MOFO
GLOBAL PROCUREMENT QUARTERLY

Summer/Fall 2014

IN THIS ISSUE

RECENT TRENDS IN FCPA ENFORCEMENT – FIRST HALF OF 2014

By Charles Duross and Hanna Abrams

Although the overall number of corporate cases brought by the government under the U.S. Foreign Corrupt Practices Act (FCPA) has been lower in the first half of 2014 than in previous years, the amount of money the government has collected in penalties has increased significantly. Each of the cases has also been the product of significant cooperation between the U.S. Department of Justice (DOJ) and the U.S. Securities and Exchange Commission (SEC) and their foreign law enforcement counterparts.

This update provides an overview of three key FCPA cases that emerged in the first half of 2014–Alcoa, Marubeni, and Hewlett-Packard. Each of the cases resulted in corporate settlements that involved a significant monetary component: Alcoa ($384 million in total), Marubeni ($88 million in total), and Hewlett-Packard ($108 million in total).

continued on page 2

Alcoa World Alumina LLC

On January 9, 2014, Alcoa World Alumina LLC entered a guilty plea to one count of violating the anti-bribery provisions of the FCPA with a 2004 corrupt transaction.[1] Alcoa World Alumina LLC, a majority-owned subsidiary, agreed to pay a criminal fine of $209 million and forfeit $14 million to settle the DOJ's charges.[2] The company also agreed to maintain and implement an enhanced anti-corruption program.[3] Alcoa Inc., the corporate parent, also agreed to resolve civil charges brought by the SEC by disgorging $161 million.[4] The settlement, totaling $384 million is one of the largest FCPA-related cases in history.[5]

The plea agreement acknowledges that millions of dollars in bribes were paid through a third-party agent to officials of the Kingdom of Bahrain by (1) entering into sham sales agreements with the agent and paying commissions intended to conceal bribe payments, and (2) selling aluminum through offshore shell companies owned by the agent, thereby allowing the agent to increase the prices as a purported distributor and use the money to pay government officials.[6]

In reaching the settlement, the DOJ acknowledged the extensive cooperation it received from international law enforcement agencies, including the Office of the Attorney General of Switzerland, the Guernsey Financial Intelligence Service and Guernsey Police, the Australia Federal Police, and the UK's Serious Fraud Office (SFO).[7]

Marubeni Corporation

On March 19, 2014, the DOJ announced that Japanese trading company Marubeni Corporation had pleaded guilty to one count of conspiring to violate the anti-bribery provisions of the FCPA and seven counts of violating the FCPA.[8] As part of the plea agreement, Marubeni agreed to pay a criminal fine of $88 million.[9] The DOJ cited, among other things, the company's "decision not to cooperate with the department's investigation when given the opportunity to do so, [and] its lack of an effective compliance and ethics program at the time of the offense."[10] This was the second time that Marubeni had been charged with FCPA violations in the past few years.[11]

The plea agreement resulted from a seven-year scheme to pay and conceal bribes to high-ranking government officials in Indonesia in order to obtain a power project.[12] The company attempted to conceal the bribes by using third-party consultants to make the payments to Indonesian government officials.[13]

In reaching this settlement, the DOJ acknowledged the significant cooperation it received from the Indonesian Komisi Pemberantasan Korupsi, the Office of the Attorney General in Switzerland, and the SFO.[14]

Hewlett-Packard

On April 9, 2014, Hewlett-Packard and its various subsidiaries resolved a series of criminal and civil FCPA violations, agreeing to pay more than $108 million in criminal and civil fines.[15] HP's Russian subsidiary pleaded guilty, its Polish subsidiary entered into a deferred prosecution agreement, and its Mexican subsidiary entered a non-prosecution agreement.[16] The three subsidiaries agreed to pay over $76 million in criminal penalties and fines to settle the FCPA violations, and $31.5 million in civil penalties to settle charges brought by the SEC.[17]

The guilty plea noted that employees of the Russian subsidiary had created an off-the-books slush fund containing millions of dollars by selling products to a channel partner of Hewlett-Packard, which in turn sold the products to an intermediary at a markup. The Russian subsidiary then repurchased the products from the intermediary at a markup and paid the intermediary for its purported services. The intermediary transferred most of the payments through shell companies, the bulk of which went to Russian government officials.[18]

