EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008. Chelmsford. MA 01824

February 15, 2016 - Volume 8, Issue 3

USML PART 121.1 Aircraft and Engines Proposed Slight Modifications

Slight Modifications and clarifications proposed for CAT VIII and XIX and ECCN's 9A610, 9B610, 9D610, 9E610 and 9A619, 9B619, 9D6197, 9E619

Most changes are clarification in language of the text.

See Federal Register Link for more specific information.
http://www.pmddtc.state.gov/FR/2016/81FR02587.pdf

DATES: The Department of State will accept comments on this proposed rule until March 25, 2016.

FOR FURTHER INFORMATION CONTACT:

Mr. C. Edward Peartree,

Director, Office of Defense Trade Controls Policy,

Department of State, telephone (202) 663–2792;

email *DDTCPublicComments@state.gov*.
ATTN: ITAR Amendment—USML Categories VIII and XIX.

NEWSLETTER NOTES

Military Flight Training 2016 Conference

The Military Flight Training Community's Annual General Meeting For The Discussion Of Military Fixed Wing And Rotary Flight Training Requirements, Capabilities And Technologies

Over its 14 year history **Military Flight Training**Community's Annual General Meeting, bringing together over 220 Chiefs of Staff, Commanders of Air Training, Heads of Air Procurement, Operational Trainers and industry executives from across the globe to discuss the challenges and success shaping **military flight training**for now and the future.

In doing so it provides a rare platform to share lessons learned and best practice in current fixed wing and rotary **military flight training** requirements, capabilities and programmes, engaging in international collaboration on a very real level with key allies and strengthen the message of cooperation with counterparts across the world.

Military Flight Training is organized with the support and direction of Senior Leaders from across the military and industry sectors of the **flight training** community. With this in mind, each presentation topic and guest speaker has been specifically selected inline with the priorities and recommendations of the community to ensure it provides attendees with the critical information they need to solve their daily **flight training** challenges.

Whats New For 2016?

*NEW Breakout streams focused on rotary training and red air training and contracted support

*NEW Training Equipment Acquisition & Program Management Focus Day

*NEW Innovation Stage providing insight into the latest flight training research and development programs and opportunities across the world

*NEW Roundtable discussions providing critical engagement on the challenges and solutions found within 5th Generation Fighter Training

*(*Continued On The Following Column)*

*NEW Exhibition opportunities enabling attendees to have first hand access to the latest synthetic technologies in the market

"The Military Flight Training conference helps me to understand what industry can provide. It helps us to have a dialogue so that the industry knows what the operator thinks is important."
Brigadier General Scott Vander Hamm, Director Plans, Programs, Requirements and Assessments, HQ Air Education and Training Command, US Air Force

"Networking with different branches of military aviation here, it's good to hear where they're standing, where they're looking to go, what technology the new world has to offer. It's good for us to have that roadmap."
Lieutenant Colonel Osama Elwefati, Libyan Air Force

Complying with U.S. Export Controls – 2 Days

The Bureau of Industry and Security invites you to register for the following seminar to learn about export control requirements under the Export Administration Regulations.

Complying with U.S. Export Controls – 2 Days

April 5-6, 2016
Wood-Ridge, NJ – $460.

This two-day program is led by BIS's professional counseling staff and provides an in-depth examination of the Export Administration Regulations (EAR). The program will cover the information exporters need to know to comply with U.S. export control requirements on commercial goods and other items controlled under the EAR. We will focus on what items and activities are subject to the EAR; how to determine your export control classification number (ECCN); steps to take to determine the export licensing requirements for your item; when you can export or reexport without applying for a license; export clearance procedures; and record keeping requirements.

MORE SEMINAR OFFERINGS

Other export control seminars offered by the Bureau of Industry and Security this Spring:

February 17-18, 2016: San Diego, CA, "Complying with US Export Controls"

March 23-24, 2016: Denver, CO, "Complying with US Export Controls"

*(*Continued On The Following Page)*

May 4-5, 2015: Newport Beach, CA, "Complying with US Export Controls"

June 9-10, 2016: Seattle, WA, "Complying with US Export Controls"

Please visit our website for additional information on these programs and for registration details: http://www.bis.doc.gov/.

