May 2013, the Directorate of Defense Trade Controls Compliance (DTCC) asked Defense Distributed, an online weapons retailer, to pull gun blueprints off its website, saying it could violate the Arms Export Control Act (AECA). Defense Distributed and the Second Amendment Foundation filed for an injunction to block DDTC's action in May 2015 in Austin, Texas, U.S. District Court. The district court denied the injunction, but the company appealed that ruling to the circuit court.

Defense Distributed argued the injunction violated its both first and second amendment rights. "Plaintiffs' constitutional claims are … without merit. Plaintiffs' First Amendment argument misunderstands the nature of the licensing scheme and ignores the context of the Department's actions here. The licensing scheme does not target plaintiffs' ability to express ideas, but rather applies here only because the computer files at issue direct a computer to produce firearm components," State responded.

"This case does not involve university lectures or discussions of matters of theoretical interest at a dinner party. Rather, the regulation's application in this case involves the dissemination of computer files to foreign nationals that can be used, automatically, to generate firearms or firearm components that are on the U.S. Munitions List," it noted.

"Plaintiffs' reliance on the Second Amendment is misplaced. The only limitation at issue here concerns the placement of certain computer data files on an unrestricted Internet site. Nothing in the statute or regulations prevents American citizens on U.S. soil from obtaining the files directly from Defense Distributed, much less from obtaining a firearm from other sources or from possessing a firearm for self-defense," State added.

"In addition, plaintiffs are mistaken in arguing that the State Department's processing times render the scheme an impermissible prior restraint. Plaintiffs have not sought a license in this case and present only general arguments about the pace of licensing decisions, without any concrete factual context. Moreover, on its face, the licensing determination appropriately involves considerations of numerous difficult questions of national security or foreign policy," it wrote.

U.S., EU RELEASE PRIVACY SHIELD FRAMEWORK, TEXTS

U.S. and European Union (EU) officials Feb. 29, 2016, moved one step closer to implementing a new transatlantic agreement on rules for the transfer of personal data to the U.S. from Europe. The two partners released the formal texts and multiple annexes of EU-U.S. Privacy Shield framework agreed in February (see *The Export Practitioner*, February 2016, page 25).

The text includes the "Privacy Shield Principles" companies have to abide by, as well as written commitments by the U.S. government on the enforcement of the arrangement, including assurance on the safeguards and limitations concerning access to data by public authorities. These principles include notice, choice, security, data integrity and purpose limitation, access, accountability for onward transfer, recourse, enforcement and liability.

To join the framework, U.S. companies will be required to self-certify to Commerce and publicly commit to comply with the framework's requirements. "While joining the Privacy Shield Framework will be voluntary, once an eligible company makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law," a Commerce fact sheet noted.

At the same time, the European Commission (EC) also made public a draft "adequacy

decision" of the new framework "Once adopted, the Commission's adequacy finding establishes that the safeguards provided when data are transferred under the new EU-U.S. Privacy Shield are equivalent to data protection standards in the EU," the EC press release said.

"The new framework reflects the requirements set by the European Court of Justice in its ruling from 6 October 2015. The U.S. authorities provided strong commitments that the Privacy Shield will be strictly enforced and assured there is no indiscriminate or mass surveillance by national security authorities," it added.

"Now that President Obama has signed the Judicial Redress Act granting EU citizens the right to enforce data protection rights in U.S. courts, we will shortly propose the signature of the EU-U.S. Umbrella Agreement ensuring safeguards for the transfer of data for law enforcement purposes. These strong safeguards enable Europe and America to restore trust in transatlantic data flows," EU Commissioner for Justice, Consumers and Gender Equality Vera Jourová said.

President Obama signed Feb. 24 the Judicial Redress Act (H.R. 1428) to provide European citizens a legal way to bring complaints in U.S. courts against the breach of their privacy. The bill passed the Senate Feb. 9 by unanimous consent. A day later, the House agreed to the Senate amendment without objection. Enactment of the bill had been one of the EU demands in the Safe Harbor negotiations.

Next Steps

With the text released and the signatures dry, the European Commission "will shortly propose the signature of the Umbrella Agreement. The decision concluding the Agreement should be adopted by the Council after obtaining the consent of the European Parliament," a Commission press release said.

In a January speech Jourová reiterated that negotiators have completed work on an "Umbrella Agreement" on data protection. "We are now in a crucial moment in our negotiations on a successor arrangement for data transfers between companies," she noted at the time.

In addition, a "committee composed of representatives of the Member States will be consulted and the EU Data Protection Authorities (Article 29 Working Party) will give their opinion, before a final decision by the College," the Commission noted. "In the meantime, the U.S. side will make the necessary preparations to put in place the new framework, monitoring mechanisms and the new Ombudsperson mechanism," it added.

To join the framework, U.S. companies will be required to self-certify to Commerce

"We hope the Framework moves swiftly through the EU approval process, so companies and individuals on both sides of the Atlantic can continue to ensure a high-level of data protection," Commerce Secretary Penny Pritzker said in a statement.

Industry Urges Quick Approval

Industry groups also hoped for a quick approval process. "We're hopeful that, with the release of the Privacy Shield details, European leaders will move quickly to fully consider and approve the agreement. The Privacy Shield creates an essential legal and political foundation for the free flow of data across the Atlantic," Mark MacCarthy, senior VP of public policy at the Software & Information Industry Association (SIIA), said in a statement.

"After our initial review, it appears that the two sides have achieved the objective of securing an agreement that both enhances privacy protections and provides the certainty needed to promote innovation and economic growth," Josh Kallmer, senior VP for global policy for Information Technology Industry Council (ITIC), noted.