In the deferred prosecution agreement with HP Poland, the alleged corrupt conduct was in connection with payments for various contracts with the Polish National Police agency.[19] In the non-prosecution agreement with HP Mexico, HP Mexico acknowledged that it secured contracts to provide hardware, software, and license packages to Mexico's state-owned petroleum company after retaining a third-party consultant who was closely aligned with the petroleum company's senior executives. HP Mexico paid a "commission" to the consultant through a long-standing channel partner who funneled money to a senior official at the petroleum company.[20] The plea agreement acknowledged HP's extensive cooperation with the DOJ's investigation.[21]

In reaching the settlement, the DOJ acknowledged the significant assistance it received from international law enforcement agencies including the Polish Anti-Corruption Bureau, the Polish Appellate Prosecutor's Office, and the Public Prosecutor's Office in Dresden, Germany.[22]

The Future

While the number of overall corporate cases is smaller so far this year, the cases themselves have been among the biggest in history, and there does not appear to be

continued on page 3

any reason to believe that will slow down, as there are a series of highly publicized ongoing investigations, a number of which are reportedly nearing resolution. Moreover, while commentators have long felt the need to analyze "trends" in quarterly or semi-annually assessments, the truth is that these cases are massive, complex, and take many years to conclude; therefore, one should be circumspect before placing too much weight on any one snapshot in time. Aside from the corporate cases, there are a number of FCPA-related cases against individuals moving toward trial in Connecticut, Maryland, New Jersey, and New York, and those contested cases may generate decisions that will impact the legal landscape of FCPA enforcement, possibly in very important ways.

1 Plea Agreement, *United States v. Alcoa World Alumina LLC*, No. 14-cr-00007 (W.D. Pa. Jan. 9, 2014), available at http://www.justice.gov/criminal/fraud/fcpa/cases/alcoa-world-alumina/01-09-2014plea-agreement.pdf.

2 Plea Agreement, *supra* note 1, ¶ 7; *see also* Judgment at 11, 7, *United States v. Alcoa World Alumina LLC*, No. 14-cr-00007 (W.D. Pa. Jan. 9, 2014), http://www.justice.gov/criminal/fraud/fcpa/cases/alcoa-world-alumina/01-09-2014judgment.pdf.

3 Plea Agreement, *supra* note 1, ¶ 9(g).

4 Cease-and-Desist Order at 11, Alcoa Inc., Exchange Act Release No. 71261 (Jan. 9, 2014), *available at* http://www.sec.gov/litigation/admin/2014/34-71261.pdf (ordering Alcoa to disgorge $175 million, but noting that $14 million of the amount was satisfied by the forfeiture payment in the related criminal matter).

5 *See* Dep't of Justice Press Release, "Alcoa World Alumina Agrees to Plead Guilty to Foreign Bribery and Pay $223 Million in Fines and Forfeiture" (Jan. 9, 2014), *available at* http://www.justice.gov/opa/pr/2014/January/14-crm-019.html.

6 Plea Agreement, *supra* note 1, Ex. 3.

7 Press Release, *supra* note 5.

8 Dep't of Justice, Press Release, "Marubeni Corporation Agrees to Plead Guilty to Foreign Bribery Charges and to Pay an $88 Million Fine" (Mar. 19, 2014), *available at* http://www.justice.gov/opa/pr/2014/March/14-crm-290.html.

9 Plea Agreement ¶ 17, *United States v. Marubeni Corp.*, No. 14-cr-052 (D. Conn. Mar. 19, 2014), *available at* http://www.justice.gov/criminal/fraud/fcpa/cases/marubeni-corp/marubeni-corp-plea-agreement.pdf. Marubeni is not an "issuer" within the meaning of the FCPA and, accordingly, there was no parallel SEC action.

10 Press Release, *supra* note 8.

11 Deferred Prosecution Agreement, *United States v. Marubeni Corp.*, No. 12-cr-022 (S.D. Tex. Jan. 17, 2012) (prosecution deferred for two-year period and $54.6 million penalty paid by Marubeni). At the time, the DOJ announced that a four-company joint venture called TSKJ "paid approximately $132 million to a Gibraltar corporation controlled by [a third-party agent] and $51 million to Marubeni during the course of the bribery scheme and intended for these payments to be used, in part, for bribes to Nigerian government officials" to secure $6 billion in contracts to construct liquefied natural gas facilities on Bonny Island, Nigeria. Dep't of Justice Press Release, "Marubeni Corporation Resolves Foreign Corrupt Practices Act Investigation and Agrees to Pay a $54.6 Million Criminal Penalty" (Jan. 17, 2012), *available at* http://www.justice.gov/opa/pr/2012/January/12-crm-060.html.