Barclays Bank Plc Settles

ENFORCEMENT INFORMATION FOR February 8, 2016

The Economic Sanctions Enforcement Guidelines, as well as recent final civil penalties and enforcement information, can be found on OFAC's Web site at http://www.treasury.gov/ofac/enforcement**.**

ENTITIES – 31 C.F.R. 501.805(d)(1)(i)

Barclays Bank Plc Settles Potential Civil Liability for Apparent Violations of the Zimbabwe Sanctions Regulations: Barclays Bank Plc ("Barclays"), a financial institution headquartered in London, United Kingdom, has agreed to remit $2,485,890 to settle its potential civil liability for 159 apparent violations of § 541.201 of the Zimbabwe Sanctions Regulations, 31 C.F.R. part 541 (ZSR). From July 2008 to September 2013, Barclays processed 159 transactions totaling approximately $3,375,617 to or through financial institutions located in the United States – including Barclays' New York branch ("Barclays NY") – for or on behalf of corporate customers of Barclays Bank of Zimbabwe Limited ("BBZ") that were owned 50 percent or more, directly or indirectly, by a person identified on the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) List of Specially Designated Nationals and Blocked Persons (the "SDN List").

OFAC has determined that Barclays did not voluntarily self-disclose the apparent violations to OFAC, and that the apparent violations constitute a non-egregious case. The total base penalty amount for the apparent violations was $5,029,000.

Beginning in or around 2005, local restrictions precluded Barclays from implementing measures for complying with economic sanctions, including sanctions screening, in Zimbabwe. Consequently, beginning in 2006, the bank's operations in the United Kingdom ("Barclays UK") began screening cross-border transactions involving BBZ and/or BBZ's customers. Under the new procedure, Barclays UK relied on BBZ's electronic customer records and documentation to perform sanctions-related customer screening and transaction screening involving BBZ.

*(*Continued On The Following Column)*

In 2006, BBZ implemented an electronic customer system that allowed the bank to input and maintain customer information in an electronic format. The system had several limitations, however, that prevented BBZ from accurately capturing and/or screening beneficial ownership information for its corporate customers. For example, when BBZ introduced the system, it was capable of capturing information related to a single primary account party (*i.e.*, BBZ's customer) but was initially unable to include data for a related party – such as the ultimate beneficial owner of the customer – in the electronic system even if the information appeared in the paper file for a customer. Barclays identified this shortcoming in 2007 and attempted to address the issue, but the changes did not allow BBZ to effectively capture or otherwise identify all of its customers' beneficial owners in the bank's electronic system. In 2009, Barclays again attempted to correct the shortcoming by building a "work-around" that the bank stated was ultimately cumbersome to implement and little used.

Barclays' Group Anti-Money Laundering (AML) policies in place during the period in which the apparent violations occurred required the bank's operations – including BBZ – to identify the ultimate beneficial owners of corporate customers. BBZ's Know Your Customer (KYC) procedures were ambiguous and difficult to follow with respect to the requirement to identify related parties and/or beneficial owners of corporate customers. As a result, the bank failed to obtain information on ultimate beneficial owners for a portion of BBZ's corporate customers in its paper files and/or failed to upload this information into BBZ's electronic customer system. Due to BBZ's failure to include updated beneficial ownership information in its electronic customer files (which, as noted above, was utilized by Barclays UK for OFAC sanctions compliance screening), Barclays UK was unaware of, and incapable of screening, this information for certain BBZ customers.

On July 25, 2008, OFAC designated Industrial Development Corporation of Zimbabwe (IDCZ) pursuant to Executive Order 13469 of July 25, 2008, "Blocking Property of Additional Persons Undermining Democratic Processes or Institutions in Zimbabwe." At the time of OFAC's designation, 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 persons pursuant to OFAC's Guidance on Entities Owned by Persons Whose Property and Interests in Property are Blocked. 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 the ZSR.

