www.t-b.com

U.S. EXPORT CONTROLS PAST, PRESENT AND FUTURE (2017 Edition)

Introduction – Looking Back at 2017 2
2017 Export Control Reform Updates 3
Spacecraft Systems 3
Infrared Detection items 4
Temporary Modification of Category XI of the USML 4
2017 Sanctions Updates 5
Russia and Ukraine 6
Cuba 9
North Korea 10
Sudan 12
Additional Sanctions Updates 12
Regulatory Updates 14
Enforcement Actions 25
International Export Control Agreements and Regimes 50
Wassenaar Arrangement 50
Missile Technology Control Regime 56
Australia Group 58
Nuclear Suppliers Group 59
Recommendations for 2018 60

Introduction – Looking Back at 2017

There were a number of important changes to the export control laws and regulations in 2017 implemented by the U.S. Government, including the Commerce Department's Bureau of Industry and Security (BIS), Treasury Department's Office of Foreign Assets Control (OFAC) and the State Department's Directorate of Defense Trade Controls (DDTC):

- BIS, OFAC and the State Department updated their Cuban sanctions regulations. BIS loosened some restrictions under License Exception SCP (Support for the Cuban People) and now authorizes additional types of items going to private sector entities. However, OFAC limited the travel authorizations that are currently implemented by OFAC in the form of general licenses. For example, individual people-to-people travel will no longer be authorized. The State Department also published a List of Restricted Entities and Subentities Associated with Cuba (Cuba Restricted List) with which direct financial transactions will generally be prohibited and BIS and OFAC amended their regulations to address the State Department's Cuba Restricted List.

- The U.S. Government resolved the enforcement action against ZTE Corporation and its affiliated companies, which were placed on the BIS Entity List last year. In total, ZTE agreed to pay the U.S. Government $892,360,064 and agreed to a significant conduct remedy, in the various plea and settlement agreements. In return, ZTE Corporation and ZTE Kangxun were removed from the Entity List, but ZTE Corporation and ZTE Kangxun, along with a new addition, former ZTE CEO Shi Lirong.

- The U.S. Government also implemented changes to the Ukraine-Related Sanctions Program against Russia and the Crimea Region of Ukraine, including the addition of the Russian FSB to the BIS Entity and OFAC SDN Lists, modifications to Directives under the Sectoral Sanctions Identifications List. In addition, the State Department published the list of parties identified under Section 231.d of the *Countering America's Adversaries Through Sanctions Act of 2017* and published guidance related to Russia's Defense and Intelligence Sectors Under Section 231. Unlike other sanctions programs, the State Department will be the enforcement agency for Section 231/235.

- OFAC issued a general license this year that suspends the comprehensive sanctions restrictions on Sudan, in connection with ongoing U.S.-Sudan bilateral engagement. However, the BIS sanctions program against Sudan still remains in place, with minor changes to its license review policy for certain civil aviation and railroad applications.

- BIS published new documentation requirements for transactions involving Hong Kong, which became effective this year. This rule covers any item with an Export Control Classification Number subject to controls based on various reasons, including encryption items controlled under ECCN 5x002. The new provision requires that an exporter or re-exporter of a covered item to Hong Kong under a US license exception must now obtain a copy of the matching Hong Kong import license that authorizes import into Hong Kong.

- BIS continued to streamline the export of Encryption Items, including the reorganization of the Note 4 decontrol note as a more positive list and an definition of the uses of encryption that are decontrolled.

- BIS also implemented the Wassenaar Arrangement 2016 Plenary meeting export controls of items, including changes to Categories 3, 4, and 5, Parts 1 and 2 of the Export Administration Regulations.

Additional information describing these changes are included below.

2017 Export Control Reform Updates

On August 13, 2009, President Obama ordered a "broad-based interagency" review of U.S. export control regulations, including those that govern dual-use and defense items. The review was to consider reforms to the system to enhance the national security, foreign policy, and economic security interests of the United States, with the goal of strengthening national security and the competitiveness of key U.S. manufacturing and technology sectors by focusing on current threats, as well as adapting to the changing economic and technological landscape. This review determined that the current export control system is overly complicated, contains too many redundancies, and, in trying to protect too much, diminishes our ability to focus our efforts on the most critical national security priorities.

As a result, the Administration launched the ECR Initiative, which will fundamentally reform the U.S. export control system. The ECR Initiative is designed to enhance U.S. national security and strengthen the United States' ability to counter threats such as the proliferation of weapons of mass destruction.

The Administration is implementing the reform in three phases. Phases I and II reconcile various definitions, regulations, and policies for export controls, all the while building toward Phase III, which will create a single control list, single licensing agency, unified information technology system, and enforcement coordination center.

Since the introduction of the ECR Initiative, we have seen:

- The move of less sensitive equipment, parts, and components from the regulatory jurisdiction of the U.S. Munitions List (USML) of the International Traffic in Arms Regulations (ITAR) administered by the DDTC to the Commerce Control List (CCL) of the Export Administration Regulations (EAR) administered by BIS, following comprehensive technical and policy reviews conducted by an interagency team of experts representing all relevant U.S. Government departments and agencies. These reforms were also developed in close consultation with Congress and the private sector, which provided extensive public review and comment on the proposed changes.
- The revision and implementation of 18 of 21 categories of the U.S. Munitions List. A summary of these changes can be found on the ECR Control List "Tracker."
- A more flexible licensing process under the CCL for the export of less sensitive defense products and services to allies and partners, benefitting U.S. manufacturers.
- A reduction in license volume in the 15 implemented USML categories for the Department of State's Directorate of Defense Trade Controls, allowing it to enhance efforts to safeguard against illicit attempts to procure sensitive defense technologies.
- The creation of an ongoing transparent periodic interagency review process to continually improve export control regulations, and to engage with industry and the defense export community to solicit public comment on proposed updates to the USML and CCL.

However, we are still waiting on revisions to Categories I (Firearms), II (Artillery Projectors) and III (Ammunition) of the ITAR, as well as updates to Phase III of the ECR Initiative to create a single control list, single licensing agency, unified information technology system, and enforcement coordination center. Additional information on the ECR Initiative can be found on the ECR website.

The changes in 2017 were minor, including a change in the EAR to the licensing policy for spacecrafts and related items, and a temporary modification to Category XI (Electronics) of the USML, as described in more detail below:

Spacecraft Systems

BIS published a final rule amending the exceptions to the general policy of denial in the EAR to address issues raised in, and public comments on, the interim final rule that was published on May 13, 2014, as well as additional clarifications and corrections. The May 13 rule added controls to the EAR for spacecraft and related items that the President has determined no longer warrant control under USML Category XV--spacecraft and related items.

This is the third final rule BIS has published related to the May 13 rule and completes the regulatory action for the interim final rule. These changes were also informed by comments received in response to the May 13 rule that included a request for comments, as well as interagency discussions on how best to address the comments. The changes made in this final rule are grouped into four types of changes: Changes to address the movement of additional spacecraft and related items from the USML to the CCL, as a result of changes in aperture size for spacecraft that warrant ITAR control, in response to public comments and further U.S. Government review; changes to address the movement of the James Webb Space Telescope (JWST) from the USML to the CCL; other corrections and clarifications to the spacecraft interim final rule; and addition of .y items to Export Control Classification Number 9A515.

This final rule is being published in conjunction with the publication of DDTC final rule, which makes changes, including corrections and clarifications, to the provisions adopted in the State Department's own May 13, 2014 rule. The State May 13 rule revised USML Category XV (22 CFR 121.1) to control those articles the President has determined warrant control on the USML. Both May 13 rules and the subsequent related rules are part of the President's Export Control Reform Initiative. This rule is also part of Commerce's retrospective regulatory review plan under Executive Order (EO) 13563 (see the SUPPLEMENTARY INFORMATION section of this rule for information on the availability of the plan).

Infrared Detection items

On October 12, 2016, BIS published a final rule entitled “Revisions to the EAR: Control of Fire Control, Laser, Imaging, and Guidance Equipment the President Determines No Longer Warrant Control Under the United States Munitions List (USML).” This notice of inquiry is published to request comments from the public on the impact of further increasing certain controls implemented by that final rule.

On October 12, 2016, BIS published a final rule entitled “Revisions to the Export Administration Regulations (EAR): Control of Fire Control, Laser, Imaging, and Guidance Equipment the President Determines No Longer Warrant Control Under the USML” (81 FR 70320), hereafter referred to as the “October 12 final rule.” This final rule was preceded by two proposed rules published on May 5, 2015 (80 FR 25798) (“May 5, 2015 proposed rule”) and February 19, 2016 (81 FR 8421) (“February 19, 2016 proposed rule”). Revisions made by the October 12 final rule became effective on December 31, 2016. During the course of public comment and interagency discussion on the rule that became effective at the end of 2016, several ideas for new types of controls under the ITAR arose. Because these controls were not proposed earlier and not subject to public comment, they were not included in the October 12 final rule. Thus, the Department of State is publishing a notice of inquiry addressing those controls. Along with those possible new controls under the ITAR, this notice of inquiry requests comments from the public on the potential impact of increasing certain EAR controls established in the October 12 final rule. Items controlled in certain ECCNs in Category 6 of the CCL can be incorporated into foreign military commodities. To provide greater visibility into exports, reexports, and in-country transfers of such items, the October 12 final rule increased the scope of controls described in §744.9 (Restrictions on exports, reexports, and transfers of certain cameras, systems, or related components) and the scope of ECCN 0A919 (“Military Commodities” Located and Produced Outside the United States . . . .).

Temporary Modification of Category XI of the USML

The Department of State, pursuant to its regulations and in the interest of the security of the United States, temporarily modifies Category XI of the USML. On July 1, 2014, the Department published a final rule revising Category XI of the USML, 79 FR 37536, effective December 30, 2014. That final rule, consistent with the two prior proposed rules for USML Category XI (78 FR 45018, July 25, 2013 and 77 FR 70958, November 28, 2012), revised paragraph (b) of Category XI to clarify the extent of control and maintain the existing scope of control on items described in paragraph (b) and the directly related software described in paragraph (d). The Department has determined that exporters may read the revised control language to exclude certain intelligence-analytics software that has been and remains controlled on the USML. Therefore, the Department determined that it is in the interest of the security of the United States to temporarily revise USML Category XI paragraph (b), pursuant to the provisions of 22 CFR 126.2, while a long-term solution is developed. The Department will publish any permanent revision to USML Category XI paragraph (b) addressing this issue as a proposed rule for public comment. This temporary revision clarifies that the scope of control in existence prior to December 30, 2014 for USML paragraph (b) and

directly related software in paragraph (d) remains in effect. This clarification is achieved by reinserting the words "analyze and produce information from" and by adding software to the description of items controlled.

The Department previously published a final rule on July 2, 2015 (80 FR 37974) that temporarily modified USML Category XI(b) until December 29, 2015. The Department published a final rule on December 16, 2015 (80 FR 78130) that continued the July 2, 2015 modification to August 30, 2017. This final rule extends the July 2, 2015 modification to August 30, 2018 to allow the U.S. government to review USML Category XI in full and publish proposed and final rules.

2017 Sanctions Updates

There were several changes to U.S. sanctions programs this year, most of which expand the sanctions programs, including Iran, Russia, Cuba and North Korea. For example, on July 25 and 27, 2017 both houses of Congress passed a bill expanding U.S. Sanctions on Iran, Russia, and North Korea. The bill, titled, *Countering America's Adversaries Through Sanctions Act*, was presented to President Trump on July 28 to be signed into law. The bill expands blocking sanctions for both Iran and Russia as well as additional sectoral sanctions on Russian banks, oil and gas companies and their subsidiaries. Some noteworthy provisions of the bill include:

Sanctions on Iran

- Sanctions in response to Iran's ballistic missile program
- Terrorism related sanctions for the IRGC
- Sanctions for human rights abuses
- Arms embargo
- Blocking of property and assets and exclusion from the U.S.

Sanctions on Russia

- Sanctions against persons contributing the situation in Ukraine
- Sanctions for activities of Russian Federation undermining cybersecurity
- Sanctions to special Russian crude oil projects
- Sanctions for Russian financial institutions
- Sanctions on persons responsible for significant corruption
- Sanctions for transactions with foreign sanctions evaders/ human rights abusers
- Sanctions for human rights abusers
- Sanctions for persons engaging in transactions with intelligence/defense sectors of Russian Government
- Sanctions for contributing to the development of Russian Federation pipelines
- Sanctions for facilitation of privatization of state owned
- Sanctions for transfer of arms and related material to Syria
- Blocking of property and assets and exclusion from the U.S.
- Export Import Bank Assistance – directed not to give approval to sanctioned person
- Export Sanction – Not to issue license or grant specific authority to export to sanctioned person
- Loans – Prohibit U.S. financial institution from providing loans/credits
- Loans International – Direct to use voice and vote of U.S. to oppose loan from international institution to sanctioned person
- Sanctions on Financial Institutions
- Procurement – U.S may not procure from or contract with sanctioned person
- Prohibit Transactions in Foreign Exchange subject to U.S. jurisdiction
- Banking Transactions
- Property Transactions
- Ban on Investment in Equity/Debt of sanctioned person
- Exclusion of corporate officers/shareholders of sanctioned person
- Any of these sanctions may be applied to principal executive officer of sanctioned person

Sanctions on North Korea

- Sanctions for forced labor and slavery overseas of North Koreans
- Prohibition of goods made with North Korean labor except for those found by commissioner of U.S. customs and Border Protection were not produced with slave labor
- Sanctions on foreign persons employing North Korean Labor
- Enforcing shipping sanctions – no vessels to enter waterways of U.S.
- Blocking transactions in property

Russia and Ukraine

Cyber-Related Sanctions

On December 29, 2016, President Obama issued a new Executive Order entitled "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities."

This new EO amended Executive Order 13694, originally issued on April 1, 2015, to expand cyber-related sanctions, and designated five Russian entities and four Russian individuals. These parties were determined to have tampered with, altered, or caused a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. They are deemed blocked and have been added to the OFAC List of Specially Designated Nationals and Blocked Persons (SDN List).

Included on this list was the Russian FSB (the "Federalnaya Sluzhba Bezopasnosti" or Federal Security Service).

The FSB is responsible for technical evaluations and import notifications/licenses, which are required in order to qualify commercial information technology (encryption) products for importation, distribution and use in the Russian Federation. As part of this process, a list of protocols, algorithms, and key lengths would need to be provided, eventually, to the FSB.

There were a number of questions and concerns with regards to how the sanctions against the FSB would affect certifications and imports of information technology products into the Russian Federation,

This year, OFAC published **Cyber-related General License (GL) 1**, "Authorizing Certain Transactions with the Federal Security Service," pursuant to Executive Order 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." GL 1 authorizes certain transactions with the FSB that are necessary and ordinarily incident to requesting certain licenses and authorizations for the importation, distribution, or use of certain information technology products in the Russian Federation, as well as transactions necessary and ordinarily incident to comply with rules and regulations administered by, and certain actions or investigations involving, the FSB.

The General License appears to authorize transactions related to FSB's involvement in the import and certification process. There are, however, some important caveats:

1. The export, reexport, or provision of good and technology subject to the EAR still need authorization from BIS. The FSB was added to the BIS Entity List on January 4, 2017, which means that BIS imposed on the FSB a license requirement for exports, reexports, or transfers (in-country) of all items subject to the EAR and a license review policy of presumption of denial. This could include the transfer of technology subject to the EAR in support of certification or import notification/license.
2. The payments to the FSB for such licenses, permits, certifications, or notifications cannot exceed $5,000 in any calendar year.
3. The General License does not authorize the exportation, reexportation, or provision of any goods, technology, or services to the Crimea region of Ukraine.

4. Transactions with certain blocked persons and entities are still restricted.

If the transactions with the FSB comply with OFAC's General License, and are not subject to the EAR, then an individual license would not be required to complete Russian certifications and import notifications. If you are still unsure about a specific transaction, we would be happy to discuss this notice with you in greater detail.

Later in the year, OFAC provided the following four FAQs related to the December 29, 2016 sanctions imposed on the FSB and the February 2, 2017, issuance of General License 1, "Authorizing Certain Transactions with the Federal Security Service," pursuant to Executive Order 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities."

> *501. What does General License 1 (GL 1), "Authorizing Certain Transactions with the Federal Security Service," authorize?*
>
> GL 1 *authorizes transactions with the Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (FSB) that are necessary and ordinarily incident to requesting, receiving, utilizing, paying for, or dealing in certain licenses and authorizations for the importation, distribution, or use of certain information technology products in the Russian Federation. It also authorizes transactions necessary and ordinarily incident to compliance with rules and regulations administered by, and certain actions or investigations involving, the FSB.*
>
> *This general license does not authorize U.S. persons to transact with the FSB except for the limited purposes described above, nor does it authorize the exportation, reexportation, or provision of any goods, technology, or services to the Crimea region of Ukraine.*
>
> *502. What sanctions remain in place on the FSB following the issuance of GL 1?*
>
> *GL 1 only authorizes certain transactions with the FSB acting in its administrative and law enforcement capacities. The GL was issued in order to ensure that U.S. persons engaging in certain business activities in Russia that are not otherwise prohibited are not unduly impacted. All other transactions involving any property within U.S. jurisdiction or within the possession or control of U.S. persons, in which the FSB has an interest, including all other transactions directly or indirectly with the FSB, remain prohibited unless exempt or otherwise authorized by OFAC.*
>
> *503. Does GL 1 authorize the exportation of hardware or software directly to the FSB, or where the FSB is the end user of such hardware and software?*
>
> *No. GL 1 does not authorize the export of any goods, technology, or services directly or indirectly to the FSB or any other blocked person or entity, except for the limited purposes of complying with certain rules, regulations, and investigations involving the FSB or requesting certain licenses or authorizations for the importation, distribution, or use of information technology products in the Russian Federation.*
>
> *504. I understand that travel to Russia involves clearing Russian border control, which is part of the FSB. Do I need a license from OFAC to travel to Russia, or to clear Russian customs?*
>
> *No, the sanctions on FSB do not apply to transactions by U.S. persons that are ordinarily incident to travel to or from Russia, including those transactions required to enter into or exit the country (i.e., complying with Russian border control requirements).*

As noted above, the export, reexport, or provision of good and technology subject to the Export Administration Regulations \still need authorizations from BIS, since the FSB was added to the BIS Entity List on January 4, 2017, which means that BIS imposed on the FSB a license requirement for exports, reexports, or transfers (in-country) of all items subject to the EAR and a license review policy of presumption of denial. This could include the transfer of technology subject to the EAR in support of certification or import notification/license. However, later in the year,

In February, we notified you that OFAC issued a General License authorizing certain transactions with the Russian Federal Security Service (FSB) related to import licenses, permits, certifications and notifications. General License 1 authorizes transactions that are necessary and ordinarily incident to:

> *Requesting, receiving, utilizing, paying for, or dealing in licenses, permits, certifications, or notifications issued or registered by the Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a. FSB) for the importation, distribution or use of information technology products in the Russian Federation, provided that (i) the exportation, reexportation, or provision of any goods or technology that are subject to the EAR, 15 CFR parts 730 through 774, are licensed or otherwise authorized by the Department of Commerce and (ii) the payment of any fees to the Federal Security Service for such licenses, permits, certifications, or notifications does not exceed $5,000 in any calendar year.*

In light of OFAC's General License No. 1, BIS makes a conforming change by modifying the listing for the Federal Security Service on the Entity List under the destination of Russia. This final rule modifies the license requirement column for this entity to specify that the Entity List's license requirements do not apply to items subject to the EAR that are related to transactions authorized by OFAC pursuant to new General License No. 1 (i.e., transactions that are necessary and ordinarily incident to requesting, receiving, utilizing, paying for, or dealing in licenses, permits, certifications, or notifications issued or registered by the FSB for the importation, distribution, or use of information technology products in the Russian Federation, so long as the transactions do not involve exportation, reexportation, or provision of any goods, technology, or services to the Crimea region of Ukraine and do not otherwise violate E.O. 13757).

Ukraine-Related Sanctions

Earlier this year, OFAC published changes to the Russia Sectoral Sanctions Directive 1 and Directive 2. These changes were made in accordance with the Countering Russian Influence in Europe and Eurasia Act of 2017 (CRIEEA).

Previously, transactions subject to Directive 1 (e.g., those involving a sanctioned party related to Russia's financial sector) were subject to prohibitions on dealing in any "new debt" with a maturity longer than 30 days, among other things. This includes a U.S. seller offering payment terms of longer than 30 days. As of November 28, 2017, the Directive 1 prohibition changed to 14 days.

Similarly, transactions subject to Directive 2 (e.g., those involving a sanctioned party related to Russia's energy sector) were previously subject to prohibitions on dealing in any "new debt" with a maturity longer than 90 days, among other things. As of November 28, 2017, the Directive 2 prohibition changed to 60 days.

Later in the year, the Trump administration turned over to Congress a list of Russia-connected entities it will use to determine new sanctions meant to rebuke Russia for actions in Eastern Europe, Syria and the 2016 United States presidential election. Administration officials made clear to lawmakers that they intended to impose sanctions on individuals in the United States and elsewhere who did "significant" business with the Russian entities, sending an early warning that such deals must soon end.