12 Plea Agreement Ex. 3, *supra* note 9.

13 *Id.*

14 Press Release, *supra* note 8.

15 Dep't of Justice Press Release, "Hewlett-Packard Russia Agrees to Plead Guilty to Foreign Bribery" (Apr. 9, 2014), *available at* http://www.justice.gov/opa/pr/2014/April/14-crm-358.html.

16 Plea Agreement, *United States v. Zao Hewlett-Packard A.O.*, No. 14-cr-00201 (N.D. Cal. Apr. 9, 2014), *available at* http://www.justice.gov/criminal/fraud/fcpa/cases/hewlett-packard-zao/hp-russia-plea-agreement.pdf; Deferred Prosecution Agreement, *United States v. Hewlett-Packard Polska SP Z O.O.*, No. 14-cr-202 (N.D. Ca. Apr. 9, 2014), *available at* http://www.justice.gov/criminal/fraud/fcpa/cases/hewlett-packard-polska/hp-poland-dpa.pdf; Non-Prosecution Agreement, *Hewlett-Packard Mexico, S. de R.L. de C.V.* (Apr. 9, 2014), *available at* http://www.justice.gov/criminal/fraud/fcpa/cases/hewlett-packard-mexico/hp-mexico-npa.pdf.

17 Press Release, *supra* note 15; see also Cease-and-Desist Order, Hewlett-Packard Co., Exchange Act Release No. 71916 (Apr. 9, 2014), *available at* http://www.sec.gov/litigation/admin/2014/34-71916.pdf; Press Release, U.S. Sec. & Exch. Comm'n, "SEC Charges Hewlett-Packard With FCPA Violations" (Apr. 9, 2014), *available at* http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541453075#.VBKH12OZqiw.

18 Plea Agreement Ex. 5, *United States v. Zao Hewlett-Packard A.O.*, No. 14-cr-00201 (N.D. Cal. Apr. 9, 2014), *available at* http://www.justice.gov/criminal/fraud/fcpa/cases/hewlett-packard-zao/hp-russia-plea-agreement.pdf.

19 Deferred Prosecution Agreement, *United States v. Hewlett-Packard Polska SP Z O.O.*, *supra* note 16.

20 Non-Prosecution Agreement, *Hewlett-Packard Mexico, S. de R.L. de C.V.*, *supra* note 16.

21 Press Release, *supra* note 15.

22 Dep't of Justice Press Release, "Hewlett-Packard Russia Agrees to Plead Guilty to Foreign Bribery" (Apr. 9, 2014), *available at* http://www.justice.gov/opa/pr/2014/April/14-crm-358.html.

UKRAINE/RUSSIA–RELATED SANCTIONS

By Nick Spiliotes, Aki Bayz and Betre Gizaw

Overview

As a result of Russia's annexation of Crimea and destabilization of Ukraine, in March 2014, President Obama issued a series of Executive Orders (EOs) authorizing U.S. government sanctions against individuals and entities ("persons") that have contributed to the conflict in Ukraine.[1] Pursuant to the EOs, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) has implemented the Ukraine-related sanctions regime which (i) designates Russian and Ukrainian persons as Specially Designated Nationals and Blocked Persons (SDN) and (ii) imposes targeted sanctions against entities in the Russian financial services, energy, and defense sectors (the "Sectoral Sanctions"), most recently on September 12, 2014. In addition, on August 6, 2014, the U.S. Commerce Department's Bureau of Industry and Security (BIS) imposed controls on the export of certain items to Russia for use in the oil and gas sectors.[2]

U.S. persons must be particularly diligent to avoid engaging in transactions that involve SDNs, that are prohibited by the Sectoral Sanctions, or involve the export of controlled items to Russia.

Specially Designated Nationals List

Since March 2014, OFAC has added numerous persons to the SDN list under authority of the Ukraine-related EOs.[3] As with all SDN designations, all property and interests in property of Ukraine sanctions–related SDNs within the possession or control of a U.S. person are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in. This prohibition includes the making of any contribution or provision of funds, goods, or services

continued on page 4

by, to, or for the benefit of any SDN, and the receipt of any contribution or provision of funds, goods, or services from any SDN. On September 12, 2014, OFAC designated several new SDNs, including five Russian state-owned defense-technology firms, and OFAC will likely designate additional Russian and Ukrainian SDNs as events further develop.