*(*Continued On The Following Page)*

By no later than 2011, Barclays became aware of weaknesses and shortcomings in relation to certain of BBZ's KYC practices, including the bank's inability to capture data for related parties (*i.e.*, beneficial owners) in its customer files. As part of a remediation effort in 2011, Barclays targeted a number of bank operation centers in Africa, including BBZ, in order to determine whether those locations were fully implementing the bank's Group AML policies. As part of these efforts, BBZ updated the paper files for one of the customer accounts to reflect IDCZ's beneficial ownership of the company, but the bank failed to include this information in the electronic customer system (which Barclays UK utilized and relied upon to conduct sanctions- related screening).

Beginning in October 2012, U.S. financial institutions blocked four funds transfers that Barclays NY processed on behalf of one of the three corporate entities beneficially owned by IDCZ located in Harare, Zimbabwe. Three of the funds transfers were originated by the aforementioned company's account with BBZ, whereas the fourth was destined for an account maintained by the company at a third-country financial institution unaffiliated with Barclays. Upon receiving notification that a transaction it processed had been blocked by another U.S. financial institution, Barclays NY conducted an internal investigation and determined that BBZ's customer was owned, indirectly, 50 percent or more by IDCZ, an entity on OFAC's SDN List. 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 November 2012 and September 2013 – all of which were blocked by other U.S. financial institutions.

The settlement amount reflects OFAC's consideration of the following facts and circumstances, pursuant to the General Factors Affecting Administrative Action under OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. OFAC found the following to be aggravating factors in this case: although Barclays attempted to comply with OFAC sanctions despite various constraints imposed by the local Zimbabwean authorities, Barclays failed to implement adequate controls to prevent the apparent violations from occurring despite numerous warning signs that its conduct could lead to a violation of U.S. sanctions laws; multiple business lines and personnel within Barclays, including supervisory and management staff in the bank's Compliance and Audit functions, had actual knowledge or reason to know of the conduct that led to the apparent violations (including the bank's awareness of the limitations of the systems used by BBZ with respect to capturing full information concerning the beneficial ownership of certain of its corporate customers); Barclays processed 159 funds transfers totaling approximately $3,375,617 that conferred economic benefit to, and provided indirect access to the U.S. financial system for,

*(*Continued On The Following Column)*

blocked persons, causing harm to the Zimbabwe sanctions program and its associated policy objectives; Barclays is a large and commercially sophisticated international financial institution; and Barclays' compliance program was inadequate to identify BBZ's customers as blocked persons and/or prevent the apparent violations from occurring.

OFAC considered the following to be mitigating factors: Barclays has not received a penalty notice or Finding of Violation in the five years preceding the earliest date of the transactions giving rise to the apparent violations; Barclays took remedial action in response to the apparent violations; and Barclays substantially cooperated with OFAC's investigation by submitting detailed and organized information, and by executing a statute of limitations tolling agreement and an extension to the agreement. OFAC also considered the fact that the prohibited entities were not publicly identified or designated and included on the SDN List at the time that Barclays processed transactions for or on their behalf.

This settlement demonstrates that an enforcement response may be particularly appropriate, even when an individual or entity is not included on the SDN List, in response to apparent violations in which: (a) the apparent violator is an institution that maintains direct customer relationships for entities that are beneficially owned, directly or indirectly, 50 percent or more by one or more SDNs, and is processing or routing transactions to or through the United States on behalf of such customers; (b) the institution's own records clearly demonstrate or otherwise clarify the SDN ownership of the customer, but the institution failed to act on the information; and/or (c) information concerning the SDN ownership of the customer is publicly available and allows intermediary banks to identify and block such transactions.

This enforcement action highlights the importance for institutions with operations in countries with a significant presence of persons (individuals and entities) on the SDN List to take appropriate measures to ensure compliance with U.S. economic sanctions when processing transactions for or on behalf of their customers to, through, or within the United States.