According to the State Department Press Briefing, Secretary of State Rex Tillerson, in accordance with Section 231 of the *Countering America's Adversaries Through Sanctions Act of 2017* (CAATSA) has authorized the department to issue guidance to the public specifying the persons or entities that are part of or operating on behalf of the defense or intelligence sectors of the Government of the Russian Federation. Section 231 requires the imposition of certain sanctions on persons determined to have knowingly engaged in a significant transaction, on or after the date the Act was enacted, with a person that is part of or operating for or on behalf of the defense or intelligence sectors of the Government of the Russian Federation.

In determining whether a transaction is "significant" for purposes of section 231 of the Act, the Department of State will consider the totality of the facts and circumstances surrounding the transaction and weigh various factors on a case-by-case basis. The factors considered in the determination may include, but are not limited to, the significance

of the transaction to U.S. national security and foreign policy interests, in particular whether it has a significant adverse impact on such interests; the nature and magnitude of the transaction; and the relation and significance of the transaction to the defense or intelligence sector of the Russian government.

OFAC, in accordance with section 223(d) of Title II of the CAATSA, amended Directive 4 of the Russia/Ukraine-Related Sanctions. The new Directive 4 prohibits the following activities by a U.S. person or within the United States with entities subject to Directive 4 pursuant to OFAC's Sectoral Sanctions Identifications (SSI) List:

The provision, exportation, or reexportation, directly or indirectly, of goods, services (except for financial services), or technology in support of exploration or production for deepwater, Arctic offshore, or shale projects:

1. *that have the potential to produce oil in the Russian Federation, or in maritime area claimed by the Russian Federation and extending from its territory, and that involve any person determined to be subject to this Directive or any earlier version thereof, their property, or their interests in property; or*
2. *that are initiated on or after January 29, 2018, that have the potential to produce oil in any location, and in which any person determined to be subject to this Directive or any earlier version thereof, their property, or their interests in property has (a) a 33 percent or greater ownership interest, or (b) ownership of a majority of the voting interests.*

Additional information can be found in the Sanctions Summary published by the State Department, as well as the New OFAC FAQ Related to CAATSA.

Later in the year, OFAC issued Ukraine-Russia-related General License 1B and is publishing updated Ukraine-Russia-related FAQs and one new Ukraine-Russia-related FAQ . These changes relate to the amended Ukraine-Russia-related Directives 1 and 2 that were issued on September 29, 2017 in accordance with Title II of CAATSA. Certain CAATSA-related prohibitions in amended Directives 1 and 2 had a delayed effective date of November 28, 2017. In order to account for the fact that the CAATSA-related prohibitions in amended Directives 1 and 2 have now come into effect, OFAC is issuing General License 1B to address the decrease in the maturity dates for Directive 1 from 30 days to 14 days, and the decrease in the maturity dates for Directive 2 from 90 days to 60 days; in the case of both directives, these new prohibitions relate to debt issued on or after November 28, 2017.

Finally, OFAC published the list of items defined as medical supplies (List of Medical Supplies) and generally licensed for exportation or reexportation to the Crimea region of Ukraine pursuant to General License 4 under Executive Order 13685 of December 19, 2014, which is part of OFAC's Ukraine-related sanctions program. OFAC is publishing the List of Medical Supplies both as originally posted on December 19, 2014 and as updated on August 12, 2016 to include additional items. The complete list can be found on OFAC's website.

Cuba

The White House released the National Security Presidential Memorandum on Strengthening the Policy of the United States Toward Cuba. President Trump seeks to reaffirm the U.S. statutory embargo of Cuba by enhancing travel and economic restrictions. This would be a reversal of the policies of the prior administration that sought to re-establish diplomatic, economic, and travel relations between the U.S. and Cuba, ending more than half a century of isolation. The memorandum directs the Treasury and Commerce Departments to begin the process of issuing new regulations within 30 days. However, these policy changes will not take effect until those Departments have finalized their new regulations, a process that may take several months.

Later in the year, OFAC has posted new frequently asked questions in connection with the President's announcement on changes to U.S. policy with respect to Cuba. According to the FAQ responses, OFAC will implement the Treasury-specific changes via amendments to its Cuban Assets Control Regulations. The Department of Commerce will implement any necessary changes via amendments to its Export Administration Regulations. OFAC expects to issue its regulatory amendments in the coming months. The announced changes do not take effect until the new regulations are issued.

One of the more significant changes is to the travel authorizations that are currently implemented by OFAC in the form of general licenses. For example, individual people-to-people travel will no longer be authorized. OFAC defines this term as follows:

> *Individual people-to-people travel is educational travel that: (i) does not involve academic study pursuant to a degree program; and (ii) does not take place under the auspices of an organization that is subject to U.S. jurisdiction that sponsors such exchanges to promote people-to-people contact. The President instructed Treasury to issue regulations that will end individual people-to-people travel. The announced changes do not take effect until the new regulations are issued.*

The forthcoming regulations will be prospective and thus will not affect existing travel, contracts and licenses. We will have more information when the changes are implemented into the Cuban Assets Control Regulations.

Later in the year, the U.S. government published changes to the export controls and sanctions on Cuba made pursuant to the **National Security Presidential Memorandum on Strengthening the Policy of the United States Toward Cuba** and both loosen and tighten the trade restrictions.

One noteworthy loosening of the restrictions targets License Exception SCP (Support for the Cuban People) at 15 CFR 740.21. Previously, paragraph (b) of this license exception authorized exports to Cuba of items classified as EAR99 or subject only to Antiterrorism (AT) controls if the items (1) were of a certain type (e.g., building materials and tools) and going to private sector entities or (2) were going to private individuals. Under the new rule, there is no restriction on the types of items going to private sector entities provided the items are EAR99 or subject only to AT controls (except for medicines, medical devices, and agricultural commodities).

Therefore, many items can now be exported to private sector entities in Cuba under this license exception. The covered items include, for example, hardware and software products classified as mass-market encryption items under ECCNs 5A992/5D992 and networking equipment classified under ECCN 5A991.

Before using License Exception SCP, please note that there are some limitations. The items cannot primarily generate revenue for the government of Cuba or contribute to the operation of the Cuban government, including through the construction or renovation of state-owned buildings. There are also restricted parties in Cuba that were named today. Please review these limitations carefully before engaging in any activity, and be mindful of any activity incident to an export that may itself require a license (e.g., financial transactions, travel, interactions with government officials, etc.)

Aside from the changes to License Exception SCP noted above, there were several other regulatory changes, including:

- A BIS policy of denial for the export or reexport of items destined to the Cuban military, police, intelligence, or security services; and
- Publication of **New List of Restricted Entities in Cuba**, including the list of Cuban government officials ineligible to receive items exported under License Exceptions GFT, CCD, and SCP.

OFAC has also published a Fact Sheet and OFAC FAQ pertaining to the changes.

North Korea

The President issued a new Executive Order this year, Executive Order 13810 of September 20, 2017, imposing additional sanctions with respect to North Korea. The Executive Order blocks the property or interest in property of any person determined by OFAC:

1. to operate in the construction, energy, financial services, fishing, information technology, manufacturing, medical, mining, textiles, or transportation industries in North Korea;

2. to own, control, or operate any port in North Korea, including any seaport, airport, or land port of entry;
3. to have engaged in at least one significant importation from or exportation to North Korea of any goods, services, or technology;
4. to be a North Korean person, including a North Korean person that has engaged in commercial activity that generates revenue for the Government of North Korea or the Workers' Party of Korea;
5. to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any person whose property and interests in property are blocked pursuant to this order; or
6. to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order.

In response to the Executive Order, OFAC published new and updated FAQs along with a new General License 10 and an updated General License 3-A.

The Executive Order should not have an impact on current exports to North Korea, since the country has been under a general embargo. This is noted in the OFAC FAQ:

> *459. What impact does the prohibition on the exportation or reexportation of goods, services, or technology under Executive Order (E.O.) 13722 have on the regulations of the Department of Commerce's Bureau of Industry and Security (BIS)?*
>
> *None. E.O. 13722 prohibits the exportation or reexportation, from the United States, or by a United States person, of any goods, services, or technology to North Korea. BIS maintains authority to license exports and reexports of goods and technology subject to the Export Administration Regulations to persons who are not Specially Designated National (SDNs) and involving the Government of North Korea and the Workers' Party of Korea. In most instances, to export to designated individuals and entities, U.S. persons must obtain a license from both OFAC and BIS. Regulated financial entities processing a transaction in accordance with a BIS license may want to request a copy of the license to ensure the transaction meets the terms, conditions, and criteria of the BIS license.*

According to OFAC, however, the new Executive Order changes the current sanctions program in the following way:

> *E.O. 13722 provides the Secretary of the Treasury, in consultation with the Secretary of State, additional tools to disrupt North Korea's ability to fund its weapons of mass destruction (WMD) and ballistic missile programs. Specifically, the Executive order:*
>
> 1. *establishes several new designation criteria;*
> 2. *prohibits vessels and aircraft that have called or landed at a port or place in North Korea in the previous 180 days, and vessels that engaged in a ship-to-ship transfer with such a vessel in the previous 180 days, from entering the United States;*
> 3. *provides authority to block any funds transiting accounts linked to North Korea that come within the United States or possession of a United States person; and*
> 4. *provides authority to impose sanctions on a foreign financial institution that knowingly conducted or facilitated, on or after the date of the order (i) any significant transaction on behalf of certain blocked persons or (ii) any significant transaction in connection with trade with North Korea. The sanctions applicable to foreign financial institutions can be restrictions on correspondent or payable-through accounts or full blocking sanctions.*

It does not, however, restrict NGOs from providing humanitarian assistance to the people of North Korea and other activities that have generally been approved through a BIS license.

Sudan

Earlier this year, OFAC issued a general license that suspends the comprehensive sanctions restrictions on Sudan, in connection with ongoing U.S.-Sudan bilateral engagement. Newly authorized transactions include the processing of transactions involving persons in Sudan; the importation of goods and services from Sudan; the exportation of goods, technology, and services to Sudan; and transactions involving property in which the Government of Sudan has an interest. This authorization also applies to some Specially Designated Nationals designated pursuant to the Sudan program. Exports of medical devices, medicine and other items under the TSRA program will generally still require the use of such licenses. However, OFAC noted that it has the authority to suspend, modify or revoke today's authorization at any time. OFAC updated its website with the General License and FAQ.

But, not so fast. BIS maintains separate restrictions on exports of items to Sudan, including hardware, software and technology, as described on the BIS Sudan Country Guidance page of its website. BIS only issued a narrow change to its license review policy for certain civil aviation and railroad applications. BIS did not issue any new authorizations. Therefore, the restrictions on exports to Sudan for anti-terrorism reasons under Section 742.10 of the EAR remain in effect. As a result, outside of the civil aviation and railroad end-use situations, there will be only marginal, if any, impact to many U.S. exporters. Companies that export items controlled under EAR99, or that only provide services (e.g., SaaS applications), may now be authorized to export to Sudan without obtaining a specific license.

Additional Sanctions Updates

Sanctions on the Government Venezuela

The U.S. issued new sanctions making the Government of Venezuela a restricted party under Executive Order 13808, Imposing Additional Sanctions With Respect to the Situation in Venezuela. These sanctions apply to any agency of the Government of Venezuela, as well as any organization/entity owned 50% or more by the government (except there is a general license covering CITGO Holding, Inc.). The scope of these sanctions is limited to financial-related transactions, and is similar in scope to OFAC's Sectoral Sanctions program previously imposed against Russian entities. The sanctions that are most likely applicable to U.S. exporters are those prohibiting any dealing in "new debt" of the Government of Venezuela longer than 30 days or 90 days, depending on the situation.

"New debt" includes offering credit terms for new purchases, such as NET-60 payment terms. Specifically, the restrictions on new debt cover:

- New debt with a maturity of greater than 90 days of Petroleos de Venezuela, S.A. (PdVSA); and
- New debt with a maturity of greater than 30 days of the Government of Venezuela, other than debt of PdVSA.

OFAC published FAQs addressing the new sanctions against the Government of Venezuela.

Removal of Burmese Sanctions Regulations

OFAC published a final rule this year removing from the Code of Federal Regulations the Burmese Sanctions Regulations as a result of the termination of the national emergency on which the regulations were based. On May 20, 1997, the President issued Executive Order 13047, "Prohibiting New Investment in Burma" (E.O. 13047), in which the President declared a national emergency to deal with the unusual and extraordinary threat to the national security and foreign policy of the United States posed by the actions and policies of the Government of Burma, in response to a deepening pattern of severe repression by the State Law and Order Restoration Council, the then-governing regime in Burma.

In E.O. 13047, the President also determined and certified that, for purposes of section 570(b) of the Foreign Operations, Export Financing, and Related Programs Appropriations Act, 1997 (Public Law 104-208), the Government of Burma had committed large-scale repression of the democratic opposition in Burma after September

30, 1996, and E.O. 13047 imposed a prohibition on new investment in Burma. The scope of the national emergency with respect to Burma was modified and additional steps were taken to respond to the threat posed by the actions and policies of the Government of Burma in Executive Order 13310 of July 28, 2003 (E.O. 13310); Executive Order 13448 of October 18, 2007 (E.O. 13448); Executive Order 13464 of April 30, 2008 (E.O. 13464); Executive Order 13619 of July 11, 2012 (E.O. 13619); and Executive Order 13651 of August 6, 2013 (E.O. 13651). Further actions also were taken under Burma sanctions statutes, namely the Burmese Freedom and Democracy Act of 2003 (Public Law 108-61) and the Tom Lantos Block Burmese JADE (Junta's Anti-Democratic Efforts) Act of 2008 (Public Law 110-286) (JADE Act).

On May 21, 1998, OFAC issued the Burmese Sanctions Regulations, 31 CFR part 537 (the "Regulations"), as a final rule to implement E.O. 13047. The Regulations were amended and reissued in their entirety in 2005 to implement E.O. 13310, and again in 2014 to implement E.O. 13448, E.O.13464, E.O. 13619, and E.O. 13651. OFAC also has amended the Regulations on various occasions to add general licenses and make other updates, as well as issued and made available on its Web site several general licenses.

On October 7, 2016, the President issued Executive Order 13742, "Termination of Emergency With Respect to the Actions and Policies of the Government of Burma" (E.O. 13742). In E.O. 13742, the President found that the situation that gave rise to the declaration of a national emergency in E.O. 13047, with respect to the actions and policies of the Government of Burma, had been significantly altered by Burma's substantial advances to promote democracy, including historic elections in November 2015 that resulted in the former opposition party, the National League for Democracy, winning a majority of seats in the national parliament and the formation of a democratically elected, civilian-led government; the release of many political prisoners; and greater enjoyment of human rights and fundamental freedoms, including freedom of expression and freedom of association and peaceful assembly. Accordingly, the President terminated the national emergency declared in E.O. 13047, and revoked that order, E.O. 13310, E.O. 13448, E.O. 13464, E.O. 13619, and E.O. 13651.

As a result, OFAC is removing the Regulations from the Code of Federal Regulations. Pursuant to section 202 of the National Emergencies Act (50 U.S.C. 1622) and section 1 of E.O. 13742, termination of the national emergency declared in E.O. 13047, as modified in scope by E.O. 13448 and E.O. 13619, shall not affect any action taken or proceeding pending not fully concluded or determined as of 1:00 p.m. eastern daylight time on October 7, 2016 (the effective date of E.O. 13742), any action or proceeding based on any act committed prior to the effective date, or any rights or duties that matured or penalties that were incurred prior to the effective date.

Removal of Côte d'Ivoire Sanctions Regulations

OFAC also published a final rule this year removing from the Code of Federal Regulations the Côte d'Ivoire Sanctions Regulations as a result of the termination of the national emergency on which the regulations were based. On February 7, 2006, the President issued Executive Order 13396, "Blocking Property of Certain Persons Contributing to the Conflict in Côte d'Ivoire" (E.O. 13396), in which the President declared a national emergency to deal with the unusual and extraordinary threat to the national security and foreign policy of the United States posed by the situation in or in relation to Côte d'Ivoire. That situation, which had been addressed by the United Nations Security Council in Resolution 1572 of November 15, 2004, and subsequent resolutions, had resulted in the massacre of large numbers of civilians, widespread human rights abuses, significant political violence and unrest, and attacks against international peacekeeping forces leading to fatalities. E.O. 13396 blocked all property and interests in property of the persons listed in the Annex to E.O. 13396 and any person determined to meet one or more of the criteria set out in E.O. 13396.

On April 13, 2009, OFAC issued the Persons Contributing to the Conflict in Côte d'Ivoire Sanctions Regulations, 31 CFR part 543 (the "Regulations"), as a final rule to implement E.O. 13396 (74 FR 16763, April 13, 2009). On July 21, 2009, OFAC issued an amendment to the Regulations to change the heading of the Regulations to the Côte d'Ivoire Sanctions Regulations (74 FR 35802, July 21, 2009). OFAC also amended the Regulations on February 8, 2012, to add a definition of a term used in the Regulations (77 FR 6463, Feb. 8, 2012).

On September 14, 2016, the President issued Executive Order 13739, "Termination of Emergency With Respect to the Situation in or in Relation to Côte d'Ivoire" (E.O. 13739). In E.O. 13739, the President found that the situation that gave rise to the declaration of a national emergency in E.O. 13396 with respect to the situation in or in relation to Côte d'Ivoire had been significantly altered by the progress achieved in the stabilization of Côte d'Ivoire, including the successful conduct of the October 2015 presidential election, progress on the management of arms and related materiel, and the combatting of illicit trafficking in natural resources. Accordingly, and in view of the removal of multilateral sanctions by the United Nations Security Council in Resolution 2283, the President terminated the national emergency and revoked E.O. 13396. Therefore, OFAC is removing the Regulations from the Code of Federal Regulations. Pursuant to section 202 of the National Emergencies Act (50 U.S.C. 1622) and section 1 of E.O. 13739, termination of the national emergency declared in E.O. 13396 shall not affect any action taken or proceeding pending and not fully concluded or determined as of 8:00 a.m. eastern daylight time on September 14, 2016 (the effective date of E.O. 13739), any action or proceeding based on any act committed prior to the effective date, or any rights or duties that matured or penalties that were incurred prior to the effective date.

Regulatory Updates

In addition to the ECR and Sanctions Updates provided above, BIS, DDTC and OFAC issued several regulatory changes this year. Significant changes are highlighted below. Significant changes and additional regulatory updates are included in the attached regulatory summary.

Hong Kong Export and Reexport Requirements

BIS published new documentation requirements for transactions involving Hong Kong. The new requirements became effective on April 19, 2017. This rule covers any item with an ECCN subject to controls based on National Security (NS), Missile Technology (MT), Nuclear Nonproliferation (NP) column 1, or Chemical and Biological Weapons (CB) reasons, including encryption items controlled under ECCN 5x002.

The new provision at Section 740.2(a)(19) will require that an exporter or re-exporter of a covered item (see above) to Hong Kong under a US license exception (e.g., ENC, GBS, TMP, TSR, TSU) must now obtain a copy of the matching Hong Kong import license that authorizes import into Hong Kong. In cases where no Hong Kong import license is required, the exporter or re-exporter must obtain a copy of a written statement issued by the Hong Kong authorities stating that no import license is required. This documentation must be obtained prior to export/re-export, and is subject to the 5-year recordkeeping requirement under the EAR.

A new provision at Section 748.13 will require that an exporter or re-exporter of a covered item (see above) to Hong Kong under a US export license must obtain the same documentation as described above for use of license exceptions. This documentation must be obtained prior to export/re-export, and is subject to the 5-year recordkeeping requirement under the EAR.

Finally, new provisions at Section 740.2(a)(20) and Section 748.13 will require a re-exporter of a covered item (see above) from Hong Kong to any other location to obtain either (1) a Hong Kong export license or (2) a copy of a written statement issued by the Hong Kong authorities stating that no export license is required. This documentation must be obtained prior to export/re-export, and is subject to the 5-year recordkeeping requirement under the EAR.
For those companies dealing in covered items, this new documentation requirement could impact a wide range of activities (e.g., production shipments, non-production shipments, software downloads, infrastructure operations and outsourced development/production). We suggest that companies impacted should:

1. Conduct a survey of those situations that give rise to an import into Hong Kong or export from Hong Kong of a covered item.
2. Amend existing processes to account for the new documentation requirement and train the relevant personnel.
3. Work with partners in Hong Kong who are likely responsible for obtaining the licenses (e.g., distributors and resellers) and explore whether they could obtain an import license or formal pre-classification review by Hong Kong TID prior to export or re-export in order to satisfy the documentation requirement.

Later in the year, published a new online FAQ addressing the import documentation requirement for exports/re-exports of certain controlled items to Hong Kong. Under the new Hong Kong Rule, exporters/re-exporters of items controlled for national security, missile technology, chemical/biological weapons or nuclear non-proliferation category 1 reasons to Hong Kong must obtain written documentation of the authorization to import into Hong Kong (e.g., an import license) prior to shipment.

In new FAQ #11 (reproduced below), BIS has relaxed the documentation requirement. If the importing party participates in the Hong Kong "Approval-in-Principle" (AIP) program and maintains a valid AIP letter covering the types of items and end-users involved in a particular shipment, that AIP letter can satisfy the new BIS documentation requirement. Therefore, the exporter/re-exporter would not need to obtain copies of each individual import license obtained by the AIP party.