It is important to note that an entity in which one or more SDNs owns a 50% or greater interest is deemed to be an SDN, even if such entity is not specifically identified on the SDN list.[4] OFAC also advises parties to be cautious regarding transactions with entities in which SDNs have a significant, but less than 50%, interest because these entities may be the subject of future sanctions.

Sectoral Sanctions Identifications List

EO 13622 established a legal framework for a novel OFAC sanctions program: It authorizes the imposition of sanctions on persons active in certain sectors of the Russian economy, specifically identifying the financial services, energy, metals and mining, engineering, and defense and related materiel sectors. On July 16, 2014, pursuant to EO 13662, OFAC issued its initial Sectoral Sanctions Identifications (SSI) list,[5] and since then, has periodically added entities to this list. On September 12, 2014, OFAC significantly expanded the list, adding several larger financial institutions, including Sberbank of Russia, Russia's largest bank; and in the energy industry, Gazprom, a global energy company. At present, the SSI list includes entities in the financial services, energy, and defense sectors.

With respect to the financial services SSI list entities, U.S. persons are prohibited from transacting in, providing financing for, or otherwise dealing in new debt of longer than 30 days' maturity (originally 90 days' maturity under the initial sanctions) or new equity of such SSI entities.[6] The same long-term debt prohibition applies to the energy sector SSI list entities for debt of longer than 90 days' maturity, but not the new equity prohibition.[7] With respect to the defense and related materiel sector of Russia, there is also a long-term debt prohibition for debt of longer than 30 days' maturity.[8] Any entity owned 50% or more by an entity on the SSI list is also deemed to be subject to the Sectoral Sanctions.

The SSI list is separate from the SDN list. The OFAC press release announcing the SSI list makes clear that "[a]ll other transactions with these persons or involving any property in which one or more of these persons has an interest are permitted, provided such transactions do not otherwise involve [an SDN]." For example, transactions involving old debt, short-term debt, and correspondent bank account transactions with SSI list entities are permitted. Moreover, OFAC issued a general license permitting U.S. persons to engage in transactions involving a derivative product where its value is linked to an underlying asset subject to Sectoral Sanctions.[8] However, an entity on the SSI list may also be on the SDN list, and in those cases, U.S. persons cannot engage in any transaction with the SDN or any 50% or more controlled subsidiary.

Certain Licensing Requirements for Export Products

On August 6, 2014, BIS announced a new rule imposing export license requirements on certain specifically identified oil and gas related products (such as oil and gas pipes, drilling equipment, pipe and casting, subsea processing equipment, and related software and technology) if the exporter knows (or should have known) that the items are for use, directly or indirectly, in Russian deep-water, Arctic offshore or shale projects, or if the exporter is unable to determine whether the items will be used in such projects.[10] Given the broad scope of this prohibition, it may be difficult for exporters to obtain appropriate use assurances to meet this test. In any event, the BIS rule also states that license requests for the export of such items to Russia will be subject to a "presumption of denial."

Blanket Prohibition Against Exporting Certain Products to Certain Russian Energy Companies

The September 12, 2014 OFAC sanctions also prohibit the exportation of goods, services (not including financial services), or technology in support of exploration or production for Russian deep-water, Arctic offshore, or shale projects that have the potential to produce oil with respect to certain Russian energy companies, including Gazprom, Gazprom Neft, Lukoil, Surgutneftegas, and Rosneft.[11] U.S. persons have until September 26, 2014 to wind down applicable transactions, but must report such activity to OFAC.

Conclusion

Given the ongoing changes to the Ukraine-related sanctions programs, U.S. persons should have appropriate procedures in place to comply with existing sanctions and monitor developments to ensure ongoing compliance.

1 Executive Order 13660, Blocking Property of Certain Persons Contributing to the Situation in Ukraine (Mar. 10, 2014); Executive Order 13661, Blocking Property of Additional Persons Contributing to the Situation in Ukraine (Mar. 19, 2014); Executive Order 13662, Blocking Property of Additional Persons Contributing to the Situation in Ukraine (Mar. 24, 2014).

2 *See* http://www.gpo.gov/fdsys/pkg/FR-2014-08-06/pdf/2014-18579.pdf.