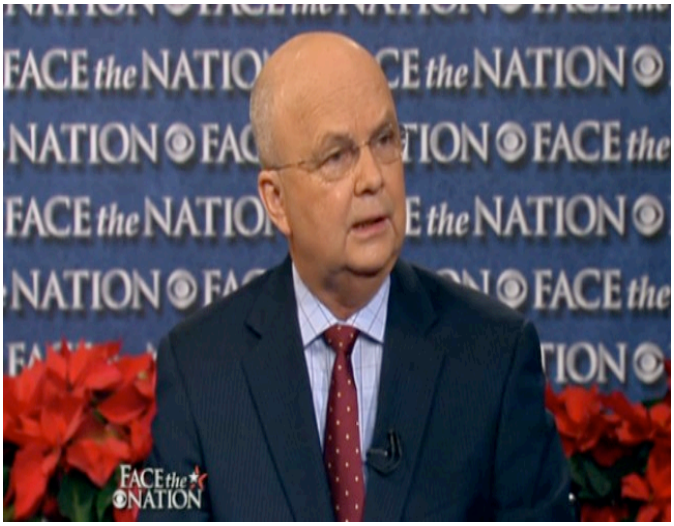
For more information regarding OFAC regulations, please visit: http://www.treasury.gov/ofac.

Former CIA director endorses unbreakable encryption

The former director of the Central Intelligence Agency and the National Security Agency said this week that the government should not have a backdoor into encrypted communications.

*(*Continued On The Following Page)*

"America is more secure with end-to-end unbreakable encryption," said General Michael Hayden, now a principal of the security and risk management firm Chertoff Group, speaking at a **Wall Street Journal** conference.



Hayden's comments are part of a tense debate over the degree of access that law enforcement agencies should have into secure communications.

In the wake of the terror attacks in Paris and San Bernardino, Calif., law enforcement and some lawmakers have been pressing tech companies to give investigators guaranteed access to encrypted data.

Led by FBI Director James Comey, they say encryption has allowed terrorists and criminals to plot beyond the reach of investigators.

But a growing chorus is joining the tech and privacy community in resisting the push. Hayden's remarks echo National Security Agency Director Adm. Michael Rogers, who earlier this month **insisted** "encryption is foundational to the future."

Critics say that building any type of guaranteed access into encryption algorithms introduces vulnerabilities that weaken the security of day-to-day uses of the Internet, such as banking.

Rogers did not directly back one argument over the other, but he did stress the value and the ubiquity of encryption to modern life.

"So spending time arguing about 'Hey, encryption is bad and we ought to do away with it,' that's a waste of time to me," Rogers said.

*(*Continued On The Following Column)*

DTAG: Notice of Membership.

The U.S. Department of State's Bureau of Political-Military Affairs is accepting membership applications for the 2016 DTAG. The Bureau of Political-Military Affairs is interested in applications from subject matter experts from the United States defense industry, relevant trade and labor associations, academic, and foundation personnel. (02.03.16)
http://www.pmddtc.state.gov

Cuba

On January 27, 2016, the Department of Commerce's Bureau of Industry and Security (BIS) and the Department of the Treasury's Office of Foreign Assets Control (OFAC) will take additional coordinated actions in support of the President's Cuba policy. These actions include a rule published by BIS that adds a general policy of approval for certain exports and reexports previously subject to case-by-case review and a policy of case-by-case review for exports and reexports to meet the needs of the Cuban people, including exports and reexports for this purpose made to state-owned enterprises and agencies and organizations of the Cuban government that provide goods and services to the Cuban people.

These actions further implement the President's policy to chart a new course in bilateral relations with Cuba and to further engage and empower the Cuban people, announced on December 17, 2014. The President explained that these steps build upon actions taken since 2009 that have been aimed at supporting the ability of the Cuban people to gain greater control over their own lives and determine their country's future. On January 16, 2015, BIS and OFAC published regulations to implement certain elements of this policy, including changes to licensing policy and license exceptions in the EAR that are consistent with U.S. support for the Cuban people (see 80 FR 2286 and 80 FR 2291). Additionally, on July 22, 2015, BIS published a rule implementing the May 29, 2015, rescission of Cuba's State Sponsor of Terrorism designation (see 80 FR 43314). On September 21, 2015, BIS and OFAC published rules to further implement the President's Cuba policy, which included additional amendments to license exceptions and licensing policy in the EAR (see 80 FR 56898 and 80 FR 56915).

Although these changes revise the licensing policy for certain types of exports, the United States continues to maintain a comprehensive embargo on trade with Cuba. The export and reexport to Cuba of all items subject to the EAR still requires a BIS license, unless authorized by a license exception specified in § 746.2(a)(1) of the EAR or exempted from license requirements in § 746.2(a)(2) of the EAR.