> *Q11. The company that will be importing my items into Hong Kong sent me an Approval-in-Principle letter from the Hong Kong government. Does this letter allow me to ship items prior to obtaining a copy of the Hong Kong import license?*
>
> *The "Approval-in-Principle Arrangement for Bulk users of Strategic Commodities Licensing Service" (AIP) is a special program that expedites license processing times for frequent shippers in Hong Kong. Companies who qualify and apply for AIP are notified of their qualification by an AIP letter issued by the Government of the Hong Kong Special Administrative Region, setting out the relevant products, suppliers/consignees, endusers, etc. for shipments that may be covered by AIP. The AIP letter has a validity period that is normally one year, and companies must renew the letter before it expires to continue enjoying the benefits of AIP. For purposes of the EAR only, you may treat a copy of the AIP letter as a Hong Kong import license, as long as the AIP letter is valid when your shipment takes place and as long as the AIP letter covers the items and parties relevant to your export or reexport to Hong Kong. If you are using an AIP letter as a Hong Kong import license for purposes of the EAR, you must obtain and retain a copy of the AIP letter pursuant to the recordkeeping provisions of sections 740.2(a)(19) and 748.13 of the EAR. Additional information on AIP may be found on Hong Kong Trade and Industry Department's website: https://www.stc.tid.gov.hk/english/circular_pub/2009_stc09.html.*
>
> *The use of an AIP letter for purposes of the EAR does not remove the responsibility of you or your Hong Kong client to comply with any of the import requirements of the Government of the Hong Kong Special Administrative Region, including the requirement to obtain any necessary individual Hong Kong licenses.*

While this new relaxation to the Hong Kong Rule is helpful, exporters/re-exporters still will need to:

1. determine whether the importing party is an AIP participant,
2. identify whether a shipment falls under the particular authorizations in the AIP letter, and
3. determine whether the AIP letter is valid or expired.

Also, note that, according to the Hong Kong TID website, intangible imports of software and technology are not subject to import licensing. Only tangible goods are subject to the licensing requirement. This means that physical shipments of software stored on drives or other tangible media can require import licenses, but electronic transfers do not. FAQs about these rule changes can be found at **BIS Hong Kong FAQs and Hong Kong TID FAQs.**

Encryption Changes

Last year, BIS published amendments to the EAR government the export of Encryption items. These amendments include (1) changes arising from the Obama Administration's ongoing ECR effort, and (2) changes to Category 5, Part 2 of the Commerce Control List of the EAR arising from the 2015 Wassenaar Dual Use List Review. Further, a reorganization of Category 5 – Part 2 resulted in a major reorganization of ECCN 5A002, including the addition of two new ECCN 5A00X subclassifications creating categories for three primary sets of items: Cryptographic "Information Security;" Non-Cryptographic "Information Security;" and, Cryptanalytic Items. Along with the

reorganization of ECCN 5A002, ECCNs 5A992, 5D992, and 5E992 have been adjusted and most items that are not Note 3 (Mass market) items, will be moved from the 5X992 classifications to EAR99.

This year, BIS has updated the encryption section of its website to reflect the changes to the encryption regulations, which were published in September 2016. The encryption section includes:

- Category 5, Part 2 Quick Reference Guide;
- 2 flowcharts that lay out the analysis to follow for determining if and how the EAR and Cat.5 Part 2 apply to a product incorporating cryptography; and
- "Encryption Outline" to determine if items ARE or ARE NOT subject to the EAR, Types of Authorizations for encryption items, and pre- and post-shipment requirements.

Later in the year, BIS amended Category 5, Part 2 of the EAR based on the changes agreed upon by the Wassenaar Arrangement at the 2016 Plenary meeting advocating implementation of effective export controls on strategic items, including a reorganization of various decontrol and exclusionary notes into more positive language. These changes are described in detail in the *Wassenaar Implementation* section below.

ZTE Entity List Addition

In 2016, BIS added ZTE Corporation and several related entities to the **BIS Entity List**, which imposed a licensing requirement for activities involving listed entities for all items subject to the EAR, with a presumption of denial for all export license applications.

The four (4) entities added to the Entity List (3 in China and 1 in Iran) in March were:

1. Beijing 8-Star International Co., Unit 601, 6th Floor, Tower 1, Prosper Center, No. 5, Guanghua Road, Chaoyang District, Beijing, China;
2. Zhongxing Telecommunications Equipment (ZTE) Corporation, ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District, Shenzen, China; and
3. ZTE Kangxun Telecommunications Ltd., 2/3 Floor, Suite A, Zte Communication Mansion Keji (S) Road, Hi-New Shenzhen, 518057 China.
4. ZTE Parsian, No. 100, Africa Ave., Mirdamad Entersection, Tehran, Iran.

According to the BIS Website, the principal bases for the addition of these entities were two ZTE corporate documents entitled Report Regarding Comprehensive Reorganization and the Standardization of the Company Export Control Related Matters and Proposal for Import and Export Control Risk Avoidance. These documents outline a ZTE-developed scheme to violate U.S. export control laws by establishing, controlling, and using a series of “detached” (e.g., shell or front) companies to illicitly reexport controlled items to sanctioned countries without authorization.

Later in the month, BIS published a final rule that temporarily permitted exports to ZTE Corp. and ZTE Kangxun (but not to ZTE Parsian or to Beijing 8-Star) under a new temporary general license. The net effect is that, from the date of the publication until the end of the temporary general license, the export license requirements and policies that had been in place prior to March 8, 2016 (when BIS added the four ZTE companies to the Entity List) temporarily will be reinstated (but only with respect to two of those ZTE companies).

The temporary general license was extended until March of this year, when ZTE Corporation and the Departments of Justice, Commerce and Treasury announced a global settlement of charges that ZTE violated the International Emergency Economic Powers Act (IEEPA), the Export Administration Regulations (EAR) and OFAC Regulations. In total, ZTE agreed to pay the U.S. Government $892,360,064 and agreed to a significant conduct remedy, in the various plea and settlement agreements.

In light of the settlement of administrative and criminal enforcement actions against ZTE Corporation and ZTE Kangxun, the End-User Review Committee (ERC) at BIS has determined that these two persons being removed

have performed their undertakings to the U.S. Government in a timely manner and have otherwise cooperated with the U.S. Government in resolving the matter which led to the two entities' listing. Therefore, ZTE Corporation and ZTE Kangxun were removed from the Entity List in a final rule published by BIS. Note also that ZTE Pars and Beijing 8Star remained on the Entity List.

In an interesting twist, BIS added former ZTE CEO Shi Lirong to the Entity List, claiming that Shi Lirong signed and approved the document "Report Regarding Comprehensive Reorganization and Standardization of the Company Export Control Related Matters," which described how ZTE planned and organized a 7 scheme to establish, control and use a series of "detached'' (i.e., shell) companies to illicitly reexport controlled items to Iran in violation of U.S. export control laws. Additional details describing the enforcement actions can be found in the *Enforcement Actions* section below.

Wassenaar Implementation

BIS published amendments to the EAR in the Federal Register to the EAR. These amendments include changes agreed upon by the Wassenaar Arrangement at the 2016 Plenary meeting advocating implementation of effective export controls on strategic items. We have included several noteworthy changes to Categories 3, 4 and 5 (Part 1 and 2) highlighted below.

Summary of Changes to Category 3

3A001.a.5.a is updated. This control on analog-to-digital converters (ADCs) is revised by updating the ADC control thresholds (resolution) for the higher performance ADCs to reflect the technology that is used in the commercial mainstream, which will result in a decrease of license application submissions. In addition, the unit for resolution is amended by replacing "billion words per second" with "Giga Samples Per Second (GSPS)" and "million words per second" with "Mega Samples Per Second (MSPS)" to clarify what is being measured for this parameter.

For example, ECCN 3A001.a.5.a.1 used to control ADCs with a resolution of 8 bit or more, but less than 10 bit, with an output rate greater than 1 billion words per second. The new ECCN 3A001.a.5.a.1 will control ADCs with a resolution of 8 bit or more, but less than 10 bit, with an output rate greater than 1.3 Giga Samples Per Second (GSPS).

3A001.b.11 is updated. "Frequency synthesizer" "electronic assemblies" is amended by updating the parameters to align the 3A001.b.11 frequency synthesizer controls with the 3A002.d.3 signal generator controls. Specifically, Items paragraphs 3A001.b.11.a through .e are revised and b.11.c and .f are removed and reserved.

For example, ECCN 3A001.b.11.a used to control "Frequency synthesizer" "electronic assemblies" having "frequency switching time" less than 156 ps. The new ECCN 3A001.b.11.a will control "Frequency synthesizer" "electronic assemblies" having a "frequency switching time" less than 143 ps.

Summary of Changes to Category 4

Increase in the Adjusted Peak Performance for Computers

4A003 "Digital computers," "electronic assemblies," and related equipment: The "Adjusted Peak Performance" for "digital computers" is raised from 12.5 to 16 Weighted TeraFLOPS (WT) in Items paragraph 4A003.b.
4D001 "Software" and 4E001 "technology" is amended as follows:

1. The TSR paragraph in the List Based License Exceptions section is revising the APP from 12.5 to 16 WT
2. The Special Conditions for STA paragraph is revising the APP from 12.5 to 16 WT and
3. Items paragraph .b.1 in the List of Items Controlled section is amended by revising the APP from 6.0 to 8.0 WT.

Under License Exception APP, this rule also moves Burma from paragraph (d)(1) "Computer Tier 3" to the more favorable paragraph (c)(1) "Computer Tier 1."

Summary of Changes to Category 5, Part 1: Telecommunications

5A001.b.6 is updated. It now controls equipment employing digital signal processing to provide voice coding output at rates less than 700 bit/s. [This refers to taking samples of human voice and then converting these samples of human voice into a digital signal taking into account specific characteristics of human speech.] The previous entry specified 2,400 bit/s.

5B001.b.2.c is removed. It previously controlled equipment used to develop telecommunications equipment employing coherent optical transmission or coherent optical detection techniques

5E001.c.1 is removed. It previously controlled technology for the development/production of equipment employing digital techniques designed to operate at a total digital transfer rate exceeding 560 Gbit/s.

5E001.c.2.c is removed. It previously controlled technology for the development/production of equipment employing coherent optical transmission or coherent optical detection techniques

Summary of Changes to Category 5, Part 2: Information Security

Reorganized various decontrol and exclusionary notes into more positive language:

Reorganized the Note 4 decontrol note as a more positive list, by removing it and rewriting ECCN 5A002 and its sub-paragraphs. Previously, 5A002.a.1 was a catch-all and covered most encryption items classified under 5A002. Now, the new subparagraphs track the types of items previously ineligible for decontrol under Note 4:

- Paragraph a.1: Items having information security as a primary function
- Paragraph a.2: Digital communication or networking systems, equipment or components
- Paragraph a.3: Computers, other items having information storage or processing as a primary function, and components therefor
- Paragraph a.4: Other items where the cryptographic functionality supports a non-primary function AND where such cryptographic functionality is performed by incorporated components/software that are, as standalone items, decontrolled from 5A/5D002.

Moved cryptographic activation software from ECCN 5D002.d to 5D002.b

Added a definition of the uses of encryption that are decontrolled:

- Authentication
- Digital signature
- Data integrity
- Non-repudiation
- Digital rights management, including the execution of copy-protected software
- Encryption or decryption in support of entertainment, mass commercial broadcasts or
- Medical records management
- Key management in support of any function described above

Expanded the scope of the Note 4 decontrol through new catch-all language at 5A002.a.4. Previously, all uses of encryption must have supported the primary function of the item in order to qualify for Note 4 decontrol. Now, encryption that supports a non-primary function is still within the decontrol if the component providing that encryption is itself excluded from 5A002 (e.g., a mass-market component controlled under 5A992.c). Examples of items covered by this new expanded scope include:

- An automobile where the only cryptographic functionality is provided by a mobile telephone that is built into the car
- An exercise bike with an embedded web browse

Clarified the scope of the decontrol notes to 5A002.a (now reorganized as Note 2 to 5A002.a) so that components specially designed for a listed decontrolled item are also themselves decontrolled from 5A002. For example, this could include components for wireless PANs, components for certain RAN equipment with an RF output power limited to 0.1W, or components for certain routers/switches performing only OAM encryption.

In total, 50 ECCNs will be revised by this final rule, so we do encourage exporters to review the entire rule and determine if it affects your current export classification and licensing strategy. Some practical tips include:

1. Review any existing items/technologies currently classified under the impacted ECCNs for potential updates. This could include a minor change in subparagraph for a controlled ECCN or a drop to a less restrictive ECCN due to the control parameter increase under the rule change.
2. Identify any existing export licenses (i.e. 3E001, 4E001, 5E001.c.1 and c.2) that may no longer be applicable.
3. For encryption items, (1) determine whether products previously ineligible for control under Note 4 are now excluded from control under the new 5A002.a.4 and (2) review new Note 2 to 5A002.a to determine whether components designed for a particular decontrolled end-item may be excluded from control under Category 5 – Part 2.

Missile Technology Control Regime Implementation

BIS amended the EAR to reflect changes to the Missile Technology Control Regime (MTCR) Annex that were agreed to by MTCR member countries at the October 2016 Plenary in Busan, South Korea, and the March 2016 Technical Experts Meeting (TEM) in Luxembourg City, Luxembourg. This final rule revises thirteen Export Control Classification Numbers, adds one ECCN, revises two EAR defined terms (including making other EAR conforming changes for the use of these two terms) and makes conforming EAR changes where needed to implement the changes that were agreed to at the meetings and to better align the missile technology (MT) controls on the Commerce Control List with the MTCR Annex. This final rule amends the CCL to reflect changes to the MTCR Annex by amending thirteen ECCNs and adding new ECCN 9B104, as follows:

ECCN 1C107. This final rule amends ECCN 1C107 by revising the introductory text of paragraph d. and adding a paragraph d.3 in the List of Items Controlled section. This final rule also adds a Note and a Technical Note to ECCN 1C107.d.3 to clarify the scope of paragraph d.3. (MTCR Annex Change, Category II: Item 6.C.6., Busan 2016 Plenary). Specifically, in the introductory text of ECCN 1C107.d, this final rule removes the phrase "silicon carbide materials" and adds in its place the phrase "high-temperature materials." This change is made because of the addition of certain bulk machinable ceramic composite materials that this final rule adds to ECCN 1C107 under new "items" paragraph d.3. Ultra High Temperature Ceramic Composites (UHTCC) are materials that combine Ultra High Temperature Ceramics (UHTC) with fiber reinforcement. The UHTCs can be used in environments that exhibit extremes in temperature, chemical reactivity, and erosive attack. The combination of the UHTC and fiber reinforcement can mitigate some of the traditional drawbacks associated with ceramics, including a tendency to fracture. Typical end uses for these composites are leading edges for hypersonic vehicles, nose tips for re-entry vehicles, rocket motor throat inserts, jet vanes, and control surfaces, which this final rule adds as examples in the new control text. This final rule also adds a note to 1C107.d.3 to make clear that the UHTC materials that do not have fiber reinforcement are not caught under this control. Additionally, this final rule adds a technical note to 1C107.d to provide examples of UHTCs which are included. This change is expected to result in an increase of 1-3 applications received annually by BIS. This very small increase is because this material is not widely used or exported, but specific to the end uses described in the control text.

ECCN 1C111. This final rule amends ECCN 1C111 by revising paragraphs b.2 in the List of Items Controlled section to add a CAS (Chemical Abstract Service) Number. CAS Numbers are numerical identifiers assigned by the

Chemical Abstracts Service (CAS) to every chemical substance described in open scientific literature, including organic and inorganic compounds, minerals, isotopes and alloys. The inclusion of CAS Numbers will make it easier to identify the materials controlled under this "items" paragraph of 1C111. This final rule revises paragraph b.2 to add the CAS Number (CAS 69102-90-5) after the material "Hydroxy-terminated polybutadiene (including hydroxyl-terminated polybutadiene) (HTPB)." (MTCR Annex Change, Category II: Item 4.C.5.b., Busan 2016 Plenary). This change is not expected to have any impact on the number of license applications received by BIS.

ECCN 2B018. This final rule amends ECCN 2B018 by revising the "MT" paragraph in the table in the License Requirements section by revising the term "ballistic missile systems" to remove the term "systems" and add an "s" to the term "missile." (MTCR Annex Change, Category I: Item 1.A.1., Luxembourg 2016 TEM). In addition, in the same "MT" paragraph, this final rule revises the term "cruise missile systems" to remove the term "systems" and add an "s" to the term "missile." (MTCR Annex Change, Category I: Item 1.A.2., Luxembourg 2016 TEM). Lastly, this final rule makes conforming changes in the same "MT" paragraph by replacing the term "unmanned air vehicles" with "unmanned aerial vehicles" wherever this term appears in this section. (Conforming Change to MTCR Annex). Substantively, there is no difference between the old and revised terms, but this final rule makes these conforming changes to ensure consistent use of the terminology throughout the EAR. These are conforming changes for the changes described above to the definitions of "missiles" and "unmanned aerial vehicles." This is a clarification and will not change any scope of control. This change is not expected to have any impact on the number of license applications received by BIS.

ECCN 2B109. This final rule amends ECCN 2B109 by revising the list of examples included in the second technical note. This final rule expands the list of examples to include interstages, because interstages can also be manufactured using the flow forming machines described in ECCN 2B109. (MTCR Annex Change, Category II: Item 3.B.3., Busan 2016 Plenary). This change is not expected to have any impact on the number of license applications received by BIS, because this is only a change to the list of examples of products that can be made by this type of machine, and it does not change the scope of control.

ECCN 5A101. This final rule amends the heading of ECCN 5A101 by revising the term "ballistic missile systems" to remove the word "systems" and add an "s" to "missile." (MTCR Annex Change, Category I: Item 1.A.1., Luxembourg 2016 TEM). The final rule revises the heading by revising the term "cruise missile systems" to remove the word "systems" and add an "s" after "missile." (MTCR Annex Change, Category I: Item 1.A.2., Luxembourg 2016 TEM). These are conforming changes for the changes described above to the definitions of "missiles" and "unmanned aerial vehicles." In addition, this final rule revises the heading of ECCN 5A101 to create a separate parenthetical phrase for the illustrative list of examples that are unmanned aerial vehicles. This final rule does this by removing the examples of "cruise missiles, target drones, and reconnaissance drones" from the list of examples that followed the terms "unmanned aerial vehicle or rocket systems" in the heading and adding those examples immediately after the term unmanned aerial vehicle. This final rule retains the rest of the examples from the parenthetical that follows the term "rocket systems," which will make it clearer that this parenthetical list is an illustrative list of "rocket systems." (Conforming Change to MTCR Annex). These are clarifications and will not change any scope of control. These changes are not expected to have any impact on the number of license applications received by BIS.

ECCN 7A103. This final rule amends ECCN 7A103 by adding a definition for "inertial measurement equipment and systems" for purposes of ECCN 7A103. In addition, this final rule revises "items" paragraph a and adds Note 3 in the List of Items Controlled section. (MTCR Annex Change, Category II: Item 9.A.6., Luxembourg 2016 TEM). This final rule makes these changes to remove the ambiguous term "other equipment." Instead, the locally defined term "inertial measurement equipment or systems" that the final rule adds to ECCN 7A103, along with an illustrative list of such equipment and systems, clarifies which types of equipment containing the specified accelerometers or gyros are caught by this entry. This final rule also removes the phrase "and systems incorporating such equipment" because this phrase has been removed from the MTCR Annex. The changes this final rule makes to ECCN 7A103 to increase the clarity of the control should make the control more precise and rule out items not strictly used for navigation purposes. This change is expected to result in a decrease of 3 to 5 license applications received annually by BIS. Lastly, this final rule updates and amends ECCN 7A103 by removing Related Controls paragraph (2), which is no longer accurate after changes were made to the EAR to correspond with changes made to

USML Category XII (especially for unmanned aerial vehicles (UAVs)) that became effective December 31, 2016 (See October 12, 2016, (81 FR 70320) final rule). In addition, this paragraph (2) can be removed because the USML Order of Review and CCL Order of Review will provide sufficient guidance on where items that are subject to the ITAR are classified under the USML and where items that are subject to the EAR are classified in either the "`600 series" or in other ECCNs in Category 7 of the CCL. Lastly, as a conforming change to the removal of paragraph (2), this final rule redesignates Related Controls paragraph (3) as new Related Controls paragraph (2).

ECCNs 9A101, 9E101, and 9E102. This final rule amends ECCN 9E101 by revising the Related Controls paragraph in the List of Items Controlled section to make a conforming change for the use of the term "unmanned air vehicles," which this final rule changes to "unmanned aerial vehicles." In addition, this final rule amends ECCN 9E101 and 9E102 by revising the headings of these two ECCNs to make conforming changes for the use of the term "unmanned air vehicles," which this final rule changes to "unmanned aerial vehicles." Substantively, there is not a difference in the two formulations of the term, but for consistency with how the term is used in other parts of the EAR, this final rule makes these conforming changes. (Conforming Change to MTCR Annex). This is a clarification and will not change any scope of control. These changes are not expected to have any impact on the number of license applications received by BIS.