3 The SDN list, identifying persons sanctioned under all of the OFAC programs, is available on the OFAC website at http://www.treasury.gov/ofac/downloads/t11sdn.pdf.

4 OFAC guidance on this issue can be found on OFAC's website at http://www.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf.

5 The SSI list can be found on OFAC's website at http://www.treasury.gov/ofac/downloads/ssi/ssi.pdf.

continued on page 5

6 Directive 1 (as amended) can be found on OFAC's website at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13662_directive1.pdf.

7 Directive 2 (as amended) can be found on OFAC's website at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13662_directive2.pdf.

8 Directive 3 can be found on OFAC's website at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13662_directive3.pdf.

9 General License No. 1 Authorizing Certain Transactions Related to Derivatives under Directive 1 and Directive 2 of Executive Order 13662.

10 The affected Export Control Classification Numbers (ECCNs) are: 0A998, 8D999, 1C992, 3A229, 3A231, 3A232, 6A991, and 8A992.

11 Directive 4 can be found on OFAC's website at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13662_directive4.pdf.

12 The "wind down" authorization is provided in OFAC General License No. 2, available on OFAC's website at: http://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_gl2.pdf.

NEW EXECUTIVE ORDER PLACES ADDITIONAL REPORTING OBLIGATIONS ON GOVERNMENT CONTRACTORS AND CREATES AN ADDITIONAL WEAPON IN THE GOVERNMENT'S LABOR LAW ENFORCEMENT ARSENAL

By Tina Reynolds, Susan Borschel and Daniel Westman

On July 31, 2014, President Obama signed the Fair Pay and Safe Workplaces Executive Order, which requires both government contracting officers and government contractors to track and coordinate contractor and subcontractor compliance with federal and certain state labor laws starting in 2016. Contractors that have gone through a Department of Labor administrative merits determination or civil adjudication and may even have fully resolved their compliance problems, will now face further scrutiny and the possibility of additional remedial measures being imposed.

The most significant substantive changes and impact on contractors and subcontractors are discussed below.

Summary of Requirements

All offerors for government contracts worth in excess of $500,000 must disclose as part of their proposal certifications all administrative merits determinations, arbitral awards or decisions, and civil judgments relating to violations of a host of federal and state labor laws received within the previous three years. Contract awardees must update these disclosures every six months during contract performance.

Offerors that disclose past violations must also identify how they have corrected the violations and improved compliance with labor laws. Contracting officers must consult with the agency Labor Compliance Advisor and decide what remedial actions, if any, are required. Remedies available to the contracting officer include deciding not to exercise an option, terminating the contract, or referring the contractor to the agency's suspension and debarment official.

These disclosure requirements are to be flowed down to all subcontracts with an estimated value in excess of $500,000 that are not for commercially available off-the-shelf (COTS) items. The Executive Order does not include a similar COTS exclusion at the prime contract level, so all prime contracts in excess of $500,000, even those for COTS items, will be subject to the new disclosure requirements. Also, whereas the decision whether supplemental agreements or other steps are necessary to improve labor law compliance is made pre-award for prime contractors, the decision at the subcontract level can be made up to 30 days post-subcontract award. Notably, it is the contractor, not the government, that is supposed to make the decision whether its subcontractors remain responsible sources notwithstanding prior labor law violations.

In addition to these newly imposed burdens, the Executive Order creates new requirements specifying what information must be included on contractor employee pay stubs.

Finally, subject to limited exceptions, the Executive Order requires that federal contracts valued over $1 million for other than COTS items or commercial items shall include clauses in both the solicitation and contract specifying that the decision to arbitrate claims arising under title VII of the Civil Rights Act of 1964, or any tort related to or arising out of sexual assault or harassment, may only be made with the voluntary consent of employees or independent contractors after such disputes arise. This clause must be flowed down to subcontracts worth in excess of $1 million.

Impact on Government Contractors and Subcontractors

This Executive Order only applies to contracts, but not to grants or other transaction authority agreements. The White House Fact Sheet accompanying the Executive Order claims that it will promote efficient federal contracting. However, even without the benefit of knowing what the implementing regulations will require, it appears certain that the new requirements will cause duplication of efforts, inefficiencies, and increased costs. In addition, there will be confusion as to what agency (DOL or the awarding agencies) has authority or responsibility over enforcement of labor law compliance obligations.

continued on page 6

Further, contractors already subject to an administrative merits determination, arbitral award or decision, or civil judgment, all of which normally include a compliance plan, may now be subject to new or additional compliance obligations based on the agency contracting officer's determination that the already-imposed remedies are inadequate.