*(*Continued On The Following Page)*

For additional information, please review the rule, the Department of Commerce and Department of the Treasury's joint fact sheet, and BIS's updated Frequently Asked Questions, For any specific questions regarding exports or reexports to Cuba, please contact the Foreign Policy Division at (202) 482-4252.

BIS CUBA CALL-IN PROGRAM

BIS has scheduled monthly call-in programs to field questions from the exporting community concerning the Cuba rules published on January 16, 2015, July 22, 2015, September 21, 2015 and January 27, 2016.

The next programs will occur at 2 PM Eastern Time on February 9, March 8, April 12, May 10 and June 14, 2016. http://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations/cuba

Cyber Espionage Is Reaching Crisis Levels

The digital age is plaguing companies with new threats from abroad.

It's no secret that companies work hard to protect their intellectual property from theft. For innovations where confidentiality is integral to value, trade secrecy law offers a bargain: make reasonable efforts to maintain confidentiality, and those efforts will be backed up by legal sanctions. However, the rise of cybercrime is forcing companies to reevaluate the way they protect their most valuable trade secrets.

Trade secret theft costs companies billions of dollars every year. Traditionally, these crimes took the form of bribing, dumpster-diving or, as in one famous case, aerial photography. These days, industrial espionage has gone digital, introducing new threats and magnifying the impact of established techniques. Even employee raiding, an age-old tactic of trade secret mis-appropriators, is made more problematic in modern times by the sheer volume of secrets that can be stolen via digital media.

By the time AMSC launched a cyber investigation, contacted the FBI, and ultimately obtained an indictment, counterfeit copies of their software had already been sold back into the United States in Sinovel's products. Hamstrung by deficient cyber-intelligence, AMSC's legal action proved to be too little too late. The named defendants are now all in non-extradition countries and Sinovel has deployed litigation defense tactics that have stalled the case in U.S. courts while AMSC's stock has fallen from $370 per share to $5 per share.

*(*Continued On The Following Column)*

The executive and legislative branches of the U.S. Government have ramped up anti-cyber espionage efforts and are on course to amend the Economic Espionage Act of 1996 to create a federal civil remedy for trade secret theft. These efforts, coupled with increased enforcement of trade secret laws at the state level, will address the majority of misappropriation that occurs domestically.

However, acts of trade secret theft originating from outside the U.S. continue to be difficult to address. In recent times, both domestic and international companies have begun to bring cases before the U.S. International Trade Commission (ITC). In 2011, the Federal Circuit concluded that the ITC "has authority to investigate and grant relief based in part on extraterritorial conduct insofar as it is necessary to protect domestic industries from injuries arising out of unfair competition in the domestic marketplace."

This has been a helpful development, as the ITC is able to provide U.S. companies with a potent avenue of redress. It has the power to issue broad exclusion orders blocking importation and to draw adverse inferences against foreign parties who are non-responsive. Though the ITC cannot directly police the business practices of companies overseas, its adjudications can severely curtail the thieves' advantages.

http://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espionage/

Adobe Flash Player 20.0.0.286 Now Available for Download

Adobe has just rolled out Flash Player version 20.0.0.286, so users running this piece of software are recommended to download it as soon as possible.

Unsurprisingly, there is no change log available in this version, and Adobe has only recently uploaded it to its servers, but it's most likely supposed to fix some security issues or unknown vulnerabilities that have been discovered lately.

And yet, there are no reports of such known vulnerabilities, but we've reached out to Adobe to ask for more information and will update the article should new details be provided. Adobe Flash Player, which is often referred to as one of the most vulnerable applications currently available, is running on millions of computers right now, so it's critical to install new updates as fast as possible.

A recent report published by Bromium has shown that **Adobe Flash Player vulnerabilities more than tripled in 2015**, while Internet Explorer, which is also one of the most vulnerable applications out there, actually decreased the number of security flaws thanks to Microsoft putting more effort into strengthening its security system with the release of Windows 10.