New ECCN 9B104 and Related Conforming Amendments to 9D101, 9E001, and 9E002. This final rule adds new ECCN 9B104 to control certain aerothermodynamic test facilities. The facilities controlled under this new ECCN 9B104 are those that are usable for rockets, missiles, or unmanned aerial vehicles capable of achieving a "range" equal to or greater than 300 km and their subsystems, and having an electrical power supply equal to or greater than 5 MW or a gas supply total pressure equal to or greater than 3 MPa. This final rule adds this new ECCN 9B104 to complement the controls that already exist for aerodynamic test facilities in order to fully cover the types of ground test facilities necessary to reproduce the flight environments that occur during the reentry phase. Plasma arc jet and plasma wind tunnel facilities simulate the atmospheric reentry thermal effects due to high velocity around the vehicles and are key to the qualification of vehicle thermal protection subsystems. This final rule includes values for electrical power supply and gas supply total pressure in new ECCN 9B104 to exclude commercial systems of a similar nature from this new ECCN.

In addition, this final rule adds a Related Definition as part of new ECCN 9B104 to define the term "aerothermodynamic test facilities". This definition specifies that these facilities include plasma arc jet facilities and plasma wind tunnels for the study of thermal and mechanical effects of airflow on objects. (MTCR Annex Change, Category II: Item 15.B.6., Luxembourg 2016 TEM). As a conforming change to the addition of ECCN 9B104, this final rule adds 9B104 to the heading of ECCN 9D101 and revises the "MT" paragraph in the table in the License Requirements section of ECCNs 9E001 and 9E002 to add 9B104. The headings of ECCNs 9E001 and 9E002 do not need to be revised to add technology for 9B104, because those two technology ECCNs apply to 9B ECCNs, except for those specifically excluded in the ECCN headings. These changes are expected to result in an increase of no more than 1 application received annually by BIS, because such systems and their software and technology are exported infrequently.

ECCN 9D104. This final rule amends ECCN 9D104 by adding a note to the List of Items Controlled section. This note clarifies that ECCN 9D104 also includes specific software for the conversion of manned aircraft to an unmanned aerial vehicle. (MTCR Annex Change, Category II: Item 1.D.2., Luxembourg 2016 TEM). This change is expected to result in an increase of 1 to 2 applications received annually by BIS, because, although this software was already controlled here, the note will clarify the scope of ECCN 9D104.

BIS issues Clarifications to the EAR for the use of License Exceptions GOV and STA

BIS published a final rule this year making clarifications to the Export Administration Regulations to provide guidance based on existing agency understanding and practice on the use of two license exceptions. Specifically, this final rule makes three clarifications to License Exception Governments, International Organizations, International Inspections under the Chemical Weapons Convention, and the International Space Station (GOV) and adds five notes, along with making other minor clarifications, to License Exception Strategic Trade Authorization (STA). These revisions respond to questions BIS has received about the use of these two EAR license exceptions

and provide the general public answers to frequently asked questions based on existing agency interpretive practice. Therefore, the clarifications in this final rule do not change the EAR requirements for the use of the license exceptions but are intended to assist exporters new to the EAR.

This final rule revises part 740 of the EAR by clarifying two license exceptions based on existing agency understanding and practice. To provide the general public with guidance on using these license exceptions, this final rule makes three clarifications to License Exception Governments, International Organizations, International Inspections under the Chemical Weapons Convention, and the International Space Station (GOV) and adds five notes, along with making other minor clarifications, to License Exception Strategic Trade Authorization (STA). These changes are described below under sections: (A) Clarifications for License Exception GOV and (B) Clarifications for License Exception STA.

With these revisions, BIS is not changing the EAR requirements for the use of these license exceptions. Instead, the agency seeks to provide sufficient guidance within the EAR to answer questions the agency frequently receives from the public as to the application of the two license exceptions. These clarifications should be particularly helpful to exporters who are new to the EAR, including exporters of items that have recently moved to the EAR from the International Traffic in Arms Regulations as a result of the United States Munitions List to the Commerce Control List review process.

OFAC SDN List Removal Requirements

OFAC published Frequently Asked Questions on its website related to petitions for removal from the SDN list. According to the website:

> *The power and integrity of the Office of Foreign Assets Control (OFAC) sanctions derive not only from its ability to designate and add persons to the **Specially Designated Nationals and Blocked Persons List (SDN List)**, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. Each year, OFAC removes hundreds of individuals and entities from the SDN List. Each removal is based on a thorough review by OFAC. Maintaining the integrity of U.S. sanctions is a high priority for OFAC and is the driving principle behind its rigorous review process that evaluates every request for removal individually on its merits and applies consistent standards to all of them.*

Additional information can be found on the **OFAC website**.

Clarifications on Filing Requirements under the Foreign Trade Regulations

The Census Bureau issued a Final Rule amending the Foreign Trade Regulations (FTR) to reflect new export reporting requirements. Specifically, the Census Bureau is making changes related to the implementation of the International Trade Data System (ITDS), in accordance with the Executive Order 13659, "Streamlining the Export/Import Process for American Businesses." The ITDS was established by the Security and Accountability for Every (SAFE) Port Act of 2006. The changes also include the addition of the original Internal Transaction Number (ITN) data element in the Automated Export System (AES). Lastly, the Census Bureau is making remedial changes to improve clarity of the reporting requirements.

The Census Bureau is responsible for collecting, compiling, and publishing trade statistics for the United States under the provisions of Title 13 of the United States Code (U.S.C.), Chapter 9, Section 301. The ITDS is the means by which the data and business process needs of all Government agencies with a role in international trade will be incorporated into the design of the Automated Commercial Environment (ACE). Through the ITDS initiative, ACE will become the “single window,” the primary system through which the international trade community will submit import and export data and documentation required by all Federal agencies.

The AES or any successor system, is the mechanism by which the Census Bureau collects Electronic Export Information (EEI), the electronic equivalent of the export data formerly collected on the Shipper's Export

Declaration, reported pursuant to Title 15, Code of Federal Regulations, Part 30. In order to achieve the goals of the ITDS, the AES has been incorporated into ACE, the "single window" operated and maintained by U.S. Customs and Border Protection (CBP) as the primary system through which the international trade community will submit import and export data. Additionally, the AES will include export information collected under the authority of other federal agencies, which is subject to those agencies' disclosure mandates.

The Census Bureau is adding a new original Internal Transaction Number (ITN) data element. The original ITN is an optional data element that can be used if a previously filed shipment is replaced or divided and for which a new EEI record(s) must be filed. The addition of the original ITN will assist the export trade community and enforcement agencies in verifying that a filer completed the mandatory filing requirements for the original shipment and any additional shipment(s).

The revised timeframes for split shipments addressed in FTR Letter #6, Notice of Regulatory Change for Split Shipments, are incorporated into the regulatory text of this final rule.

Finally, the U.S. Department of Homeland Security and the U.S. Department of State concur with the revisions to the FTR as required by Title 13, U.S.C., Section 303, and Public Law 107-228, div. B, title XIV, Section 1404.

The Automated Export System has a New Data Element

The Census Bureau published a summary of its Final Rule entitled, "Foreign Trade Regulations (FTR): Clarification on Filing Requirements." This rule addresses new export reporting requirements related to the International Trade Data System and includes the addition of a new data element, the original Internal Transaction Number that can be reported in the Automated Export System. The original ITN field is an optional data element that can be used when a previously filed shipment is replaced, divided or cancelled.

The Census Bureau decided to add the original ITN data element to address situations when a party involved in an export transaction received penalties for shipments that were originally filed on time, but whose shipments were divided while in transit to the ultimate consignee. This data element makes it possible for U.S. Customs and Border Protection to identify AES filings that are associated with previously filed shipments. Prior to the original ITN field, CBP was unable to determine if a shipment, identified as late, was associated with a shipment originally filed in accordance with the FTR. The inclusion of the original ITN field will enable parties in an export transaction to proactively provide CBP with additional information and will allow CBP to conduct a more thorough review of these types of shipments prior to assessing any penalties.

Example:

A foreign buyer in Italy purchases $20,000 worth of jewelry from a U.S. seller. The U.S. seller ships the jewelry to the buyer, but while in transit the seller is contacted by the buyer who now only wants $8,000 worth of jewelry. The seller then finds a new buyer in Sweden for the remaining $12,000 worth of jewelry. The originally filed AES record needs to be updated to reflect the value of $8,000 for the buyer in Italy. Additionally, a new AES record is created for the new buyer in Sweden. This new filing would generate a late filing compliance alert. However, to ensure CBP is aware that the new shipment was filed prior to exportation in accordance with the FTR, the filer can include the previously filed ITN in the original ITN field.

U.S. Census Blog Updates

Combating the Fear of Routed Export Transactions

The U.S. Census Bureau published the following blog, Combating the Fear of Routed Export Transactions, *as a guide for the U.S. authorized agent and U.S. Principal Party in Interest in a routed export transaction.*

Routed export transactions always seem to be a hot topic. We receive numerous questions via our call center, webinars and seminars as companies look to better understand their roles and responsibilities to remain compliant.

The Foreign Trade Regulations (FTRs) define a routed export transaction as a transaction in which the Foreign Principal Party in Interest (FPPI) authorizes a U.S. agent to facilitate export of items from the United States on its behalf, and prepare and file the Electronic Export Information (EEI). In this type of transacti on, the FPPI is controlling the movement of the goods.

Advice for ALL Parties in a Routed Export Transaction:

- *Communication. Make sure communication is clarified and understood between all parties participating in the transaction.*
- *Documentation. Keep all documentation, such as emails, invoices and phone calls on all export transactions for five years from the date of export.*
- *Appropriate authorization. Obtain a Power of Attorney (POA) or written authorization from the FPPI. The POA or written authorization should not be provided by the U.S. Principal Party in Interest (USPPI) in a routed export transaction.*

Advice for the USPPI in a Routed Export Transaction:

- *If possible, request to file the EEI:*
    - *If filing, obtain a POA or written authorization from the FPPI before filing the EEI.*

- *If the FPPI authorizes a U.S. agent to file the EEI:*

    - *Provide the data elements listed in section 30.3(e)(1)(i) through (xii) of the FTR to the U.S. authorized agent.*
    - *Request a copy of the data elements you provided to the U.S. authorized agent filed in the Automated Commercial Environment (ACE) as well as request the Internal Transaction Number (ITN), date of export and filer name.*
    - *Request a copy of the authorized agent's POA or written authorization from the FPPI.*
    - *Sign up for ACE Export Reports. The USPPI can access ACE Report 203 for routed transactions to obtain a copy of the data elements submitted through the ACE along with the ITN, date of export and filer name. More information on accessing ACE reports can be found **here**.*

Advice for the U.S. Authorized Agent in a Routed Export Transaction:

- *Obtain a POA or written authorization from the FPPI before filing the EEI.*
- *Obtain the data elements listed in section 30.3(e)(1)(i) through (xii) of the FTR from the USPPI.*
- *If you are having trouble obtaining information from the USPPI, refer them to section 30.3(e)(1) of the FTR so the USPPI will know the law requires this information. The FTR is located **here**. If you need further assistance, please call the Trade Regulations Branch staff and we may be able to assist.*
- *Provide the USPPI with a copy of the POA or written authorization from the FPPI, a copy of the data elements provided by the USPPI that were submitted through ACE along with ITN, date of export and filer name. Authorized agents should use this as a best practice, but it is only required if requested by the USPPI.*

Finding Your Schedule B Number

The U.S. Census Bureau also published the following blog, *Finding Your Schedule B Number*, as a guide for U.S Exporters that need to determine the Schedule B Number for their exports.

Schedule B numbers are 10-digit statistical classification codes for all domestic and foreign goods being exported from the United States. With over 9,000 codes, the process can seem overwhelming. Here are the steps to find the appropriate number for your goods using the U.S. Census Bureau's Schedule B search engine. To find the Schedule

B search engine, you should start at census.gov/trade and click on the gray Schedule B tab. The link to the search engine is located in the second red box labeled Schedule B Search.

The search engine will ask questions to narrow down the Schedule B options based on key words that you input. Some searches will be easy and take you directly to the code. Other searches may require multiple attempts. The search engine may ask about composition, capacity, power source, end use or function. These key characteristics allow the search engine to hone in on the appropriate Schedule B for your product. Please see Foreign Trade Regulations §30.36-30.40 for additional details on filing exemptions per Schedule B number.

For example, you have designed a new shirt for babies and would like to sell it in foreign markets. Here is a step by step process that demonstrates the search for the new shirt's Schedule B Number:

1. *Type "shirt" into the search engine, and click the "Classify" button.*
2. *The search engine will ask about the shirt's construction.*
3. *If you choose "Knitted or Crocheted," the search engine will ask for whom the shirt is intended. By holding your cursor over the blue asterisk next to "Babies," additional detail about who is included in the category of babies will appear.*
4. *Select "Babies'." The search engine will ask about the composition of the shirt. Notice under "Known Characteristics," you can see the search engine made an assumption that the shirt was made of textile material, not bamboo, etc., and took you directly to the question about the textile material breakdown.*
5. *When you indicate that the shirt is mostly composed of other textile materials, the search engine takes you directly to the section "Babies' garments and clothing accessories, knitted or crocheted: - Of other textile materials."*
6. *First, you should always read the four-digit heading description and six-digit subheading description to make sure the results accurately describe your product. If the answer is yes, continue to step 7. However, if the description does not match your product, review the "Assumed Characteristics" and "Known Characteristics" to see if you need to change your selection or start back at the beginning using another term.*
7. *Next, you should click on the plus sign next to "- Of other textile materials:" to view detailed lines for "babies' shirts of other textile materials".*
8. *If you think you have found the correct number for your product, select the 10-digit number, or Schedule B, that best matches your product. Note that the unit of measure (UOM) on the right side of the screen for each number. These numbers require two units, the number of shirts in dozens (Doz.) and the net weight in kilograms (kg).*
9. *For additional information about the commodities in this section, click on the "Legal Notes" tab.*

Finding a Schedule B number can be a complex process, however, the Census Bureau Schedule B search engine can be helpful in narrowing down which number you report for your goods.

For more help with your search, you can call the International Trade Help Line at 800-549-0595, Option 2 for Commodity Classification Assistance, or email <eid.scheduleb@census.gov>.

Enforcement Actions

BIS added several export violation cases to its Electronic FOIA Reading Room, and the Orders and Settlement Agreements for select cases can be found on BIS's website.

OFAC's Civil Penalties and Enforcement Information can also be found on OFAC's website, and included 16 penalties and settlements in 2017.

DOJ updated the summaries of major U.S. export enforcement and embargo-related criminal cases since 2008, which resulted from investigations by the Department of Homeland Security's U.S. Immigration and Customs Enforcement, the Federal Bureau of Investigation, BIS, the Pentagon's Defense Criminal Investigative Service, and

other law enforcement agencies. The complete summary dating back to 2008 can be found on DOJ's website, but the current list has not been updated since February of this year.

The following is a selection of significant enforcement actions from 2017. Links to additional information are provided in the heading of each case, if available.

ZTE Settlement and Removal of ZTE Corporation and ZTE Kangxun from the Entity List

In 2017, ZTE Corporation and the Departments of Justice, Commerce and Treasury announced a global settlement of charges that ZTE violated the International Emergency Economic Powers Act, the Export Administration Regulations and the Office of Foreign Assets Control Regulations. In total, ZTE has agreed to pay the U.S. Government $892,360,064 and agreed to a significant conduct remedy, in the various plea and settlement agreements described below.

In light of the recent settlement of administrative and criminal enforcement actions against ZTE Corporation and ZTE Kangxun, the End-User Review Committee (ERC) at BIS determined that these two persons being removed have performed their undertakings to the U.S. Government in a timely manner and have otherwise cooperated with the U.S. Government in resolving the matter which led to the two entities' listing. Therefore, ZTE Corporation and ZTE Kangxun have been removed from the Entity List in a final rule published by BIS.

In an interesting twist, BIS added former ZTE CEO Shi Lirong to the Entity List, claiming that Shi Lirong signed and approved the document "Report Regarding Comprehensive Reorganization and Standardization of the Company Export Control Related Matters," which described how ZTE planned and organized a 7 scheme to establish, control and use a series of "detached'' (i.e., shell) companies to illicitly reexport controlled items to Iran in violation of U.S. export control laws. Note also that ZTE Pars and Beijing 8Star remain on the Entity List.

Is this the end of the ZTE saga? As part of its plea agreement, ZTE still has to cooperate with the US Government in its investigation of third parties that may have violated US export controls and economic sanctions. A summary of the IEEPA, EAR and OFAC violations are included below:

Criminal Violations of IEEPA

ZTE agreed to plead guilty to three criminal charges, including:

1. Conspiracy to unlawfully export, re-export and transship U.S.-origin servers, switches, routers and other components of a cellular network infrastructure to Iran;
2. Obstruction of justice by hiding data regarding its sales to Iran, causing its defense counsel to unwittingly provide false information to the Department of Justice, and deleting all communications related to its cover-up; and
3. Making a materially false statement that it was complying with the laws and regulations of the United States.

The criminal penalties include a fine in the amount of $286,992,532, which represents the largest criminal fine in the history of IEEPA prosecutions, and a criminal forfeiture in the amount of $143,496,266, as well as a conduct remedy discussed below. Because a conduct remedy in a case involving the violation of IEEPA, EAR and OFAC regulations is unusual, a summary of the conduct remedy and its implications is included, below the discussion of ZTE's settlement agreements with the Departments of Commerce and Treasury.

Settlement of Charges with Commerce Department

ZTE also agreed to settle charges with the Commerce Department's Bureau of Industry and Security ("BIS") of 380 violations of the EAR, including (1) Conspiracy (2) Acting with Knowledge of a violation in Connection with Unlicensed Shipments of Telecommunications Items to North Korea via China and (3) Evasion. As part of the settlement:

1. ZTE agreed to pay a penalty of $661 million to BIS, with $300 million suspended during a seven-year probationary period to deter future violations. This is the largest civil penalty ever imposed by BIS.
2. ZTE agreed to active audit and compliance requirements designed to prevent and detect future violations.
3. ZTE agreed to a seven-year suspended denial of export privileges, which could be activated by BIS if any aspect of this deal is not met.

Settlement of Charges with Treasury Department

OFAC administers a comprehensive embargo on Iran as set forth in the Iranian Transactions and Sanctions Regulations ("ITSR"; 31 CFR part 560), including prohibitions on the indirect supply of goods from the United States to Iran, the re-exportation of U.S.-origin goods with knowledge that those items are intended for Iran, and any activity designed to evade or cause a violation of the ITSR. OFAC identified at least 251 ZTE transactions that violated these prohibitions.

ZTE ultimately settled with OFAC for $100,871,266, which was 95% of the maximum statutory civil penalty. As a condition to settlement, ZTE agrees that it has terminated all conduct leading to the apparent violations and will maintain internal policies and procedures that are designed to minimize the risk of future occurrences. Should ZTE willfully violate this condition, the settlement can become null and void, subjecting ZTE to additional OFAC enforcement activity.

Key takeaways for U.S. companies include the need to identify red flags when a customer refuses to disclose the ultimate destination of goods and when a customer involves an unknown intermediary without an adequate explanation.

Conduct Remedy

The conduct remedy imposed on ZTE includes some of the elements addressed in the recently updated BIS *Export Compliance Guidelines – The Elements of an Effective Compliance Program* and elements that are above and beyond the guidelines. In addition, ZTE's press release regarding the Settlement includes additional compliance elements that the company implemented in its effort to implement an improved export compliance program. The standard elements of a compliance program that are addressed in the conduct remedy are:

1. Issuance of a statement of corporate policy of export control compliance from the chief executive officers of ZTE Corporation and ZTE Kangxun to ensure compliance with the EAR which will be distributed no less than annually to all relevant employees of ZTE Corporation and ZTE Kangxun and their subsidiaries and affiliates.
2. Implementation of a training program on applicable export control requirements to be provided to (a) its leadership, management, and employees and (b) the leadership, management and employees of its affiliates, subsidiaries, and other entities worldwide over which it has ownership or control.
3. Record retention as required by the EAR.

The elements that are above and beyond the BIS guidelines are:

- Submission of six annual audit reports regarding export compliance.
- Hiring an initial independent compliance monitor that is approved by the U.S. government for a three-year term. The duties of the monitor include preparing the initial three annual audit reports.
- Hiring an independent compliance auditor, also approved by the U.S. government, for an additional three years to prepare the remaining three annual audit reports.
- The audit reports must include a certification to BIS, executed under penalty of perjury, from the chief executive officer and chief legal officer of ZTE that to the best of their knowledge, after reasonable inquiry, ZTE and its subsidiaries and affiliates are in compliance with the terms of the Agreement including the compliance program obligations.

- An affirmative duty to report potentially unlawful transactions to the U.S. government during the probationary period.
- A requirement to meet at least annually with BIS to discuss any suggestions, comments or proposals for improvement ZTE may wish to discuss with BIS.
- A requirement to provide copies of training materials, the training schedule and training locations to BIS on a quarterly basis until January 1, 2020.