Finally, contractors will face considerable burdens in evaluating the labor compliance policies of their subcontractors.

Recommendations for Best Practices

While the Executive Order does not take effect until 2016, there are steps that federal contractors can take now to best position themselves for compliance. Among our recommendations are:

- Keep meticulous records of all labor law charges filed with relevant federal or state agencies, and of how those charges are resolved;
- Conduct more rigorous labor law compliance reviews (contractors that focus on ensuring compliance with labor law requirements will be able to "check the box" indicating that they are free of violations during the previous three years);
- Prepare to conduct additional due diligence on subcontractors; and
- When appropriate, add new FAR provisions implementing the Executive Order to FAR flow-down checklists, particularly for those clauses where flow-down will be mandatory.

A BRAVE NEW WORLD? RECENT CHALLENGES FACING FOREIGN IT COMPANIES IN CHINA

By Gordon Milner, Paul McKenzie and Jing Bu

Recent months have seen an increased focus by Chinese regulators on network security at a time of growing distrust of foreign technology and foreign IT companies (FITCs). This policy appears to have arisen, at least partly, as a response to the revelations regarding security agency activities made by former U.S. government contractor, Edward Snowden. The geopolitical climate may have been exacerbated by the U.S. government's imposition of restrictions on products from Huawei, ZTE, and other Chinese telecommunications equipment manufacturers, and its indictment in May 2014 of five Chinese military officials for allegedly stealing American companies' trade secrets.

As a result, many leading FITCs are encountering market challenges in China. By way of example, in the last three months:

- Certain high-profile security software, laptop computers, and other IT products from leading foreign brands have been removed from the list of technology permitted for government procurement;
- China state-owned enterprises (SOEs) have reportedly been prohibited by the Chinese government from procuring services from U.S. consulting companies;
- The use of Microsoft's Windows 8 operating system has been prohibited by the central government's procurement department, purportedly for security reasons; and
- The State Administration of Industry and Commerce has conducted raids on Microsoft's China offices, alleging breaches of the PRC Anti-Monopoly Law.

Much has been written about the obvious link between these developments and recent U.S. policy, with many commentators suggesting that the countries are engaged in a reciprocal "tit for tat" process. However, beyond the geopolitical headlines, there are clearly other factors that are driving developments, many of which predate recent tension in the China-U.S. relationship. In particular, China's 12th "Five Year Plan" (2011–2015) specifically identifies network and information security as a key priority, and focuses on domestic control over related hardware and software.

It is perhaps no coincidence that the current policy has coincided with the "coming of age" of a growing number of Chinese IT companies with strong technical capabilities and extensive political clout. Concerns over the security of foreign IT products have aligned with a desire to grow China's own IT industry, and have been used as a justification for promoting indigenous Chinese technologies and vendors over those of FITCs. As a result, it seems likely that the new market reality will outlive any geopolitical rapprochement.

The Existing Regulatory Environment

It is notable that the recent government actions have largely involved the Chinese authorities utilizing powers and enforcing restrictions under existing laws. In this vein, in September 2014 China's Ministry of Industry and Information Technology collated a series of new more, security-focused enforcement policies for existing laws in the Guiding Opinions on Strengthening Network Security in the Telecommunications and Internet Sectors (《关于加强电信和互联网行业网络安全工作的指导意见》; the "Opinions").

continued on page 8

Q+A CORNER

with **Victor Miller**, Vice President and General Counsel of Defense and Space at Honeywell Aerospace.

1. **What litigation, legislation or regulation are you keeping a close eye on, and why?**

   Honeywell's Defense and Space business is a global provider of key first tier guidance, navigation, cockpit and engines for all types of military aircraft, helicopter and ground vehicles. To provide legal advice for this type of business, we are focused on staying on top of evolving domestic and international procurement, export and anti-corruption regulations. Like many defense contractors, we have been finding ample opportunity with foreign allies and providing advice to the business on how to properly access those opportunities involves a combination of identifying which technologies can be sold overseas (export regulations), properly vetting sales representatives and internal sales teams pursuing those opportunities (US and foreign anti-corruption schemes) and consummating sales contracts (US FMS and FMF and foreign procurement laws). This has added to increased activity under the current Administration, which has promulgated new regulations and Executive Orders on government contractors, placing a premium on internal compliance efforts related to spotting and mitigating compliance risk early and reporting escapes properly to the government. Overall, I find that I am working on a very different set of issues than when I started at the company over a decade ago.