*(*Continued On The Following Page)*

Until more information is provided on this new release, everyone is recommended to **download Adobe Flash Player** and keep their computers up to date, especially because outdated versions of this application can lead to more attacks and successful exploits on Windows workstations.

http://www.softpedia.com/blog/adobe-flash-player-20-0-0-286-now-available-for-download-499109.shtml

Extradited Chinese National Guilty of Supplying Iran with Goods Used to Make Nuclear Weapons-Grade Uranium

BOSTON—A Chinese national pleaded guilty today in U.S. District Court in Boston in connection with supplying Iran with pressure transducers which could be used to make nuclear weapons-grade uranium.

Sihai Cheng, a/k/a Chun Hai Cheng, a/k/a Alex Cheng, 35, a citizen of the People's Republic of China (PRC), pleaded guilty to two counts of conspiring to commit export violations and smuggle goods from the United States to Iran and four counts of illegally exporting U.S. manufactured pressure transducers to Iran. U.S. District Court Chief Judge Patti B. Saris scheduled sentencing for Jan. 27, 2016.

In 2013, Cheng was charged in an indictment along with Seyed Abolfazl Shahab Jamili, an Iranian national, and two Iranian companies, Nicaro Eng. Co., Ltd. (Nicaro) and Eyvaz Technic Manufacturing Company (Eyvaz), with conspiring to export, and exporting, highly sensitive U.S. manufactured goods with nuclear applications to Iran from at least 2009 to 2012. In December 2014, Cheng was extradited from the United Kingdom to this county and has remained in U.S. custody since then. Jamili remains a fugitive, and the U.S. government, through Interpol, has requested his arrest to face prosecution in the United States.

From February 2009 through at least 2011, Cheng, Jamili, and a third individual conspired with each other and others in the PRC and Iran to illegally obtain hundreds of U.S. manufactured pressure transducers manufactured by MKS Instruments, Inc., a company headquartered in Massachusetts, and export them to Iran. Pressure transducers can be used in gas centrifuges to enrich uranium and produce weapons-grade uranium and are therefore subject to strict export controls. They cannot be shipped from the United States to China without an export license or shipped from the United States to Iran at all. Today, Cheng admitted to causing the export of 185 pressure transducers from the United States to Iran in 2009.

*(*Continued On The Following Column)*

Initially, the parts were exported to the PRC using fraudulently obtained U.S. Department of Commerce export licenses. When they arrived in the PRC, Cheng inspected them in the Shanghai Free Trade Zone and removed their U.S./MKS serial numbers to conceal the fact that he was violating U.S. law. Cheng then caused the MKS pressure transducers to be exported to Iran knowing that the parts were being supplied to the Government of Iran. Jamili advised Cheng that the Iranian end-user was Kalaye Electronic Company, which the U.S. Government designated as a proliferator of weapons of mass destruction in 2007 for its work with Iran's nuclear centrifuge program.

MKS Instruments, Inc., is not a target of this investigation and MKS Instruments, Inc., is not a target of this investigation and has been cooperating in this matter.

The charging statutes provide a sentence of no greater than 20 years in prison on the charge of conspiracy to commit export violations and on each of the four counts of illegally exporting U.S. goods to Iran; and no greater than five years in prison on the charge of conspiracy to smuggle U.S. goods to Iran, in addition to five years of supervised release and a fine of $4 million. Actual sentences for federal crimes are typically less than the maximum penalties. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

United States Attorney Carmen M. Ortiz; Harold H. Shaw, Special Agent in Charge of the Federal Bureau of Investigation, Boston Field Division; Matthew Etre, Special Agent in Charge of Homeland Security Investigations in Boston; and John J. McKenna, Special Agent in Charge of the Department of Commerce, Office of Export Enforcement, Boston Field Office, made the announcement today. The case is being prosecuted by Assistant U.S. Attorney B. Stephanie Siegmann of Ortiz's National Security Unit.