In its press release, ZTE noted that it has:

- Appointed a new Chairman and Chief Executive Officer and made major changes to the senior management team, all of whom have a mandate of leading a new ZTE with a best-in-class export compliance program.
- Created a Chief Executive Officer-led Compliance Committee with the authority and remit to significantly change the company's policies and procedures, and provide greater oversight of support for the compliance initiatives.
- Hired a new Chief Export Compliance Officer with responsibility for overseeing the continued development and improvement of the global export compliance program.
- Created a separate compliance department with increased headcount to build the compliance program with full independence.
- Issued a new Export Control Compliance Manual created in conjunction with the review of BIS to provide more detailed guidance to the employees. ZTE also now requires an annual Compliance Commitment Agreement from all employees.
- Implemented a software automation tool which screens shipments from ZTE Corporation and certain subsidiaries for export control obligations. The system is used to determine which items are subject to the Export Administration Regulations, provides embargo and restricted party screening on the transactions, and places shipments on hold that require detailed classification analysis, application of license exceptions, or application of licenses when necessary.

Florida Firm Fined $27 Million for Export Violations

BIS announced that it has reached a $27 million civil settlement with Access USA Shipping, LLC, of Sarasota, Florida, to settle allegations that it committed violations of the Export Administration Regulations during April 21, 2011 through January 7, 2013. Access USA settled 129 counts of evasion, 17 counts of exporting or attempting to export crime control items without the required license, and 4 counts of exporting or attempting to export to a sanctioned entity on the BIS Entity List without the required license. $17 million dollars of the penalty was suspended for a two-year probationary period. They illegally shipped rifle scopes, night vision lenses, weapons parts, and EAR99 items.

Access USA, a Florida-based mail and package forwarding company, provided foreign customers with a US physical address and a "suite" – designated space at its warehouse facilities – for items purchased from United States merchants that were ultimately intended for export. Customers could have such items, which included rifle scopes, night vision lenses, weapons parts, and EAR99 items, delivered to Access USA's Florida facilities while concealing from those merchants the fact that the items were destined for export, thus avoiding the necessary scrutiny.

Item descriptions were altered and merchant invoices removed in order to avoid detection by the U.S. Government and law enforcement. Access USA thereafter exported those items without regard for its export control and compliance obligations, including its recordkeeping obligations, and without regard for the lawfulness of the shipment, the accuracy of the information conveyed to customs and law enforcement authorities, or the need to first obtain a license where one was necessary. Access USA routinely undervalued, misrepresented, and evaded regulatory requirements for items intended for export using multiple different schemes.

IPSA International Services, Inc. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations

IPSA International Services, Inc., of Phoenix, Arizona, has agreed to pay $259,200 to settle its potential civil liability for 72 apparent violations of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560. The apparent violations involve, on 44 separate occasions, IPSA's importation of Iranian-origin services into the United States in apparent violation of § 560.201 of the ITSR, and on 28 separate occasions, IPSA's engagement in transactions or dealings related to Iranian-origin services by approving and facilitating its foreign subsidiaries' payments to providers of Iranian-origin services in apparent violation of §§ 560.206 and 560.208 of the ITSR.

OFAC determined that IPSA did not voluntarily disclose the apparent violations, and that the apparent violations constitute a non-egregious case. The total transaction value of the apparent violations was $290,784. The statutory maximum civil penalty amount in this case was $18,000,000, and the base civil penalty amount was $720,000.

IPSA is a global business investigative and regulatory risk mitigation firm that provides due diligence services for various countries and their citizenship by investment programs. In March 2012, IPSA entered into an engagement letter and fee agreement with a third country with respect to its citizenship by investment program (Contract No. 1). In October 2012, IPSA's subsidiary in Vancouver, Canada (IPSA Canada) entered into a similar contract with a government-owned financial institution in a separate third country (Contract No. 2). While the majority of the applicants to both of these programs were nationals from countries not subject to OFAC sanctions, some were Iranian nationals. Since most of the information about Iranian applicants could not be checked or verified by sources outside Iran, IPSA Canada and IPSA's subsidiary in Dubai, United Arab Emirates subsequently hired subcontractors to conduct the necessary due diligence in Iran, and those subcontractors in turn hired third parties to validate information that could only be obtained or verified within Iran. Although it was IPSA's foreign subsidiaries that managed and performed both Contract No. 1 and Contract No. 2, with regard to Contract No. 1, IPSA appears to have imported Iranian-origin services into the United States because the foreign subsidiaries conducted the due diligence in Iran on behalf of and for the benefit of IPSA. With regard to Contract No. 2, IPSA also appears to have engaged in transactions or dealings related to Iranian-origin services and facilitated the foreign subsidiaries' engagement in such transactions or dealings because IPSA reviewed, approved, and initiated the foreign subsidiaries' payments to providers of the Iranian-origin services.

COSL Singapore Ltd Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations

COSL Singapore Ltd (COSL Singapore), an oilfield services company located in Singapore and a subsidiary of China Oilfield Service Limited, has agreed to pay $415,350 to settle its potential civil liability for 55 apparent violations of the ITSR. The apparent violations of §§ 560.203 and 560.204 of the ITSR occurred between the approximate dates of October 7, 2011 and February 20, 2013 when COSL Singapore, through its subsidiary companies COSL Drilling Pan-Pacific (Labuan) Ltd and COSL Drilling Pan-Pacific Ltd, exported or attempted to export 55 orders of oil rig supplies from the United States to Singapore and the United Arab Emirates, and then re-exported or attempted to re-export these supplies to four separate oil rigs located in Iranian territorial waters. The transactional value of the 55 orders is $524,664.

COSL Singapore has several oil rigs in its fleet and enters into time charter agreements with third-party drilling companies to allow the third-party drilling companies to use the oil rigs for their drilling operations for a specified term and within a specified territory. COSL Singapore provides the oil rig and oil rig crews to the third-party drilling companies and is responsible for maintaining the oil rig, including by procuring equipment and spare parts for the oil rig's operations. Procurement specialists located in Singapore or assigned to an oil rig's base of operations are responsible for the day-to-day procurement and purchase orders associated with routine maintenance of the oil rigs, including initiating requests for quotation, obtaining quotations, and issuing purchase orders. The procurement specialists purchased at least 55 orders of supplies from vendors located in the United States on behalf of, and that were specifically intended for shipment and/or re-export to, four COSL Singapore oil rigs located and operating in Iranian territorial waters between October 2011 and February 2013. Although some of the purchase order quotations the COSL Singapore procurement specialists received from U.S. vendors included specific language warning that any such goods could not be shipped or re-exported to countries subject to U.S. economic sanctions, specifically including Iran, the company purchased the goods and shipped them to the oil rigs over a period of several years.

OFAC determined that COSL Singapore did not voluntarily disclose the apparent violations and that the apparent violations constitute a non-egregious case. The statutory maximum penalty amount for the apparent violations is $13,750,000, and the base penalty amount for the apparent violations is $923,000.

American Export Lines Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations

Blue Sky Blue Sea, Inc., doing business as American Export Lines and International Shipping Company (USA) (collectively referred to hereafter as AEL), of Los Angeles, California, has agreed to pay $518,063 to settle potential civil liability for 140 apparent violations of the ITSR. Specifically, from on or about April 25, 2010 to on or about June 2, 2012, AEL appears to have violated § 560.204 of the ITSR by transshipping used and junked cars and parts from the United States via Iran to Afghanistan on 140 occasions.

OFAC determined that AEL did not voluntarily self-disclose the apparent violations to OFAC, and that the apparent violations constitute a non-egregious case. The maximum statutory civil monetary penalty amount for the apparent violations was $35,000,000, and the base civil monetary penalty amount was $1,535,000.

Narender Sharma and Hydel Engineering Products of Rampur Bushahr, India, to Pay $100,000 to Settle Alleged Export Violations

Beginning no later than in or around May 2009, and continuing through in or around January 2012, Hydel/Sharma conspired and acted in concert with others, known and unknown, to violate the Regulations and to bring about an act or acts that constitutes a violation of the Regulations. The purpose of the conspiracy was to evade the long-standing and well-known U.S. embargo against Iran in order to sell and export U.S.-origin waterway barrier debris systems and related components to Iran via transshipment through third countries, including to Mahab Ghodss, an Iranian Government entity, without the required U.S. Government authorization.

The conspiracy led to the attempted export of a waterway barrier debris system, an item subject to the Regulations, designated EAR99, and valued at $420,256, from the United States to Mahab Ghodss in Iran, via transshipment through the United Arab Emirates. This item also was subject to the Iranian Transactions Regulations, administered by OFAC.

CSE Global Limited and CSE TransTel Pte. Ltd. Settle Potential Civil Liability for Apparent Violations of the IEEPA

CSE TransTel Pte. Ltd. (TransTel), a wholly-owned subsidiary of the international technology group CSE Global Limited (CSE Global), both of which are located in Singapore, has agreed to pay $12,027,066 to settle its potential civil liability for 104 apparent violations of the International Emergency Economic Powers Act and the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560. Specifically, from on or about June 4, 2012 to on or about March 27, 2013, TransTel appears to have violated § 1705 (a) of IEEPA and § 560.203 of the ITSR by causing at least six separate financial institutions to engage in the unauthorized exportation or re-exportation of financial services from the United States to Iran, a prohibition of § 560.204 of the ITSR.

Between August 25, 2010 and November 5, 2011, TransTel entered into contracts with, and received purchase orders from, multiple Iranian companies to deliver and install telecommunications equipment for several energy projects in Iran and/or Iranian territorial waters. TransTel hired and engaged a number of different third-party vendors – including several Iranian companies – to provide goods and services on its behalf in connection with the above-referenced contracts and purchase orders.

Prior and subsequent to entering into the above-referenced contracts, CSE Global and TransTel separately maintained individual U.S. Dollar (USD) and Singaporean Dollar accounts with a non-U.S. financial institution located in Singapore. In a letter entitled “Sanctions – Letter of Undertaking,” dated April 20, 2012 and signed by TransTel’s then-Managing Director and CSE Global’s then-Group Chief Executive Officer, TransTel made the

following statement to the Bank: "In consideration of [the Bank] agreeing to continue providing banking services in Singapore to our company, we, CSE TransTel Pte. Ltd … hereby undertake not to route any transactions related to Iran through [the Bank], whether in Singapore or elsewhere." TransTel continued to receive banking services from the Bank after execution and delivery of its Letter of Undertaking.

Despite the written attestation that TransTel and CSE Global provided to the Bank, TransTel appears to have begun originating USD funds transfers from its USD-denominated account with the Bank that were related to its Iranian business beginning no later than June 2012 – less than two months after TransTel's and CSE Global's management signed and submitted the Letter of Undertaking.

From on or about June 4, 2012 to on or about March 27, 2013, TransTel appears to have violated § 1705 (a) of IEEPA and/or § 560.203 of the ITSR when it originated 104 USD wire transfers totaling more than $11,111,000 involving Iran. TransTel initiated the wire transfers from its account with the Bank. The transactions were destined for multiple third-party vendors (including several Iranian parties) that supplied goods or services to or for the above-referenced energy projects in Iran, and all of the funds transfers were processed through the United States. None of the transactions contained references to Iran, the Iranian projects, or any Iranian parties.

OFAC Assesses a Civil Monetary Penalty Against ExxonMobil Corporation

OFAC has assessed a $2,000,000 civil monetary penalty against ExxonMobil Corp. of Irving, Texas, including its U.S. subsidiaries ExxonMobil Development Co. and ExxonMobil Oil Corp., for violations of § 589.201 of the Ukraine-Related Sanctions Regulations, 31 C.F.R. part 589. Between on or about May 14, 2014 and on or about May 23, 2014, ExxonMobil violated § 589.201 of the Ukraine-Related Sanctions Regulations when the presidents of its U.S. subsidiaries dealt in services of an individual whose property and interests in property were blocked, namely, by signing eight legal documents related to oil and gas projects in Russia with Igor Sechin, the President of Rosneft OAO, and an individual identified on OFAC's List of Specially Designated Nationals and Blocked Persons. OFAC determined that ExxonMobil did not voluntarily self-disclose the violations to OFAC, and that the violations constitute an egregious case.

Indian Company Settles with OFAC under Iranian Sanctions

Aban Offshore Limited (Aban), of Chennai, India, has agreed to pay $17,500 to settle potential civil liability for an apparent violation of the ITSR. The apparent violation of § 560.204 of the ITSR occurred on the approximate date of June 27, 2008, when Aban's Singapore subsidiary placed an order for oil rig supplies from a vendor in the United States with the intended purpose of re-exporting these supplies from the United Arab Emirates to a jack-up oil drilling rig located in the South Pars Gas Fields in Iranian territorial waters. The transactional value of the order was $10,127.

Alliance for Responsible Cuba Policy Foundation Settles with OFAC under Cuban Sanctions

An individual acting in his personal capacity (the Individual), as well as the Alliance for Responsible Cuba Policy Foundation (the Alliance), on whose behalf the Individual also acted, have agreed to a settlement whereby the Alliance has agreed to pay $10,000 to settle potential civil liability for alleged violations of the Cuban Assets Control Regulations, 31 C.F.R. Part 515 (CACR). OFAC alleged that the Individual violated § 515.201 of the CACR by engaging in unauthorized travel-related transactions during business travel to Cuba from on or about August 23, 2010 to on or about August 27, 2010, and separately from on or about September 8, 2011 to on or about September 11, 2011; and that the Individual violated § 515.201 of the CACR by providing unauthorized travel services related to the two aforementioned trips to a total of 20 persons.

OFAC concluded that the Alleged Violations were frequently undertaken while the Individual held himself out as an officer of the Alliance. OFAC determined that the Alleged Violations were not voluntarily

self-disclosed to OFAC. The statutory maximum civil monetary penalty amount for the Alleged Violations was $1,430,000, and the base penalty amount for the Alleged Violations was $80,000.

Toronto Bank Settles with OFAC under Sanctions Programs

Toronto-Dominion Bank (TD Bank), a financial institution headquartered in Toronto, Canada, has agreed to remit $516,105 to settle its potential civil liability for 167 apparent violations of § 515.201 of the CACR and § 560.204 of ITSR. Separately, the U.S. Department of the Treasury's Office of Foreign Assets Control has issued a Finding of Violation to TD Bank, the parent company of wholly owned subsidiaries Internaxx Bank SA (Internaxx) and TD Waterhouse Investment Services (Europe) Limited (TDWIS), for 3,491 violations of the CACR and ITSR.

Beginning as early as 2003 or 2004, TD Bank's Global Trade Finance business, based in Montreal, Canada engaged in a series of trade finance transactions that appear to have implicated the sanctions regulations administered by OFAC. These transactions generally involved import-export letters of credit for TD Bank's Canadian customers that the bank failed to screen for any potential nexus to an OFAC-sanctioned country or entity prior to processing related transactions through the U.S. financial system. For a number of years, up to and including 2011, TD Bank maintained several accounts for, and processed transactions to or through the United States on behalf of, a Canadian company owned by a Cuban company. TD Bank had reason to know about the customer's connections to Cuba through the company's ownership and business, as well as actual knowledge on the part of several TD Bank employees and business lines as early as 2005 and 2006. Pursuant to this fact pattern, between August 14, 2007 and April 22, 2011, TD Bank processed 29 transactions totaling $1,156,181.37 to or through the United States in apparent violation of the Cuban Assets Control Regulations, 31 C.F.R. Part 515.

TD Bank also maintained several accounts in Canada for a company that the bank described as "a freight, cargo and shipping business, based in Canada, that is, among other things, a transporter of oil and gas related equipment . . . [that ships its products] to destinations in the Middle East." According to a document available to TD Bank, the customer was listed as a sales agent for an entity on OFAC's List of Specially Designated Nationals and Blocked Persons and located in Iran. Between December 1, 2008 and March 28, 2012, TD Bank processed 39 transactions totaling $515,071.20 to or through the United States on behalf of this customer in apparent violation of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560.

Separately, TD Bank maintained accounts on behalf of 62 customers who were Cuban nationals residing in Canada.1 Between August 7, 2007 and January 24, 2011, TD Bank processed 99 transactions totaling $459,341.62 to or through the United States on behalf of these customers in apparent violation of the CACR. The conduct that led to the Apparent Violations involved multiple business units throughout the TD Bank network outside of the United States – including at times supervisory or management personnel – that had reason to know or actual knowledge of information regarding these customers' connections to OFAC-sanctioned jurisdictions or parties. In general, the Apparent Violations appear to have occurred due to shortcomings in the bank's OFAC compliance policies, procedures, and program.

OFAC Issues a Finding of Violation to B Whale Corporation

OFAC has issued a Finding of Violation to B Whale Corporation (BWC), a company based in Taipei, Taiwan and a member of the TMT Group of shipping companies (TMT), for a violation of the ITSR. Between on or about August 30, 2013 and on or about September 2, 2013, BWC violated §§ 560.201 and 560.211 of the ITSR when its vessel, the M/V B Whale, conducted a ship-to-ship transfer with, and received 2,086,486 barrels of condensate crude oil from, the vessel M/T Nainital, a vessel owned by the National Iranian Tanker Company and identified on OFAC's List of Specially Designated Nationals and Blocked Persons at the time the transaction occurred.

The transactions described above occurred after BWC entered into bankruptcy proceedings in the U.S. Bankruptcy Court for the Southern District of Texas on June 20, 2013. OFAC determined that BWC was a U.S. person within the scope of the ITSR because it was present in the United States for the bankruptcy proceedings when the transaction occurred. Additionally, the vessel M/V B Whale was subject to U.S. sanctions regulations because it was

property under the jurisdiction of a U.S. bankruptcy court, and therefore the oil transferred to the vessel was an importation from Iran to the United States as defined in the ITSR.

OFAC Posts Settlement Agreement with United Medical Instruments, Inc.

OFAC announced a $515,400 settlement with United Medical Instruments, Inc. (UMI), a company incorporated in California. UMI agreed to settle its potential civil liability for 56 alleged violations of the Iranian Transactions and Sanctions Regulations. The alleged violations occurred between 2007 and 2009 when UMI made sales of medical imaging equipment with knowledge or reason to know that the goods were intended specifically for supply or re-exportation to buyers located in Iran, and when it facilitated the sales of medical imaging equipment from a company located in the United Arab Emirates to Iran. OFAC determined that UMI did not voluntarily self-disclose the apparent violations to OFAC, and that the alleged violations constitute a non-egregious case.

Updates to the 2014 Epsilon Electronics Case and Reexport Due Diligence

In July 2014, Epsilon Electronics Inc., Montebello, California, also doing business as Power Acoustik Electronics, Sound Stream, Kole Audio, and Precision Audio, was assessed a penalty of $4,073,000 for violations of the Iranian Transactions and Sanctions Regulations. From on or about August 26, 2008, to on or about May 22, 2012, Epsilon violated § 560.204 of the ITSR when it issued 39 invoices for car audio and video equipment, valued at $3,407,491, which was shipped to a company that reexports most, if not all, of its products to Iran and has offices in Tehran, Iran, and Dubai, the U.A.E. Epsilon knew or had reason to know that such goods were intended specifically for supply, transshipment, or reexportation, directly or indirectly to Iran. In addition, Epsilon issued five of these invoices after it received a cautionary letter from OFAC in January 2012. The cautionary letter explained that the ITSR generally prohibited the unauthorized exportation, reexportation, sale or supply of goods, technology, or services to Iran.

Epsilon appealed the decision and argued, among other things, that OFAC's 2002 "Guidance on Transshipments to Iran" creates an exception to ITSR § 560.204 that allows US persons to export goods (that are not controlled under the US Export Administration Regulations) to distributors for their general inventory, even if the distributors later re-export the goods to Iran, provided the US exports were not specifically intended for re-export to Iran and/or the distributor's sales were not predominantly to Iran.

In March 2016, the District Court granted summary judgement in favor of OFAC, rejecting Epsilon's argument, and holding that OFAC had sufficient evidence that Epsilon had reason to know that Asra intended to ship the goods to Iran given that Asra's dealings at the time were primarily in Iran.

The main takeaway from this decision is the U.S exporters must conduct adequate due diligence into their export transactions, and look for "red flags" that the exports are intended for, or are likely to be reexport to a country in violation of U.S. export controls. The red flags could be from publicly available information that is available, such as information on a website (as in the Epsilon case), even if the U.S. person does not review this information.

American Honda Finance Corporation Settles 13 Alleged Cuba Violations

American Honda Finance Corporation (AHFC), a motor vehicle finance company headquartered in California that specializes in various forms of financing in the United States for purchasers, lessees, and authorized independent dealers of Honda and Acura products, has agreed to remit $87,255 to settle its potential civil liability for 13 apparent violations of the Cuban Assets Control Regulations.

Between February 2011 and March 2014, Honda Canada Finance, Inc. (HCFI), a majority-owned subsidiary of AHFC located in Canada, approved and financed 13 lease agreements between an unaffiliated Honda dealership in Ottawa, Canada and the Embassy of Cuba in connection with the Cuban Embassy's leasing of several Honda vehicles. The Cuban entity had the word "Cuba" in its name and provided documentation to HCFI demonstrating it was a Government of Cuba entity. Although AHFC and HCFI had policies and procedures in place to review transactions against OFAC's List of Specially Designated Nationals and Blocked Persons for compliance with U.S.

economic sanctions laws, they did not include the names of countries subject to OFAC-administered comprehensive sanctions in their screening system. AHFC and HCFI were not involved in the business of exporting vehicles internationally.