2. **What project(s) are currently taking up most of your time?**

   I typically split my time between support of business initiatives and law department projects and issues. Currently, we are supporting the rollout of various new compliance initiatives, such as new defense regulations related to the management of unclassified controlled technical information received from the Department of Defense on the programs we support on our IT systems. This involves certification to the satisfaction of various National Institute of Standards and Technology criteria for IT systems and is a collaborative effort between the Law Department and IT team. We are also involved in several key acquisitions and play a key role in due diligence, identifying key risk factors and developing mitigation and integration plans to allow deals to go forward despite identified risk.

3. **What accomplishment(s) as an attorney at Honeywell Aerospace are you most proud of?**

   On a personal level, I am most proud of the fact that the business allows the legal team at Defense & Space (a team of 4 direct reports) to be "at the table" in all aspects of the business decision making. I often tell candidates interviewing for a position to expect to spend almost 50% of your time in meetings without a clear legal issue driving the agenda. At Honeywell the job of a general counsel is to steer the business to its goal in a legal manner and not disrupt the organization. I've seen other defense businesses where the traditional interaction is to come to the Law department for a "No Objection" stamp at the end of a project. At Honeywell, we are there at the inception of the business plan, with a responsibility to participate and enable innovative approaches to a very highly regulated aerospace and defense market.

4. **What challenges and opportunities do you see for Honeywell Aerospace in the next 10 years?**

   The challenge I see is the tension between the desire by the customer for greater cost efficiency and commercialization that is often in tension with a demand for greater regulation and oversight. With shrinking budgets, not many companies will remain focused solely on the defense budgets and beholden to the type of cost disclosed, government owned IP schemes that have traditionally driven defense contracting. Instead, new models are already coming onto the scene. Commercial players like Amazon, SpaceX and others offer solutions that do not require government funding and do not want government regulatory involvement and oversight. Can we continue to buy innovative products in this country without stifling the corporations that create that innovation? In my experience, the US government pays lip service to the concepts of supporting commercial risk taking and innovation for government use but at the end of the day still wants to get into the details of how much each item costs and to make sure it owns the rights to those products. Until the essentials of the commercial bargain are understood and consistently implemented, the best commercial ideas will not come to the defense and government market, I fear.

Other notable security-related Chinese regulations that may see enhanced enforcement in the future include the 2007 Administrative Measures for the Graded Protection of Information Security (信息安全等级保护管理办法; the "Measures"), which designate various grades of information systems and stipulate mandatory security measures applicable to each grade. For certain grades of system, security product components must originate from Chinese-incorporated and controlled companies and the intellectual property comprised in any "core technology" or "critical components" must be "locally owned and independent."

Potential New Laws

New laws and regulations governing network security may also be in the offing.

For example, the State Internet Information Office of China announced on May 22, 2014, that China would adopt "cyber security" review rules in the "near term."

The text of the announcement is not publicly available, and details therefore remain unclear. However, recent reports suggest that a mandatory security review will be required for all important technology products and services affecting national security or the public interest–including, for example, computer systems in the financial and telecommunications sectors. Products and services that fail the review will be prohibited from being used in any Chinese computer systems related to national security or the public interest.

Reports also suggest that the review will focus on security of and control over the technology (and may require submission of sensitive software source code), but may also cover non-technology aspects of the products and services, such as the background of the product manufacturers and the service suppliers. This aspect of the review would likely disadvantage FITCs.

Key Takeaways

1. FITCs in China have been subject to greatly increased regulatory scrutiny and government intervention. Much of this has been implemented through a more proactive stance toward the enforcement of existing rules–which means that FITCs operating in China would be well advised to review their compliance status even in the absence of any new laws. A "business as usual" strategy may no longer be an effective or indeed safe approach to taking advantage of the opportunities afforded by the Chinese market.

2. The new regulatory environment may have been triggered by recent geopolitical events, but it is likely to continue notwithstanding any political rapprochement.