(OFAC) Determines Johnson & Johnson Violation of Sudanese Sanctions

ENF - JAN 0 7 **2016**

Dear **DEPARTMENT OF THE TREASURY WASHINGTON, D.C. 20220**

FINDING OF VIOLATION

The Office of Foreign Assets Control (OFAC) has determined that Johnson & Johnson (Middle East) Inc. (JJME), a U.S. subsidiary of Johnson & Johnson at the time of the transactions detailed below, engaged in certain conduct in violation of the Sudanese Sanctions Regulations (the "Regulations"), 31 C.F.R. part 538, promulgated pursuant to the International Emergency Economic Powers Act 50 U.S .C. §§ 1701-06 (IEEP A). Specifically,

*(*Continued On The Following Page)*

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

FINDING OF VIOLATION

ENF [redacted]

JAN 07 2016

[redacted]
Johnson & Johnson (Middle East) Inc.
[redacted]
[redacted]

Dear [redacted]:

The Office of Foreign Assets Control (OFAC) has determined that Johnson & Johnson (Middle East) Inc. (JJME), a U.S. subsidiary of Johnson & Johnson at the time of the transactions detailed below, engaged in certain conduct in violation of the Sudanese Sanctions Regulations (the "Regulations"), 31 C.F.R. part 538, promulgated pursuant to the International Emergency Economic Powers Act 50 U.S.C. §§ 1701-06 (IEEPA). Specifically,

> **OFAC has determined that between on or about March 23, 2010, to on or about October 20, 2010, JJME violated § 538.206 of the Regulations when it facilitated the exportation of goods to Sudan by coordinating and supervising five shipments from Johnson & Johnson (Egypt) S.A.E. to Khartoum, Sudan.**

OFAC has considered the General Factors Affecting Administrative Action set forth in OFAC's Economic Sanctions Enforcement Guidelines (the "Guidelines"), 31 C.F.R. Part 501, app. A, available at www.treasury.gov/ofac, as well as your response dated December 18, 2014 to our initial Finding of Violation dated November 6, 2014, and your supplemental response dated January 5, 2015. After due consideration, OFAC has determined that the issuance of this Finding of Violation, in lieu of a civil monetary penalty, is the appropriate enforcement response to the transactions identified above. This Finding of Violation represents a final enforcement response, unless OFAC later learns of additional related violations or other relevant facts, and constitutes OFAC's final agency determination that a violation has occurred.

In accordance with the Guidelines, JJME's compliance history, including the issuance of this Finding of Violation, may be considered by OFAC in determining an appropriate enforcement response to any apparent violations of OFAC-administrated sanctions programs that come to our attention in the future. Civil monetary penalties may be imposed for violations of orders or regulations issued pursuant to IEEPA, not to exceed the greater of $250,000 or an amount that is twice the amount of the transaction that is the basis of the violation. In appropriate circumstances, OFAC may refer the matter to appropriate law enforcement agencies for criminal investigation and/or prosecution.

Contact Person

If JJME has any questions concerning this matter, please feel free to contact [redacted] at telephone number [redacted]. Please have the ENF number listed at the top of this Notice available when you call.

Sincerely,

John Smith

John E. Smith
Acting Director
Office of Foreign Assets Control

*(*Continued On The Following Page)*

OFAC has determined that between on or about March 23,2010, to on or about October 20, 2010, JJME violated § 538.206 of the Regulations when it facilitated the exportation of goods to Sudan by coordinating and supervising five shipments from Johnson & Johnson (Egypt) S.A.E. to Khartoum, Sudan.

OFAC has considered the General Factors Affecting Administrative Action set forth in OFAC's Economic Sanctions Enforcement Guidelines (the "Guidelines"), 31 C.F.R. Part 501, app. A, available at www.treasury.gov/ofac, as well as your response dated December 18,2014 to our initial Finding of Violation dated November 6, 2014, and your supplemental response dated January 5, 2015. After due consideration, OFAC has determined that the issuance of this Finding of Violation, in lieu of a civil monetary penalty, is the appropriate enforcement response to the transactions identified above. This Finding of Violation represents a final enforcement response, unless OFAC later learns of additional related violations or other relevant facts, and constitutes OFAC's final agency determination that a violation has occurred.

In accordance with the Guidelines, JJME's compliance history, including the issuance of this Finding of Violation, may be considered by OFAC in determining an appropriate enforcement response to any apparent violations of OFAC-administrated sanctions programs that come to our attention in the future. Civil monetary penalties may be imposed for violations of orders or regulations issued pursuant to IEEP A, not to exceed the greater o f $250,000 or an amount that is twice the amount of the transaction that is the basis of the violation. In appropriate circumstances, OFAC may refer the matter to appropriate law enforcement agencies for criminal investigation and/or prosecution.