Overall, between February 28, 2011 and March 3, 2014, HCFI approved the financing of 13 lease agreements with the Cuban entity totaling $276,999. Three of the lease agreements, totaling $58,281, were initiated and/or approved by HCFI on or about March 3, 2014, approximately two months after AHFC submitted its initial voluntary self-disclosure to OFAC regarding similar apparent violations. The total base penalty amount for the 13 Alleged Violations was $138,500.

American International Group, Inc. Settles Potential Liability for Apparent Violations of Multiple Sanctions Programs

American International Group, Inc. (AIG) of New York, NY, an international insurance and financial services organization incorporated in Delaware and headquartered in New York, has agreed to remit $148,698 to settle its potential civil liability for 555 apparent violations of the following OFAC sanctions programs: ITSR; the Weapons of Mass Destruction Proliferators Sanctions Regulations, 31 C.F.R. Part 544 (WMDPSR); the Sudanese Sanctions Regulations, 31 C.F.R. Part 538 (SSR); and the CACR.

From on or about November 20, 2007, to on or about September 3, 2012, AIG engaged in a total of 555 transactions totaling approximately $396,530 in premiums and claims for the insurance of maritime shipments of various goods and materials destined for, or that transited through, Iran, Sudan, or Cuba, and/or that involved a blocked person. While most of the Apparent Violations occurred under global insurance policies, dozens of apparent violations occurred under single shipment policies. OFAC identified 455 apparent violations totaling $274,463.64 in which AIG extended insurance coverage to parties that were engaging in a voyage, shipment, or transshipment to, from, or through Iran, and/or accepted premium payments or paid claims arising from that insurance coverage, in apparent violation of § 560.204 of ITSR.

In addition, OFAC identified 38 apparent violations of § 538.205 of the SSR, all of which pertained to global insurance policies that provided insurance coverage for shipments going to or from Sudan, with premiums received totaling $13,321.44. Moreover, OFAC identified 33 apparent violations of § 544.201 of the WMDPSR, all of which involved shipments aboard blocked Islamic Republic of Iran Shipping Lines vessels, with premiums received totaling $105,065.94. Finally, OFAC identified 29 apparent violations of § 515.201 of the CACR, all of which pertained to AIG's provision of insurance coverage in connection with shipments to or from Cuba, or its processing of premiums or claims arising from this coverage or that involved a Cuban entity, with premiums received totaling $3,679.

Chinese National Pleads Guilty To Economic Espionage and Theft of a Trade Secret from U.S. Company

Xu Jiaqiang pled guilty to economic espionage and theft of a trade secret, in connection with Xu's theft of proprietary source code from Xu's former employer, with the intent to benefit the National Health and Family Planning Commission of the People's Republic of China. Xu pled guilty earlier today to all six counts with which he was charged.

According to the compliance and indictment, from November 2010 to May 2014, Xu worked as a developer for a particular U.S. company (Victim Company). As a developer, Xu enjoyed access to certain proprietary software (Proprietary Software), as well as that software's underlying source code (Proprietary Source Code). The Proprietary Software is a clustered file system developed and marketed by the Victim Company in the United States and other countries. A clustered file system facilitates faster computer performance by coordinating work among multiple servers. The Victim Company takes significant precautions to protect the Proprietary Source Code as a trade secret. Among other things, the Proprietary Source Code is stored behind a company firewall and can be accessed only by a small subset of the Victim Company's employees. Before receiving Proprietary Source Code access, Victim Company employees must first request and receive approval from a particular Victim Company official. Victim Company employees must also agree in writing at both the outset and the conclusion of their employment that they

will maintain the confidentiality of any proprietary information. The Victim Company takes these and other precautions in part because the Proprietary Software and the Proprietary Source Code are economically valuable, which value depends in part on the Proprietary Source Code's secrecy.

In May 2014, Xu voluntarily resigned from the Victim Company. Xu subsequently communicated with one undercover law enforcement officer (UC-1), who posed as a financial investor aiming to start a large-data storage technology company, and another undercover law enforcement officer (UC-2), who posed as a project manager, working for UC-1. During these communications, Xu discussed his past experience with the Victim Company and indicated that he had experience with the Proprietary Software and the Proprietary Source Code. On March 6, 2015, Xu sent UC-1 and UC-2 a code, which Xu stated was a sample of Xu's prior work with the Victim Company. A Victim Company employee (Employee-1) later confirmed that the code sent by Xu included proprietary Victim Company material that related to the Proprietary Source Code.

Xu subsequently informed UC-2 that Xu was willing to consider providing UC-2's company with the Proprietary Source Code as a platform for UC-2's company to facilitate the development of its own data storage system. Xu informed UC-2 that if UC-2 set up several computers as a small network, then Xu would remotely install the Proprietary Software so that UC-1 and UC-2 could test it and confirm its functionality.

In or around early August 2015, the FBI arranged for a computer network to be set up, consistent with Xu's specifications. Files were then remotely uploaded to the FBI-arranged computer network (Xu Upload). Thereafter, on or about August 26, 2015, Xu and UC-2 confirmed that UC-2 had received the Xu Upload. In September 2015, the FBI made the Xu Upload available to a Victim Company employee who has expertise regarding the Proprietary Software and the Proprietary Source Code (Employee-2). Based on Employee-2's analysis of technical features of the Xu Upload, it appeared to Employee-2 that the Xu Upload contained a functioning copy of the Proprietary Software. It further appeared to Employee-2 that the Xu Upload had been built by someone with access to the Proprietary Source Code who was not working within the Victim Company or otherwise at the Victim Company's direction.

On December 7, 2015, Xu met with UC-2 at a hotel in White Plains, New York (Hotel). Xu stated, in sum and substance, that Xu had used the Proprietary Source Code to make software to sell to customers, that Xu knew the Proprietary Source Code to be the product of decades of work on the part of the Victim Company, and that Xu had used the Proprietary Source Code to build a copy of the Proprietary Software, which Xu had uploaded and installed on the UC Network (i.e., the Xu Upload). Xu also indicated that Xu knew the copy of the Proprietary Software that Xu had installed on the UC Network contained information identifying the Proprietary Software as the Victim Company's property, which could reveal the fact that the Proprietary Software had been built with the Proprietary Source Code without the Victim Company's authorization. Xu told UC-2 that Xu could take steps to prevent detection of the Proprietary Software's origins – i.e., that it had been built with stolen Proprietary Source Code – including writing computer scripts that would modify the Proprietary Source Code to conceal its origins.

Later on December 7, 2015, Xu met with UC-1 and UC-2 at the Hotel. During that meeting, Xu showed UC-2 a copy of what Xu represented to be the Proprietary Source Code on Xu's laptop. Xu noted to UC-2 a portion of the code that indicated it originated with the Victim Company as well as the date on which it had been copyrighted. Xu also stated that XU had previously modified the Proprietary Source Code's command interface to conceal the fact that the Proprietary Source Code originated with the Victim Company and identified multiple specific customers to whom Xu had previously provided the Proprietary Software using Xu's stolen copy of the Proprietary Source Code.

Pennsylvania Man Indicted For Export Violations and Unlawful Possession of Ammunition

The United States Attorney's Office for the Middle District of Pennsylvania announced today that Mark Komoroski, age 54, of Nanticoke, Pennsylvania, was indicted on May 10, 2017, for violating federal export laws and unlawfully possessing ammunition as a previously convicted felon. The indictment was unsealed on May 11, 2017, following Komoroski's arrest and initial appearance before United States Magistrate Judge Karoline Mehalchick.

According to United States Attorney Bruce D. Brandler, the indictment alleges that in February and March of 2016, Komoroski attempted to export two riflescopes to an individual in Russia without first obtaining the export licenses required by federal law. The indictment also alleges that Komoroski, a previously convicted felon, possessed over 25,000 rounds of ammunition.

Czech Republic and Slovak Republic Nationals Charged with Violating U.S. Export Laws

The indictments allege that:

- Between June 2011 and November 2011, Josef Zirnsak, of the Czech Republic, shipped from the U.S. to Germany an infrared dual beam aiming laser and a rifle scope, both of which are designated as defense articles on the U.S. Munitions List.
- Between May 2012 and June 2012, Martin Gula, also known as "Mark Welder," of the Slovak Republic, purchased and attempted to arrange the export of night vision goggles and an aviator night vision system from the U.S. to the United Kingdom. The indictment also alleges that, during the same time period, Gula used a false U.S. passport as proof of residency and citizenship in the U.S.

Zirnsak and Gula are each charged with two counts of violating the Arms Export Control Act, an offense that carries a maximum term of imprisonment of 20 years on each count GULA also is charged with two counts of export smuggling and one count of use of a false passport, offenses that carry a maximum term of imprisonment of 10 years on each count.

Defense Contractor Employee Pleads Guilty to Selling Satellite Secrets to Undercover Agent Posing as Russian Spy

Gregory Allen Justice, of Culver City, California, pleaded guilty to federal charges of one count of attempting to commit economic espionage and one count of attempting to violate the Arms Export Control Act. The charges are related to Justice's selling sensitive satellite information to a person he believed to be an agent of a Russian intelligence service. Justice was an engineer who worked for a cleared defense contractor. Specifically, he worked on military and commercial satellite programs.

According to a plea agreement filed in this case, Justice stole proprietary trade secrets from his employer and provided them to a person he believed to be a Russian agent – but who in fact was an undercover FBI employee. In addition to their proprietary nature, the documents contained technical data covered by the U.S. Munitions List and therefore were subject to controls restricting export from the U.S. under the International Traffic in Arms Regulations.

In exchange for providing these materials during a series of meeting between February and July of 2016, Justice sought and received thousands of dollars in cash payments. During one meeting, Justice and the undercover agent discussed developing a relationship like one depicted on the television show "The Americans," and during their final meeting, Justice offered to take the undercover agent on a tour of his employer's production facilities where Justice said all military spacecraft were built, according to the plea agreement.

Seven People Charged With Conspiring to Steal Trade Secrets for Benefit of Chinese Manufacturing Company

Seven people are charged in the U.S. District Court for the District of Columbia with conspiracy to commit theft of trade secrets. The government also filed a related civil forfeiture complaint in the District of Columbia for two pieces of real property which were involved in, and are traceable to, the alleged illegal conduct. Those arrested and charged include four U.S. citizens: Shan Shi, 52, of Houston, Texas; Uka Kalu Uche, 35, of Spring, Texas; Samuel Abotar Ogoe, 74, of Missouri City, Texas; and Johnny Wade Randall, 48, of Conroe, Texas. Also charged were Kui Bo, 40, a Canadian citizen who has been residing in Houston, and Gang Liu, 31, a Chinese national who has been residing in Houston as a permanent resident. Additionally, charges were filed against one Chinese national living in

China, Hui Huang, 32, an employee of the Chinese manufacturing firm allegedly involved in tasking employees of the Houston company.

According to an affidavit filed in support of the criminal complaint, the trade secrets were stolen in order to benefit a manufacturer located in China; this manufacturer was the only shareholder for a company that had been incorporated in Houston. Between in or about 2012 and the present, the affidavit alleges that the Chinese manufacturer and employees of its Houston-based company engaged in a systematic campaign to steal the trade secrets of a global engineering firm, referred to in the affidavit as "Company A," that was a leader in marine technology.

The case involves the development of a technical product called syntactic foam, a strong, light material that can be tailored for commercial and military uses, such as oil exploration; aerospace; underwater vehicles, such as submarines; and stealth technology. According to the affidavit, the Chinese manufacturer intended to sell syntactic foam to both military and civilian, state-owned enterprises in China – part of a push toward meeting China's national goals of developing its marine engineering industry.

The affidavit alleges that the conspirators took part in the theft of trade secrets from Company A, a multi-national company with a subsidiary in Houston that is among the major producers of syntactic foam. The affidavit identifies a number of trade secrets allegedly taken from the company between January and June of 2015, including secrets that allegedly were passed to people associated with the Chinese manufacturer and Houston-based company.

Defendant Shi was hired by the Chinese company on a contract basis in March 2014 in order to bring in experts, set up a design team, and push forward marine buoyancy technology. That same month, Shi incorporated the new company in Houston that was owned by the Chinese manufacturer.

The affidavit alleges that defendants Shi and Bo then began to systematically target U.S. employees with experience in the production of syntactic foam. Between late 2014 and early 2015, the new company in Houston hired two former Company A employees, defendants Ogoe and Liu, by offering a combination of cash incentives and high paying positions. Uche, who was at the time a current employee of Company A, provided trade secrets to Ogoe, the affidavit alleges. Defendant Randall, who was at the time a current employee of Company A, allegedly provided at least one stolen trade secret to Ogoe.

Ogoe provided these trade secrets as well as additional information to the company owned by the Chinese manufacturer in Houston shortly after being hired, the affidavit alleges. Liu also provided Company A trade secrets shortly after being hired.

Some of these trade secrets were sent by Shi and Bo and others to defendant Huang, an employee of the manufacturer in China, so that the Chinese manufacturer could create a functional syntactic foam manufacturing facility, the affidavit states.

Los Angeles-area woman arrested on federal charges alleging a scheme to smuggle restricted space communications technology to China

A Pomona woman was arrested on federal charges that accuse her of conspiring to procure and illegally export sensitive space communications technology to her native China. Si Chen, also known as Cathy Chen, was arrested on federal charges that accuse her of conspiring to procure and illegally export sensitive space communications technology to her native China.

The 14-count indictment accuses Chen of violating the International Emergency Economic Powers Act, which controls and restricts the export of certain goods and technology from the United States to foreign nations. Chen is also charged with conspiracy, money laundering, making false statements on an immigration application, and using a forged passport.

According to the indictment, from March 2013 to December 2015, Chen purchased and smuggled sensitive items to China without obtaining licenses from the U.S. Department of Commerce that are required under IEEPA. Those items allegedly included components commonly used in military communications "jammers" from which Chen removed the export-control warning stickers prior to shipping. Additionally, Chen is suspected of smuggling communications devices worth more than $100,000 that are commonly used in space communications applications. On the shipping paperwork Chen falsely valued the items at $500. The indictment further describes how Chen received payments for the illegally exported products through an account held at a bank in China by a family member.

In addition to the export violations, Chen is also charged with employing several aliases and using a forged passport in an effort to conceal her alleged smuggling activities on behalf of unnamed co-conspirators in China. The indictment alleges the defendant used a Chinese passport bearing her photo and a false name – "Chunping Ji" – to rent an office in Pomona where she took delivery of the export-controlled items. After receiving the goods, the indictment alleges Chen shipped the devices to Hong Kong in parcels that bore her false name, along with false product descriptions and monetary values, all done in an effort to avoid attracting law enforcement scrutiny.

Under IEEPA, it is crime to willfully export or attempt to export items that appear on the Commerce Control List without a license from the U.S. Department of Commerce. These are items authorities have determined could be detrimental to regional stability and national security.

Exporter of Microelectronics to Russian Military Sentenced to 135 Months in Prison Following Convictions on All Counts

Alexander Posobilov, 62, of Houston, Texas, was sentenced to 135 months in prison for conspiring to export and illegally exporting controlled microelectronics to Russia, and for conspiring to launder money. Posobilov, as well as ten other individuals and two corporations – ARC Electronics, Inc. (ARC) and Apex System, L.L.C. (Apex) – were indicted in October 2012. Posobilov and two co-conspirators were subsequently convicted at trial on all counts in October 2015. Of the remaining defendants, five pleaded guilty and three remain at large. ARC is now defunct, and Apex, a Russian-based procurement firm, failed to appear in court.

Posobilov joined ARC in 2004, where he ascended to become the procurement manager and day-to-day director of the company. Between approximately October 2008 and October 2012, Posobilov managed a team of employees who worked to obtain advanced, technologically cutting-edge microelectronics from manufacturers and suppliers located within the U.S. and to export those high-tech goods to in Russia, while evading the government licensing system set up to control such exports. These commodities have applications and are frequently used in a wide range of military systems, including radar and surveillance systems, missile guidance systems and detonation triggers. Russia was not capable of producing many of these sophisticated goods domestically. Between 2002 and 2012, ARC shipped approximately $50,000,000 worth of microelectronics and other technologies to Russia. ARC's largest clients were certified suppliers of military equipment for the Russian Ministry of Defense.

To induce manufacturers and suppliers to sell these high-tech goods to ARC, and to evade applicable export controls, Posobilov and his co-conspirators provided false end user information in connection with the purchase of the goods, concealed the fact that they were exporters and falsely classified the goods they exported on export records submitted to the Department of Commerce. Ultimate recipients of ARC's products included a research unit for the Russian FSB internal security agency, a Russian entity that builds air and missile defense systems and another that produces electronic warfare systems for the Russian Ministry of Defense.

Ukrainian National Arrested In Connection With Scheme to Illegally Export Rifle Scopes and Thermal Imaging Equipment

Volodymyr Nedoviz, a lawful permanent resident of the United States and citizen of Ukraine, was arrested on federal charges of illegally exporting controlled military technology from the United States to end-users in Ukraine. Federal agents also executed a search warrant at a Philadelphia, Pennsylvania location that was used in connection with Nedoviz's illegal scheme.

The complaint alleges that the defendant conspired with others located in both Ukraine and the United States to purchase export-controlled, military-grade equipment from sellers in the United States and to export that equipment to Ukraine without the required licenses. The devices obtained by the defendant and his co-conspirators included some of the most highly powerful and technologically sophisticated night vision rifle scopes and thermal imaging equipment available, including, among others, an Armasight Zeus-Pro 640 2-16x50 (60Hz) Thermal Imaging weapons sight, a FLIR Thermosight R-Series, Model RS64 60 mm 640x480 (30Hz) Rifle Scope, and a ATN X-Sight II 5-20x Smart Rifle Scope. In many cases, the devices purchased by the defendant and his co-conspirators retail for almost $9,000, and they are specifically marketed to military and law enforcement consumers.

As part of the conspiracy, in order to induce U.S.-based manufacturers and suppliers to sell them the export-controlled devices and to evade applicable controls, the defendant and his co-conspirators falsely purported to be United States citizens and concealed the fact they were exporters. The defendant and his co-conspirators also recruited, trained, and paid other U.S.-based individuals to export the controlled devices to Ukraine via various freight forwarding companies. Among other things, the defendant and his co-conspirators instructed the U.S.-based individuals to falsely describe the nature and value of the equipment they were attempting to export. In addition, to conceal their identities, as well as the true destination of the rifle scopes and thermal imaging equipment, the defendant and his co-conspirators instructed that the items be shipped using false names and addresses.

The export of military-grade rifle scopes and thermal imaging equipment requires a license from either the United States Department of State or the United States Department of Commerce. Both the Department of State and the Department of Commerce have placed restrictions on the export of items that they have determined could make a significant contribution to the military potential and weapons proliferation of other nations and that could be detrimental to the foreign policy and national security of the United States.

Kansas Man Sentenced to 52 Months for Exporting Firearms to Overseas Purchasers

A Kansas man was sentenced to 52 months in prison for his role in a scheme involving the illegal export of firearms from the United States using a hidden online marketplace. Michael Andrew Ryan previously pleaded guilty to six counts of exporting and attempting to export firearms illegally from the United States to individuals located in other countries on June 6, 2016, and was remanded into custody on Oct. 6, 2016.

In connection with his plea, Ryan admitted that he used the hidden internet marketplace Black Market Reloaded, a website hosted on the Tor network where users can traffic anonymously in illegal drugs and other illegal goods, to unlawfully export or attempt to export firearms from the United States to Cork, Ireland; Mallow, Ireland; Pinner, England; Edinburgh, Scotland; Victoria, Australia. These goods included dozens of firearms, including pistols, revolvers, UZIs and Glocks, some from which the manufacturer's serial numbers had been removed, altered or obliterated, as well as magazines and hundreds of rounds of ammunition.

Long Beach woman pleads guilty to illegally shipping ammunition to the Philippines

A Long Beach woman has pleaded guilty to federal offenses for illegally shipping tens of thousands of rounds of ammunition to the Philippines. Marlou Mendoz pleaded guilty in U.S. District Court to three counts of failing to provide the required written notice to freight forwarders that she was shipping ammunition to a foreign country.

Marlou Medoza admitted she sent .22-caliber ammunition and bullets to the Philippines in three shipments in June 2011. The shipments contained 131,300 rounds, the defendant admitted in court. Marlou Mendoza, who remains free on bond, is scheduled to be sentenced April 20 by U.S. District Judge George H. Wu. As a result of the three guilty pleas, she faces a statutory maximum penalty of 15 years in federal prison.

In a related case unsealed last year, Mark Louie Mendoza, Marlou Mendoza's son, was charged with illegally shipping hundreds of thousands of dollars' worth of firearms parts and ammunition to the Philippines – munitions that were concealed in shipments falsely claimed to be household goods.bMark Mendoza, who remains a fugitive, is

named in an eight-count indictment that charges him with conspiracy, the unlawful export of munitions, smuggling, and money laundering.