"We will be reviewing the text more thoroughly in the coming days, and we look forward to engaging with officials in the U.S. government, the European Commission, Member State governments, and EU data protection authorities (DPAs) to support the implementation of this new arrangement," Kallmer said.

END NOTES

ENTITY LIST: BIS in Federal Register Feb. 23, 2016, added eight persons in UAE to Entity List. Four additions "have been involved in supplying U.S.-origin items to persons designated by the Secretary of State as Foreign Terrorist Organizations (FTOs)," BIS said. Other four "prevented the successful accomplishment of end-use checks by BIS officials," notice said. Agency also removed nine entities in Ireland and UAE based on information provided by entities in their appeal request and further review conducted by the End-User Review Committee. BIS also revised six entries in Iran, Armenia, Greece, India, Pakistan and UK.

NORTH KOREA: President Obama signed Feb. 18, 2016, North Korea Sanctions and Policy Enhancement Act of 2016 (H.R. 757). House adopted Feb. 12 Senate amendment to bill, which Senate voted 96-0 two days before. House passed legislation, introduced by Rep. Ed Royce (R-Calif.) in response to Pyongyang nuclear test and missile launch in January (see *The Export Practitioner,* February 2016, page 26). "I look forward to the full and aggressive implementation of this new law," Royce said in statement. At same time, South Korea suspended operations at joint-run Kaesong industrial complex and Japan's Prime Minister announced new sanctions.

UK DEFENSE TRADE: DDTC Chief Brian Nilsson traveled to UK for management board meeting on U.S.-UK Defense Trade Cooperation Treaty (DTCT) Jan. 26-30. Board committed to more frequent meetings to respond to industry complaints about treaty implementation.

TRADE PEOPLE: Tina Kaidanow was named acting assistant secretary of State for political-military affairs Feb. 22, 2016, replacing Puneet Talwar, who left government for private sector in November 2015, State official said. Prior to joining bureau, Kaidanow had served since February 2014 as counterterrorism coordinator.

Are you risking high fines and penalties due to violations of Deemed Export Controls?

Mastering Deemed Exports can help you avoid costly mistakes

Mastering Deemed Exports is an invaluable video-training program on deemed exports. It provides an introduction to Deemed Export regulations, an overview of the government agencies that administer them, and the requirements for hiring foreign nationals.

Produced by *The Export Practitioner* and *Spark Media, Inc.*, *Mastering Deemed Exports* should be part of your export compliance training program.

See a preview of *Mastering Deemed Exports* at www.deemedexports.com

Order your copy of *Mastering Deemed Exports* for only $595 with a 30-day, No-Risk guarantee that you can return it for a full refund if you are not totally satisfied.

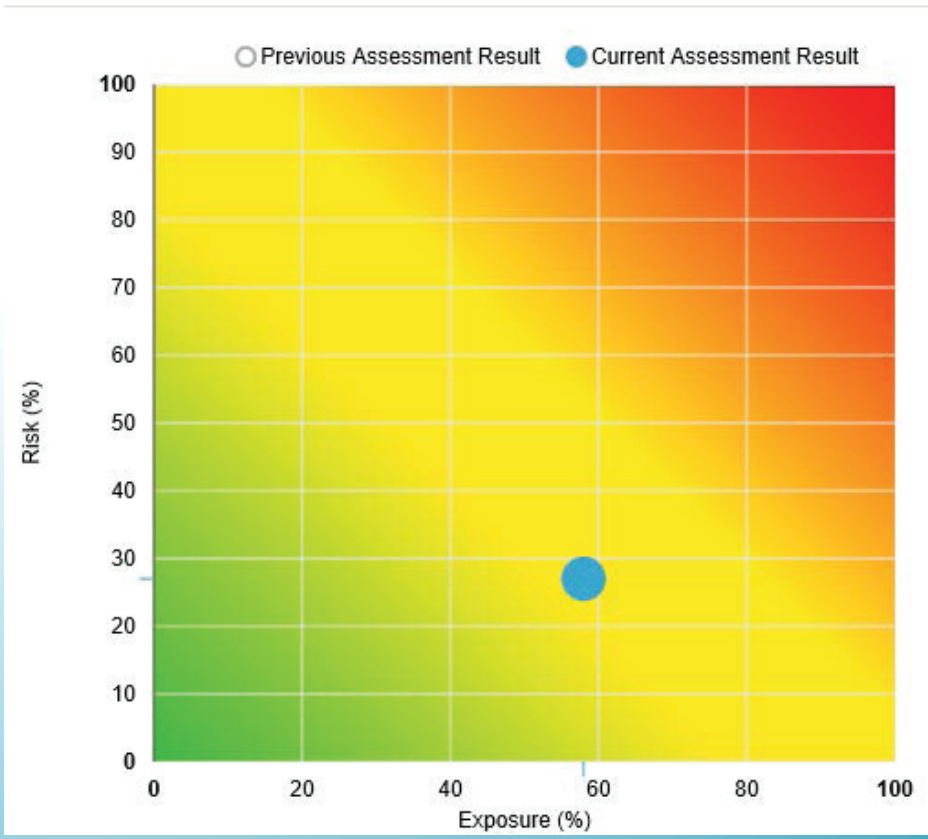
For more information or to order your copy of MASTERING DEEMED EXPORTS Please call 301-460-3060 or Fax your request to 301-460-3086 or E-Mail it to info@deemedexports.com

Trade Compliance Group

TCAT

The Industry's First Automated Trade Compliance Assessment Tool

Quantifies RISK and EXPOSURE



Go online for more information, or call for a free trial account or demo

tcat.tradecompliancegroup.com
www.tradecompliancegroup.com
202-621-5481

Trade Compliance Assessments Have Never Been So Simple SM