*(*Continued On The Following Column)*

The Bureau of Industry and Security

Western Regional Office Cosponsored by: The Professional Association of Exporters and Importers (PAEI)

The 11th Annual Export Control Forum April 20-21, 2016 Burlingame, California

The Export Control Forum is a one-and-a-half day program dedicated to bringing the business community up-to-speed on the latest initiatives underway in the export control field, including the latest developments in the Export Control Reform initiative.

Over the day-and-a half program, you will hear key policy, management, technical, legal, and enforcement personnel from the Bureau of Industry and Security and other relevant agencies provide detailed information on recent changes and those you can expect in the near future. Under Secretary for Industry and Security Eric Hirschhorn will provide the opening keynote address. Day one will conclude with a networking opportunity to mingle and discuss issues of concern with the presenters and other participants. On day two, we will continue in plenary session; there will be no breakout sessions as in previous years.

Continuing legal education credit (MCLE) is available, and varies with the length of each seminar, for California State Bar members.

Location/Time

The Export Control Forum will be held April 20-21, 2016, at the Hyatt Regency in Burlingame, CA located at 1333 Bayshore Highway, Burlingame, CA 94010, telephone number (650) 357-1234. Registration and continental breakfast will begin at 7:30am. The program begins at 8:30am in the Hyatt Ballroom.

The exhibit hall will be open during the entire Forum from 7:30 a.m. – 5:00 p.m. on Wednesday, April 20, 2016, and 7:30 a.m. – noon on Thursday, April 21, 2016.

Tentative Agenda

We will post an agenda for this event when it becomes available.

Accommodations

Register early, a limited number of guest rooms are available at a reduced rate until March 29, 2016.

*(*Continued On The Following Page)*

Registration

The registration fee for attendees is $695.00 per person. The fee includes continental breakfast, breaks, lunch, and conference materials. The Hyatt requires advance notice for any special needs. If you require a vegetarian type meal, it must be specified during your online registration, with a check mark on your registration form. Online registration is required regardless of the payment method. The method of payment can be made by credit card or by check for both attendee and exhibitor registration. Make checks payable to the Professional Association of Exporters and Importers (PAEI). Mail checks to Professional Association of Exporters and Importers (PAEI), P.O. Box 712743, San Jose, CA 95161-2743. All mailed registrations (check payments) must be postmarked no later than April 4, 2016. Registration is not complete until payment has been received. Tax ID No. 680117035.

Cancellations must be made by email. All cancellations prior to April 4, 2016 will be assessed a $50.00 cancellation fee. No refunds after April 4, 2016.

Transfer requests must be made by email prior to April 4, 2016. If you would like to transfer your registration you must receive prior approval from PAEI. Registrations may NOT be transferred outside of your organization and registrations may NOT be resold. Please include "Transfer Request" in the subject line of your email, along with all contact information for the new attendee.

Questions, please call the BIS Western Regional Office at (949) 660-0144, (408) 998-8806, or by email

http://www.bis.doc.gov/index.php/component/content/article/81-compliance-a-training/export-administration-regulations-training/seminar-details/992-april-20-21-2016-burlingame-ca

Save the Date -- Webinar on Encryption Controls

On Wednesday, February 17, 2016 at 2:30 p.m. Eastern Time, BIS will offer a special one and a half hour webinar. Export Administration officials will provide an overview of the Export Administration Regulations related to the unique provisions for encryption controls. Topics will include Note 4 to Category 5, Part 2; various decontrols; encryption mass market provisions (742.15); License Exception ENC (740.17); publicly available; encryption licensing; and foreign products developed from U.S. origin encryption parts and components. Participants will be able to submit questions by email during the webinar, and BIS officials will respond orally at the end of the presentation. There will be a $50 charge for this webinar. We expect the registration link for registration and payment to be active on February 12. It will provide detailed instructions on registration and payment, and how to join the webinar on the day of the broadcast.

EIB World Trade Headlines
Evolutions In Business • www.eib.com • (978) 256-0438 • P.O. Box 4008, Chelmsford, MA 01824