Mark Mendoza, who was the president of a "tools and equipments" company known as Last Resort Armaments, ordered more than $100,000 worth of ammunition and firearms accessories, much of which was delivered to his parent's Long Beach residence over a six-month period in 2011. The items Mark Mendoza ordered included parts for M-16 and AR-15-type rifles, and these parts are listed as defense articles on the United States Munitions List. Pursuant to the Arms Export Control Act, items on the Munitions List may not be shipped to the Philippines without an export license issued by the Department of State.

The money laundering charge against Mark Mendoza alleges that during the first six months of 2011, he transferred more than $650,000 in proceeds generated by the illegal ammunition exports from an account in the Philippines to a money remitter in Los Angeles.

"Federal export regulations and laws like the Arms Export Control Act are designed to prevent dangerous materials from reaching the hands of people who may cause harm to the United States, its interests, or its allies," said United States Attorney Eileen M. Decker. "This case involves a significant amount of ammunition destined for the Philippines, and once there the items could have been transported anywhere in the world and used for any purpose. This case exemplifies the importance of stopping the flow of illegally trafficked weapons to foreign nations, and the dedicated efforts of law enforcement to prevent such conduct."

Mark Mendoza is charged with conspiracy, three counts of unlawful export of munitions, three counts of export smuggling and one count of money laundering. If he were to be convicted of all counts in the indictment, Mark Mendoza would face a statutory maximum sentence of 115 years in federal prison.

Production and Development of Nuclear Material for China

On Jan. 6, 2017, in the Eastern District of Tennessee, Szuhsiung Ho, aka Allen Ho, a naturalized U.S. citizen, pleaded guilty to conspiracy to unlawfully engage or participate in the production or development of special nuclear material outside the U.S., without the required authorization from the U.S. Department of Energy (DOE), in violation of the Atomic Energy Act. In Apr. 2016, a federal grand jury issued a two-count indictment against Ho; China General Nuclear Power Company (CGNPC), the largest nuclear power company in China; and Energy Technology International (ETI), a Delaware corporation. At the time of the indictment Ho was a nuclear engineer, employed as a consultant by CGNPC, and was also the owner of ETI. CGNPC specialized in the development and manufacture of nuclear reactors and was controlled by China's State-Owned Assets Supervision and Administration Commission. According to documents filed in the case, beginning in 1997 and continuing through Apr. 2016, Ho conspired with others to engage or participate in the development or production of special nuclear material in China, without specific authorization to do so from the U.S. Secretary of Energy, as required by law. Ho assisted CGNPC in procuring U.S.-based nuclear engineers to assist CGNPC and its subsidiaries with designing and manufacturing certain components for nuclear reactors more quickly by reducing the time and financial costs of research and development of nuclear technology. In particular, Ho sought technical assistance related to CGNPC's Small Modular Reactor Program; CGNPC's Advanced Fuel Assembly Program; CGNPC's Fixed In-Core Detector System; and verification and validation of nuclear reactor-related computer codes. Under the direction of CGNPC, Ho also identified, recruited, and executed contracts with U.S.-based experts from the civil nuclear industry who provided technical assistance related to the development and production of special nuclear material for CGNPC in China. Ho and CGNPC also facilitated travel to China for and payments to the U.S.-based experts in exchange for their services.

Nogales man sentenced to more than 7 years for attempting to export ammunition into Mexico

A Nogales man convicted of attempting to smuggle more than 5,000 rounds of ammunition into Mexico has been sentenced to 92 months in prison, following a probe by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI). Gabriel Rivero, 41, appeared in federal court before U.S. Senior District

Judge Frank R. Zapata. At the sentencing, Judge Zapata ordered that Rivero will be subject to three years of supervised release upon completion of his prison term.

According to evidence presented during Rivero's December 2016 trial, the smuggling attempt came to light in February of last year when a spare tire fell off the pickup truck Rivero was driving near the Mariposa Port of Entry in Nogales. Initially, Rivero attempted to retrieve the tire, but then he got back into the truck and traveled through the border crossing into Mexico. When U.S. Customs and Border Protection officers inspected the tire, they discovered more than 5,500 rounds of pistol and rifle ammunition hidden inside. Rivero was subsequently identified using surveillance video from the port of entry and arrested.

Lebanese Businessman Tied to Hizballah Arrested for Violating IEEPA and Defrauding the U.S. Government

Kassim Tajideen, a prominent financial supporter of the Hizballah terror organization, has been arrested and charged with evading U.S. sanctions imposed on him because of his financial support of Hizballah. Tajideen, 62, of Beirut, Lebanon, was arrested overseas on March 12, 2017, based on an 11-count indictment unsealed today in the U.S. District Court for the District of Columbia following his arrival to the United States. Tajideen made his initial court appearance today before Magistrate Judge Robin M. Meriweather.

According to the indictment, Tajideen allegedly presided over a multi-billion-dollar commodity distribution business that operates primarily in the Middle East and Africa through a web of vertically integrated companies, partnerships and trade names. The indictment further alleges that Tajideen and others engaged in an elaborate scheme to engage in business with U.S. companies while concealing Tajideen's involvement in those transactions.
The Department of the Treasury's Office of Foreign Assets Control named Tajideen a Specially Designated Global Terrorist on May 27, 2009. This designation prohibits U.S. companies from transacting unlicensed business with Tajideen or any companies which are operated for his benefit – in essence stripping Tajideen's global business empire of its ability to legally acquire goods from, or wire money into, the U.S. However, the indictment alleges that Tajideen restructured his business empire after the designation in order to evade the sanctions and continue conducting transactions with U.S. entities. Tajideen and others are alleged to have created new trade names and to have misrepresented his ownership in certain entities in order to conceal Tajideen's association. The scheme allowed Tajideen's companies to continue to illegally transact business directly with unwitting U.S. vendors, as well as to continue utilizing the U.S. financial and freight transportation systems to conduct wire transfers and move shipping containers despite the sanctions against Tajideen.

According to the indictment, between approximately July of 2013 until the present day, the conspirators illegally completed at least 47 individual wire transfers, totaling over approximately $27 million, to parties in the U.S. During the same time period, the conspirators caused dozens of illegal shipments of goods to leave U.S. ports for the benefit of Tajideen, without obtaining the proper licenses from the U.S. Department of the Treasury.

Lebanese Man Convicted of Buying Guns in Lebanon Smuggled from the U.S.

A Lebanese man pleaded guilty in federal court to buying guns in Lebanon that were shipped from Cedar Rapids, Iowa by family members convicted of gun smuggling last year. Fadi Yassine, 42, pleaded to one count of conspiring to violate the Arms Export Control Act — not having a license to export guns.

Yassine was arrested on a warrant when he arrived on an international flight Feb. 6 in New York City, court documents show. Following a federal hearing in Brooklyn, he waived further proceedings in New York and a judge transferred him back to U.S. District Court in Cedar Rapids.

During the plea, Yassine admitted to conspiring with one or more people to broker guns, and shipping and transporting firearms without a license between late 2013 and May 12, 2015.

Court documents show Yassine purchased guns in Lebanon that had been shipped from the United States by Ali Al Herz, 51, his son Adam Al Herz, 23, his brother Bassem Herz, 31, and Bassem's wife, Sarah Zeaiter, 24. A

Homeland Security Investigation special agent reviewed Facebook account records and determined Yassine was advising Bassem Herz on purchasing firearms, court documents show. In the Facebook messages, the two men referenced the fact that a certain Glock model was the newest firearm on the market. Yassine also advised Bassem Herz not to buy Kimber guns or ammunition.

The affidavit also shows Yassine gave $30,000 in cash to Ali Al Herz in Lebanon for him to acquire more guns in the United States. The Al Herz family members were convicted last year for smuggling guns from Iowa to Lebanon and are all serving federal prison terms. Yassine also admitted during the hearing that he knew the purpose was to export firearms to Lebanon.

The initial investigation of the Al Herz family led to the March 2015 seizure of 53 guns and thousands of rounds of ammunition concealed inside Bobcat skid loaders within a shipping container at the Norfolk, Virginia, seaport bound for Lebanon. A subsequent investigation led to the May 2015 seizure of a second shipping container, loaded at Midamar Corp. in Cedar Rapids, also destined for Lebanon, with 99 guns and ammunition concealed inside skid loaders.

Evidence presented during hearings showed the containers were bound for southern Lebanon, which is controlled by Hezbollah, a terrorist organization. But the evidence showed none of the family was part of the terrorist group. Prosecutors said the motive for the crime was greed, as the guns could be sold for 10 times their value in Lebanon than in the United States.

Connecticut Business Owner Pleads Guilty to Export Violation

Imran Khan pleaded guilty in federal court to violating U.S. export control laws. According to court documents and statements made in court, from at least 2012 to December 2016, Khan and others were engaged in a scheme to purchase goods that were controlled under the Export Administration Regulations and export those goods without a license to Pakistan, in violation of the EAR. Khan conducted business as Brush Locker Tools or as Kauser Enterprises-USA. When asked by U.S. manufacturers about the end-user for a product, Khan either informed the manufacturer that the product would remain in the U.S., or he completed an end-user certification indicating that the product would not be exported.

After the products were purchased, they were shipped by the manufacturer to Khan's North Haven residence or Cerda Market in New Haven, a business owned by Khan. The products were then shipped to Pakistan on behalf of either the Pakistan Atomic Energy Commission, the Pakistan Space & Upper Atmosphere Research Commission, or the National Institute of Lasers & Optronics, all of which were listed on the U.S. Department of Commerce Entity List. Khan never obtained a license to export any item to the designated entity even though he knew that a license was required prior to export.

Israeli Executive Sentenced to Prison for Defrauding the Foreign Military Financing Program

A former executive of an Israel-based defense contractor was sentenced to 30 months in prison for his role in multiple schemes to defraud a multi-billion dollar United States foreign aid program. After being extradited from Bulgaria in October 2016, Yuval Marshak pleaded guilty to one count of mail fraud, two counts of wire fraud and one count of major fraud against the United States in U.S. District Court for the District of Connecticut on 13 March 2017. In addition to his prison sentence, he was ordered to pay restitution to the U.S. Department of Defense (DoD) in the amount of $41,170 and pay a criminal fine of $7,500.

According to court documents, Marshak carried out three separate schemes between 2009 and 2014 to defraud the DoD's Foreign Military Financing (FMF) program. Marshak and others falsified bid documents to make it appear that certain FMF contracts had been competitively bid when they had not. Marshak further caused false certifications to be made to the DoD stating that no commissions were being paid and no non-U.S. content was used in these contracts, when, in fact, Marshak had arranged to receive commissions and to have services performed outside the United States, all in violation of the DoD's rules and regulations. Marshak arranged for these undisclosed

commission payments to be made to a Connecticut-based company that was owned by a close relative to disguise the true nature and destination of these payments.

Former U.S. Naval Attaché and Military Advisor to the U.S. Ambassador in the Philippines Sentenced for Taking Bribes in Massive Navy Corruption Scandal

A Retired U.S. Navy Captain was sentenced in federal court to 41 months in prison for his role in a massive bribery and fraud scheme involving foreign defense contractor Leonard Glenn Francis and his firm, Singapore-based, Glenn Defense Marine Asia (GDMA). Brooks, who served as the U.S. Naval Attaché at the U.S. Embassy in Manila, Philippines, from 2006 to 2008, has admitted accepting bribes of travel and entertainment expenses, hotel rooms and the services of prostitutes. In return, Brooks admitted that he used his power and influence to benefit GDMA and Francis, including by securing quarterly clearances for GDMA vessels, which allowed GDMA vessels to transit into and out of the Philippines under the diplomatic imprimatur of the U.S. Embassy. Neither GDMA nor any other defense contractor has ever been granted such unfettered clearances.

Brooks admitted that he also allowed Francis to ghostwrite official U.S. Navy documents and correspondence, which Brooks submitted as his own. For example, Brooks admitted allowing GDMA to complete its own contractor performance evaluations. A November 2007 evaluation, drafted by GDMA and submitted by Brooks, described the company's performance as "phenomenal," "unsurpassed," "exceptional" and "world class." Brooks also admitted providing Francis with sensitive, internal U.S. Navy information, including U.S. Navy ship schedules and billing information belonging to a GDMA competitor, at times using a private Yahoo! e-mail account to mask his illicit acts.

Two Iranian Nationals Charged in Hacking of Vermont Software Company

Mohammed Reza Rezakhah and Mohammed Saeed Ajily, both Iranian nationals, were charged with a criminal conspiracy relating to computer fraud and abuse, unauthorized access to, and theft of information from, computers, wire fraud, exporting a defense article without a license, and violating sanctions against Iran.

According to the allegations in the indictment filed in Rutland, Vermont, beginning in or around 2007, Rezakhah, Ajily, and a third actor who has already pleaded guilty in the District of Vermont for related conduct, conspired together to access computers without authorization in order to obtain software which they would then sell and redistribute in Iran and elsewhere outside the U.S. Ajily, a businessman, would task Rezakhah and others with stealing or unlawfully cracking particular pieces of valuable software. Rezakhah would then conduct unauthorized intrusions into victim networks to steal the desired software. Once the software was obtained, Ajily marketed and sold the software through various companies and associates to Iranian entities, including universities and military and government entities, specifically noting that such sales were in contravention of U.S. export controls and sanctions.

As part of this conspiracy, in October 2012, Rezakhah hacked a Vermont-based engineering consulting and software design company best known for its software that supports aerodynamics analysis and design for projectiles. This software is designated as a "defense article" on the U.S. Munitions List of the International Traffic in Arms Regulations, meaning it cannot be exported from the U.S. without a license from the U.S. Department of State. Ajily thereafter promoted the same software as one of the products he could offer to his Iranian clients.

Indiana man admits role in Darknet weapons trafficking scheme

An Indiana man admitted to transporting weapons to New Jersey in connection with illegal firearms trafficking and sales activity he conducted on an underground internet based marketplace known as Alphabay. Benjamin Donald Brunni, 19, of Greensburg, Indiana, pleaded guilty before U.S. District Judge Brian R. Martinotti in Trenton federal court to one count of transporting and selling firearms without a license. Co-defendant Nicholas Michael Albertson, 20, of Columbus, Indiana, pleaded guilty to the same offense on July 14, 2017.

Beginning in April 2013, HSI special agents conducted an undercover investigation of illicit sales activity on various Darknet internet platforms. During the course of the investigation, Alphabay was identified as a website that provided a platform for vendors and buyers to conduct anonymous online transactions involving the sale of a variety of illegal goods, including firearms, ammunition, explosives, narcotics, and counterfeit items.

Unlike mainstream e-commerce websites, Alphabay was only accessible via the "Tor" network, which enabled its users to conceal their identities and physical locations. Although Tor has known legitimate uses, it is also used by cybercriminals seeking anonymity during illicit online activities.

During the course of the investigation, HSI agents learned that Brunni maintained a profile on Alphabay in which he expressed interest in the sale and purchase of firearms and ammunition. For approximately one month, Brunni negotiated with an undercover officer, whom he believed was an international purchaser of firearms, for the sale of numerous semi-automatic handguns and rifles.

Ultimately, Brunni agreed to sell 10 firearms to the undercover agents, including eight Glock-model semi-automatic handguns with obliterated serial numbers and two semi-automatic rifles for $7,550. Brunni also agreed to transport the weapons from his home in Indiana to New Jersey to complete the transaction.

On Sept. 9, 2016, Brunni and Albertson traveled to the meeting spot at a truck stop in Phillipsburg, New Jersey, and were subsequently arrested. Law enforcement agents recovered a loaded Smith & Wesson Model 5906 S-A Pistol in the vicinity of the Mercedes driver's seat, as well as three Glock Model 22 Pistols, one Glock Model 17 Gen 4 Pistol, one Glock Model 20 Pistol, one Glock Model 26 Gen 4 Pistol, one Glock Model 30 Pistol, one Glock Model 34 Pistol, one Rugar AR-556 assault rifle and one Anderson Mfg. AM-15 assault rifle. The serial numbers from each of the Glock handguns were obliterated and unrecognizable.

The unlicensed sale and weapons transportation charge carries a maximum potential penalty of five years in prison and a $250,000 fine. Sentencing for Brunni and Albertson is scheduled for Nov. 28, 2017 and Nov. 13, 2017, respectively.

New Zealand man sentenced for conspiring to export sensitive parts to China

A New Zealand man who traveled to Seattle last year to take possession of export-restricted parts designed for missile and space applications was sentenced to two years in federal prison for conspiring to violate the Arms Export Control Act. William Ali, 38, has been in federal custody since his arrest April 11, 2016, by HSI special agents.

According to records in the case and testimony presented at trial, Ali emailed several companies and distributors in April 2015 about purchasing certain accelerometers that are designed for use in spacecraft and missile navigation. These accelerometers cannot be exported from the United States without a license from the U.S. State Department, which Ali did not have. HSI learned of Ali's inquiries and began an investigation.

Over the next year, Ali communicated by phone and email with an HSI undercover special agent, and with a person in China known in his emails as "Michael." Michael was the person seeking the accelerometers, as well as certain gyroscopes that are designed for military use. Ali was working to find a way to purchase the devices and transport them secretly to Michael in China. In multiple emails, Ali made clear he was aware that export of the accelerometers and gyroscopes was illegal. Ali sent the undercover agent nearly $25,000 for the devices – money he got from Michael. Ali traveled to Seattle and met with the undercover HSI special agent April 11, 2016, at a downtown hotel. Shortly after Ali took possession of the devices he was arrested. Ali had with him an airline ticket to Hong Kong and a visa to travel to China.

California Man Arrested for Alleged Scheme to Smuggle Export-Controlled Rifle Scopes and Tactical Equipment to Syria

Rasheed Al Jijakli, the chief executive officer of an Orange County, California check cashing business, was arrested on federal charges that accuse him of procuring and illegally exporting rifle scopes, laser boresighters and other tactical equipment from the U.S. to Syria, in violation of the International Emergency Economic Powers Act.

The indictment accuses Jijakli, a naturalized U.S. citizen, of violating IEEPA, which authorizes the President of the U.S. to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy or economy of the U.S. In accordance with that authority, the President issued an executive order that included broad restrictions on exports to Syria. The U.S. Department of Commerce subsequently issued corresponding regulations restricting exports to Syria of items subject to the Export Administration Regulations. Jijakli also faces charges of conspiring to violate IEEPA and smuggling.

From January 2012 through March 2013, Jijakli and three other individuals purchased and smuggled export-controlled items to Syria without obtaining licenses from the Department of Commerce. Jijakli and others allegedly hand-carried the items through Istanbul, Turkey and provided them to fighters in Syria. Those items allegedly included day-and night-vision rifle scopes, laser boresighters (tools used to adjust sights on firearms for accuracy when firing), flashlights, radios, a bulletproof vest and other tactical equipment.

Texas Man Pleads Guilty to Conspiring to Illegally Export Radiation Hardened Integrated Circuits to Russia and China

Peter Zuccarelli of Plano, Texas pleaded guilty to conspiring to smuggle and illegally export from the U.S., radiation hardened integrated circuits (RHICs) for use in the space programs of China and Russia, in violation of the International Emergency Economic Powers Act. Zuccarelli pleaded guilty to engaging in a conspiracy to smuggle and illegally export from the U.S. items subject to IEEPA, without obtaining licenses from the Department of Commerce. According to the allegations contained in the Information filed against Zuccarelli and statements made in court filings and proceedings, including the guilty plea:

Between approximately June 2015 and March 2016, Zuccarelli and his co-conspirators agreed to illegally export RHICs to China and Russia. RHICs have military and space applications, and their export is strictly controlled. In furtherance of the conspiracy, Zuccarelli's co-conspirator received purchase orders from customers seeking to purchase RHICs for use in China's and Russia's space programs. Zuccarelli received these orders from his co-conspirator, as well as payment of approximately $1.5 million to purchase the RHICs for the Chinese and Russian customers. Zuccarelli placed orders with U.S. suppliers, and used the money received from his co-conspirator to pay the U.S. suppliers. In communications with the U.S. suppliers, Zuccarelli certified that his company, American Coating Technologies was the end user of the RHICs, knowing that this was false. Zuccarelli received the RHICs he ordered from U.S. suppliers, removed them from their original packaging, repackaged them, falsely declared them as "touch screen parts," and shipped them out of the U.S. without the required licenses. He also attempted to export what he believed to be RHICs. In an attempt to hide the conspiracy from the U.S. government, he created false paperwork and made false statements.

Chinese National Sentenced to Three Years for Attempting to Illegally Export High-Grade Carbon Fiber to China

Fuyi Sun, aka "Frank," 53, a citizen of China, was sentenced to three years in prison for violating the International Emergency Economic Powers Act in connection with a scheme to illegally export to China, without a license, high-grade carbon fiber, which is used primarily in aerospace and military applications. Sun pleaded guilty on April 21.

Since approximately 2011, Sun has attempted to acquire extremely high-grade carbon fiber, including Toray type M60JB-3000-50B carbon fiber (M60 Carbon Fiber). M60 Carbon Fiber has applications in aerospace technologies, unmanned aerial vehicles (commonly known as drones) and other government defense applications. Accordingly, M60 Carbon Fiber is strictly controlled for nuclear non-proliferation and anti-terrorism reasons. As part of these restrictions, the export of M60 Carbon Fiber to China without a license is prohibited.