3. Domestic Chinese technology companies are rising in prominence and are likely to be favored under the evolving regulatory regime. In order to compete effectively, FITCs may need to review how their businesses are structured in China with a view to building confidence in the local market.

WORLD BANK SUSPENSION AND DEBARMENT REPORT

By Bradley Wine, Charles Duross, Tina Reynolds, and Catherine Chapple

On June 26, 2014, the World Bank's Office of Suspension and Debarment (OSD) released its public report covering sanctions arising from World Bank-financed projects during OSD's first six years of operation. The report includes case processing and other performance statistics related to 224 sanctioned firms and individuals in Bank-financed projects, and highlights the World Bank's efforts to improve transparency and accountability, while maintaining confidentiality and providing due process for those accused of fraud and corruption.

The OSD, or the "sanctions regime," as it is often called, represents the first level of adjudication within the World Bank. The OSD is intended to exclude proven wrongdoers from World Bank-financed operations, while simultaneously ensuring that accused parties are treated fairly and given a chance to mount a defense. Sixty percent of cases at the World Bank were resolved at the OSD level, with the remaining forty percent leading to at least one appeal at the Sanctions Board level.

According to the report, debarment is the most frequently imposed sanction, meaning that the debarred firm or individual is declared ineligible to receive World Bank-financed contracts from shareholder governments. In the majority of cases, the firm or individual was also subject to cross-debarment by other Multilateral Development Banks.[1] And because notice of debarments and other sanctions are posted on the World Bank's public website, they are observable by national and local governments and other public and private sector organizations conducting due diligence prior to procurement or other business decisions.

Also according to the report, between 2007 and 2013, the World Bank's OSD fully debarred or otherwise sanctioned 224 firms and individuals. Of these, 39 were pursuant to settlement agreements and 185 were based on sanctions proceedings. Of the 172 sanctions submitted to OSD by the World Bank Group's Integrity Vice Presidency (INT), the independent arm of the Bank responsible for investigating

continued on page 9

allegations of fraud and corruption in Bank-financed projects, 18 were withdrawn by INT or closed by OSD.

The World Bank's just-released OSD Report is here.

The role played by the World Bank in anti-corruption and fraud enforcement, both by itself and as an organization that refers matters to national enforcement authorities, has significantly increased in the past decade. The World Bank has resolved matters involving Siemens and Alstom, and besides debarring SNC-Lavalin, it began the investigation of the company that has now led to a series of cases being brought by Canadian authorities.[2] As a result of this more active role and the potentially severe consequences of cross-debarment, companies involved in World Bank-financed projects, or with any MDB for that matter, should pay close attention to this developing area of law. Morrison & Foerster attorneys have represented parties and individuals in World Bank suspension and debarment matters and are available to answer any questions regarding the process or this report.

1 On April 9, 2010, the African Development Bank Group, the Asian Development Bank, the European Bank for Reconstruction and Development, the Inter-American Development Bank Group, and the World Bank Group entered into an agreement under which entities debarred by one MDB will be sanctioned for the same misconduct by other signatories, that is, the principal of "debarred by one, debarred by all." *See Agreement for Mutual Enforcement of Debarment Decisions* (Apr. 9, 2010), *available at* http://www.ebrd.com/downloads/integrity/Debar.pdf.

2 *See, e.g.,* CNCNews, 2 *former SNC-Lavalin execs face criminal charges* (Feb. 2, 2014) (engineering company executives charges with money laundering and foreign bribery, among other crimes), *available at* http://www.cbc.ca/news/canada/montreal/2-former-snc-lavalin-execs-face-criminal-charges-1.2520367; World Bank Group, Press Release: *World Bank Debars SNC-Lavalin Inc. and its Affiliates for 10 years* (Apr. 17, 2013), *available at* http://www.worldbank.org/en/news/press-release/2013/04/17/world-bank-debars-snc-lavalin-inc-and-its-affiliates-for-ten-years; World Bank Group, Press Release: Enforcing Accountability: *World Bank Debars Alstom Hydro France, Alstom Network Schweiz AG, and their Affiliates* (Feb. 12, 2012), *available at* http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:23123315~menuPK:51062075~pagePK:34370~piPK:34424~theSitePK:4607,00.html; World Bank Group, Press Release: *Siemens to pay $100m to fight corruption as part of World Bank Group settlement* (July 2, 2009), *available at* http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:22234573~pagePK:34370~piPK:34424~theSitePK:4607,00.html.