In furtherance of his attempts to illegally export M60 Carbon Fiber from the U.S. to China without a license, Sun contacted what he believed was a distributor of carbon fiber – but which was, in fact, an undercover entity created by the Department of Homeland Security, Homeland Security Investigations (HSI) and "staffed" by HSI undercover special agents (the UC Company). Sun inquired about purchasing the M60 Carbon Fiber without the required license. In the course of his years-long communications with the undercover agents and UC Company, Sun suggested various security measures that he believed would protect them from "U.S. intelligence." Among other such measures, at one point, Sun instructed the undercover agents to use the term "banana" instead of "carbon fiber" in their communications. Consequently, soon thereafter he inquired about purchasing 450 kilograms of "banana" for more than $62,000. In order to avoid detection, Sun also suggested removing the identifying barcodes for the M60 Carbon Fiber, prior to transshipment, and further suggested that they identify the M60 Carbon Fiber as "acrylic fiber" in customs documents.

On April 11, 2016, Sun traveled from China to New York for the purpose of purchasing M60 Carbon Fiber from the UC Company. During meetings with the undercover agents on April 11 and 12, among other things, Sun repeatedly suggested that the Chinese military was the ultimate end-user for the M60 Carbon Fiber he sought to acquire from the UC Company, and claimed to have personally worked in the Chinese missile program. Sun further asserted that he maintained a close relationship with the Chinese military, had a sophisticated understanding of the Chinese military's need for carbon fiber, and suggested that he would be supplying the M60 Carbon Fiber to the Chinese military or to institutions closely associated with it.

On April 12, 2016, Sun agreed to purchase two cases of M60 Carbon Fiber from the UC Company. On that date, Sun paid the undercover agents purporting to represent the UC Company $23,000 in cash for the carbon fiber, as well as an additional $2,000 as compensation for the risk he believed the UC Company was taking to illegally export the carbon fiber to China without a license. Sun was arrested the next day.

CEO of International Metallurgical Company Sentenced to 57 Months in Prison for Conspiring to Export Specialty Metals to Iran

Erdal Kuyumcu, the chief executive officer of Global Metallurgy, LLC, based in Woodside, New York, was sentenced to 57 months in prison following his June 14, 2016 guilty plea to conspiracy to violate the International Emergency Economic Powers Act by exporting specialty metals from the United States to Iran. According to court documents, Kuyumcu, a U.S. citizen, conspired to export from the United States to Iran a metallic powder primarily composed of cobalt and nickel, without having obtained the required license from the U.S. Treasury Department's Office of Foreign Assets Control (OFAC). As established during a two-day presentencing evidentiary hearing, the metallic powder has potential military and nuclear applications. Such specialized metals are regulated by the U.S. Department of Commerce to combat nuclear proliferation and terrorism, and exporting them without the required license is illegal.

In furtherance of the illegal scheme, Kuyumcu and others plotted to obtain more than 1,000 pounds of the metallic powder from a U.S.-based supplier. To hide the true destination of the goods from the supplier, Kuyumcu arranged for the metallic powder to be shipped first to Turkey and then to Iran. Kuyumcu used coded language when discussing shipment of the powder with a Turkey-based co-conspirator, such as referring to Iran as the "neighbor." Shortly after one of the shipments was sent from Turkey to Iran, a steel company in Iran sent a letter-sized package to Kuyumcu's Turkey-based co-conspirator. The Iranian steel company had the same address as an OFAC-designated Iranian entity under the Weapons of Mass Destruction proliferators sanctions program that was associated with Iran's nuclear and ballistic missile programs.

BD White Birch Investment LLC Settles Potential Civil Liability for Apparent Violations of the Sudanese Sanctions Regulations

White Birch USA, a company headquartered in Greenwich, Connecticut, has agreed to pay $372,465 to settle its potential civil liability for three apparent violations of the Sudanese Sanctions Regulations. Specifically, White Birch USA appears to have violated §§ 538.205 and 538.206 of the SSR when it facilitated the sale and shipment of 543.952 metric tons of Canadian-origin paper from Canada to Sudan with a value of $354,602.26. The export

transactions occurred in April and December 2013. Various personnel within White Birch USA and its Canadian subsidiary, White Birch Paper Canada Company NSULC ("White Birch Canada"), were actively involved in discussing, arranging, and executing the export transactions to Sudan.

OFAC determined that White Birch USA did not voluntarily disclose the apparent violations to OFAC, and that the apparent violations constitute a non-egregious case. The statutory maximum civil monetary penalty amount for the apparent violations was $853,746, and the base civil monetary penalty amount for the apparent violations was $445,000.

Florida Businessman Pleads Guilty to Foreign Bribery Charges in Connection With Venezuela Bribery Scheme

A partial owner of several Florida-based energy companies pleaded guilty today to foreign bribery charges for his role in a scheme to corruptly secure contracts from Venezuela's state-owned and state-controlled energy company, Petroleos de Venezuela S.A. (PDVSA). Fernando Ardila Rueda (Ardila), 49, of Miami, pleaded guilty in federal court in Houston, to one count of conspiracy to violate the Foreign Corrupt Practices Act (FCPA) and one count of violating the FCPA. U.S. District Judge Gray H. Miller of the Southern District of Texas accepted the guilty plea.

According to admissions made in connection with his plea, Ardila conspired with U.S.-based businessmen Abraham Jose Shiera Bastidas (Shiera) and Roberto Enrique Rincon Fernandez (Rincon) to pay bribes and other things of value to PDVSA purchasing analysts. The bribes were paid to ensure that Shiera's and Rincon's companies were placed on PDVSA bidding panels and in order to obtain or retain business with PDVSA. From 2008 through 2014, while he was sales director, manager and partial owner of several of Shiera's companies, Ardila provided entertainment and offered bribes to PDVSA officials based on a percentage of the value of contracts the officials helped to award to Shiera's companies. Rincon, Shiera and two other former employees of Shiera's companies have also pleaded guilty in the case. Including Ardila, the Justice Department has announced a total of 10 individuals have pleaded guilty and are pending sentencing as part of a larger, ongoing investigation by the U.S. government into bribery at PDVSA.

BCC Corporate SA Settles Potential Liability for Apparent Violations of the Cuban Assets Control Regulations

BCC Corporate SA (BCCC) is a Belgium-based credit card issuer and corporate service company that issues various payment products, such as credit cards, to its European-based corporate customers. At the time of the apparent violations, BCCC was a wholly owned subsidiary of Alpha Card Group (Alpha Card), which in turn was owned 50 percent by American Express Company (AMEX), a U.S. financial institution. AMEX has agreed to remit $204,277 to settle potential civil liability for 1,818 apparent violations of the CACR.

Between April 9, 2009 and February 3, 2014, credit cards BCCC had issued to its corporate customers were used to make credit card purchases in Cuba. Although Alpha Card and BCCC had policies and procedures in place to review transactions for matches to OFAC's List of Specially Designated Nationals and Blocked Persons for compliance with U.S. economic sanctions laws, Alpha Card and BCCC nevertheless failed to implement controls to prevent BCCC-issued credit cards from being used in Cuba. Between April 9, 2009 and February 3, 2014, BCCC processed 1,818 transactions totaling $583,649.43 for more than 100 distinct corporate customers of BCCC whose cards were used in Cuba or that otherwise involved Cuba.1 The total base penalty amount for the 1,818 apparent violations was $291,825.OFAC has determined that AMEX voluntary self-disclosed the apparent violations to OFAC and that the apparent violations constitute a non-egregious case.

The settlement amount reflects OFAC's consideration of the following facts and circumstances, pursuant to the General Factors under OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. OFAC considered the following to be aggravating factors: (1) personnel within both Alpha Card and BCCC had reason to know of the conduct that led to the apparent violations; (2) despite Alpha Card's business model prior to its acquisition of BCCC in March 2009, in which it dealt exclusively with AMEX-related products (and therefore had

insight into all the parties involved in any transactions throughout the network), none of the companies involved appear to have appreciated the possibility or risk that BCCC-issued credit cards could be used in Cuba, and the company should have taken steps to assess the level of sanctions risk, and related controls, for BCCC-issued credit cards; (3) the apparent violations resulted in harm to U.S. sanctions program objectives at the time they occurred; (4) AMEX is a large and commercially sophisticated financial institution; and (5) during OFAC's investigation, AMEX and BCCC provided certain information on multiple occasions that was verifiably inaccurate or incomplete, including material omissions.

OFAC considered the following to be mitigating factors: (1) BCCC has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions giving rise to the apparent violations; (2) upon discovering the apparent violations, AMEX took swift and appropriate remedial action; (3) AMEX and BCCC voluntarily self-disclosed the apparent violations to OFAC; and (4) BCCC signed a statute of limitations tolling agreement and tolling agreement extensions.

OFAC Issues a Finding of Violation to Dominica Maritime Registry, Inc. for a Violation of the Iranian Transactions and Sanctions Regulations

OFAC has issued a Finding of Violation to Dominica Maritime Registry, Inc. (DMRI), of Fairhaven, Massachusetts, for a violation of the Iranian Transactions and Sanctions Regulations. Specifically, OFAC determined that on July 4, 2015, DMRI violated § 560.211 of the ITSR by dealing in the property or interests in property of the National Iranian Tanker Company (NITC), an entity identified by OFAC as meeting the definition of the Government of Iran and whose property and interests in property are blocked.1 In particular, DMRI executed a binding Memorandum of Understanding with NITC, which OFAC determined was a contingent contract and therefore property in which NITC, a blocked person, had an interest.

Section 560.211 of the ITSR prohibits U.S. persons from dealing in the property or interests in property of the Government of Iran. Since NITC is identified as an entity meeting the definition of the Government of Iran, DMRI was prohibited from dealing in its property or interests in property. Section 560.325 of the ITSR defines "property" and "property interests" to include "services of any nature whatsoever, contracts of any nature whatsoever, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent." OFAC determined that DMRI did not voluntarily disclose the violation and that the violation constitutes a non-egregious case. The determination to issue a Finding of Violation to DMRI reflects OFAC's consideration of the following facts and circumstances, pursuant to the General Factors as outlined in OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. OFAC considered the following to be aggravating factors: (1) DMRI failed to exercise a minimal degree of caution or care by executing a contingent contract with an entity it knew was listed on the SDN List at the time of the violation; (2) DMRI executives had actual knowledge of, and actively participated in, the conduct the led to the violation, and were aware of NITC's status when DMRI executed the contingent contract; and (3) DMRI undermined the policy objectives of the ITSR by dealing in the blocked property of a Government of Iran entity identified on the SDN List.

OFAC considered the following to be mitigating factors: (1) DMRI has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the date of the transaction giving rise to the violation; (2) DMRI is a small company; and (3) DMRI has taken remedial actions, including engaging trade counsel to assist it in understanding its obligations under U.S. sanctions laws, updating its OFAC compliance procedures, and undertaking a process to establish an OFAC compliance training program for all employees.

Based on the foregoing analysis of the General Factors, the conduct at issue, and the size of DMRI, OFAC determined that the issuance of this Finding of Violation is the appropriate enforcement response. OFAC found that DMRI is a small company and the scope of the underlying conduct at issue was limited. Additionally, based on information DMRI provided to OFAC, there was no performance of the contingent contract and DMRI represented that it has had no further dealings with NITC or any other sanctioned party.

Former US Army recruiter sentenced to more than 16 years in federal prison for straw purchasing firearms for Gulf Cartel

A former U.S. Army sergeant was sentenced to more than 16 years in federal prison following his role in a straw purchasing scheme that involved firearms smuggled to the Gulf Cartel. Julian Prezas, 37, from San Antonio was sentenced Nov. 2 by U.S. District Judge Orlando Garcia to 200 months in prison, three years of supervised release, and he must pay a $600 special assessment fee. On Dec. 12, 2016, Prezas pleaded guilty to five counts of making a false statement during the purchase of firearms and one count of attempting to export into Mexico defense articles on the U.S. Munitions List without obtaining a license or written authorization. By pleading guilty, Prezas admitted to conspiring with others from April to August 2015 to illegally purchase more than 40 assault rifles.

According to court records, Prezas was the actual purchaser of the firearms even though his co-defendants, other former U.S. Army soldiers, falsely indicated on their ATF form 4473 that they were buying the firearms at the time of purchase. Furthermore, Prezas, at times while in uniform and in a government vehicle, admittedly delivered the firearms to multiple individuals, one of whom was delivering them to members of the Gulf Cartel in Mexico.

DENTSPLY SIRONA Inc. Settles Potential Civil Liability for Apparent Violations of the ITSR

DENTSPLY SIRONA INC. (DSI), a U.S. company incorporated in Delaware, the successor in interest to DENTSPLY International Inc. ("DII" and, together with DSI, "DENTSPLY"), has agreed to pay $1,220,400 to settle its potential civil liability for 37 apparent violations of § 560.204 of the Iranian Transactions and Sanctions Regulations. Specifically, between on or about November 26, 2009 and July 5, 2012 DII subsidiaries UK International (UKI) and DS Healthcare Inc. (d.b.a. Sultan Healthcare) (Sultan), exported 37 shipments of dental equipment and supplies from the United States, to distributors in third-countries, with knowledge or reason to know that the goods were ultimately destined for Iran.

OFAC determined that DII did not voluntarily disclose the apparent violations and that the apparent violations constitute a non-egregious case. The statutory maximum penalty amount for the apparent violations is $9,551,082, and the base penalty amount for the apparent violations is $1,695,500. OFAC thoroughly considered the arguments DENTSPLY set forth in its submissions to OFAC, and the settlement amount reflects OFAC's consideration of the following facts and circumstances, pursuant to the General Factors under OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A.

Miami Residents Sentenced for Conspiracy to Illegally Export Prohibited Articles to Syria

Three Miami-Dade residents were sentenced today for their roles in a conspiracy to defraud the United States and to illegally export aviation parts and equipment to Syria, contrary to comprehensive U.S. economic sanctions against Syria, in violation of Title 18, United States Code, Section 371 and the International Emergency Economic Powers Act, Title 50, United States Code, Sections 1701-1706. The exports were sent to Syrian Arab Airlines, a/k/a "Syrian Air" (Syrian Air). Syrian Air had been designated as a Specially Designated National by the U.S. Department of Treasury, Office of Foreign Assets Control, meaning that U.S. persons and entities were prohibited from doing business with Syrian Air without a license.

Ali Caby, a/k/a "Alex Caby", 40, was sentenced by U.S. District Court Judge Beth Bloom to 24 months in prison, followed by two years of supervised release. Co-defendant Arash Caby, a/k/a "Axel Caby", 43, was sentenced to 24 months in prison, followed by two years of supervised release and a $10,000 fine. Co-defendant Marjan Caby, 34, was sentenced to 12 months and one day in prison, followed by two years of supervised release. The defendants had previously pled guilty to the charged conspiracy to violate IEEPA by exporting dual-use goods, that is, articles that have both civilian and military application, without a license to Syrian Air, the Syrian government's airline, which is an entity designated and blocked by OFAC for transporting weapons and ammunition to Syria in conjunction with Hizballah, a terrorist organization, and the Iranian Revolutionary Guard Corps (IRGC).

Ali Caby ran the Bulgaria office of AW-Tronics, a Miami export company that was managed by Arash Caby, and which shipped and exported various aircraft parts and equipment to Syrian Arab Airlines. Ali Caby and Arash Caby closely supervised and encouraged subordinate employees of AW-Tronics in the willful exportation of the parts and equipment to SDN Syrian Air, whose activities have assisted the Syrian government's violent crackdown on its

people. Marjan Caby, as AW-Tronics' export compliance officer and auditor, facilitated these exports by submitting false and misleading electronic export information to federal agencies.

Italian national pleads guilty to illegally exporting and attempting to export military technology

An Italian national pled guilty Thursday to illegally exporting controlled military technology from the United States to Italy following a joint investigation by U.S. Immigration and Customs Enforcement Homeland Security Investigations in New York and the Department of Defense, Defense Criminal Investigative Service, Northeast Field Office. Giovanni Zannoni, 35, of Gavorrano, Italy, has pleaded guilty to illegally exporting and attempting to export night vision equipment and assault rifle components. As part of his plea, Zannoni agreed to forfeit $436,673.73, in addition to the dozens of gun parts and night vision and thermal imaging devices recovered by the government in connection with this prosecution.

According to court filings and admissions made in court at the time he entered the guilty plea, between June 2013 and May 2017, Zannoni illegally exported and attempted to export night vision goggles and assault rifle components designated as defense articles on the United States Munitions List. The export of sensitive night vision equipment and assault rifle components requires a license from the United States Department of State. The Department of State has placed restrictions on the export of items that it has determined could make a significant contribution to the military potential and weapons proliferation of other nations and that could be detrimental to the foreign policy and national security of the United States. On May 14, 2017, the defendant was arrested after entering the United States at Miami International Airport.

International Export Control Agreements and Regimes

Wassenaar Arrangement

The 23rd Plenary Meeting of the Wassenaar Arrangement (WA) was held in Vienna on December 6 - 7, 2017. The WA continued its efforts to contribute to international and regional security and stability by promoting transparency and greater responsibility in the transfer of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations.

In 2017, WA Participating States continued to cooperate to ensure the detection and denial of undesirable exports, as well as to further refine the WA Control Lists and to make them more readily understood and user-friendly for licensing authorities and exporters. Significant attention was again given to keeping pace with international and regional security developments, advances in technology and market trends, although it is recognized that further work is needed to address new challenges. Ongoing priority was given to outreach activities to non-member countries and to encouraging voluntary adherence to the WA's standards.

Participating States agreed to the following:

- reaffirmed their strong support for robust export controls on a global basis as an important tool for ensuring international peace and stability and confirmed the continued relevance of the WA and the importance of adhering to its founding principles in this context;
- continued to exchange information on transfers of arms and dual-use goods and to assess the risks associated with illicit arms flows to specific geographic regions of concern, including areas of conflict;
- further underscored the importance of strengthening export controls and intensifying their cooperation to prevent arms trafficking and the acquisition of conventional arms and dual-use goods and technologies by terrorists, as an integral part of the global fight against terrorism;
- gave further particular attention to proliferation risks related to Small Arms and Light Weapons (SALW);
- adopted new export controls in a number of areas, including military explosives and specific electronic components. Existing controls were further clarified regarding ground stations for spacecraft, submarine diesel engines, technology related to intrusion software, software for testing gas turbine engines, analogue-to-digital converters, non-volatile memories and information security. Some controls were relaxed, such as for mechanical high-speed cameras and digital computers. For those products, control entries were either

deleted, or performance thresholds were updated taking into account the rapidly evolving capabilities of civil market products;

- agreed to continue a comprehensive and systematic review of the WA Control Lists to ensure their ongoing relevance;
- considered a number of proposals for new best practices guidelines and identified other existing guidelines for updating as appropriate in 2018 as part of a regular review cycle;
- introduced further enhancements to their electronic information-sharing tools;
- shared experiences in licensing and enforcement practice and discussed how to strengthen national export control implementation in areas such as arms trade risk assessment, effective end-use and end-user assurances, re-export and controls on intangible transfers of technology, as well as catch-all provisions;
- reviewed their principal outreach objectives and activities, including annual collective post-Plenary and technical briefings as well as bilateral dialogue (visits/meetings) with interested non-Participating States;
- continued to exchange information on industry/academia engagement and internal compliance programs; and
- maintained informal technical contacts with the Nuclear Suppliers Group (NSG) and the Missile Technology Control Regime (MTCR) on control list issues.

During the Plenary, participants agreed on the following changes to the lists of dual-use goods, technologies, and munitions. Below is a chart illustrating the changes. An updated version of the control list can be found on the Wassenaar website.

Category/Item	Comments
Category 1	
1.A.2.	- chapeau and para. a. amended- «prepregs or preforms» added
1.A.2.b.	- «Consisting of» replaced by «Made from»
1.C.1.	- «use as absorbers of» replaced by the function of «absorbing» and «waves» replaced by «radiation»
1.C.1.b.	- amended
1.C.2.c.2.; 1.C.2.d.3.	- global definitions (double quotes) changed to local definitions (single quotes) in 1.C.2.c.2. entries a. to h. and 1.C.2.d.3. entries a. to c. (new Technical Notes 1 to 10)
1.C.7.c.2., 1.C.7.d., 1.C.7.f.	- editorial correction: «listed under» replaced by «specified by» in the N.B.s
1.C.10.d.2.	- 'commingled' changed from a global to a local definition (new Technical Note)
1.C.10.e. and Technical Notes	- 'carbon fibre preforms' changed from global to local definition (new Technical Note 1) in the chapeau and in Note 1
1.C.12.a. Note b.	- 'effective grams' changed from global to local definition (new Technical Note)
1.C.12.b.	- 'Previously separated' changed from global to local definition (new Technical Note)
Category 2	
2.A.1. Note	- (or national equivalents) added
2.B.1.a. Note 2	- «and» deleted after «drilling»
2.B.1.c.1.b.	- «more» replaced by «four»
2.B.6.	- entire entry rewritten
2.B.7.a.	- deleted
2.B.8.	- chapeau amended - paras. a. and b. deleted

2.B.8.c.	- entry amended including new paras. 1 and 2 - 'Compound rotary tables' changed from global to local definition (new Technical Note)
2.B.8.d.	- new entry
2.E.3.a.	- deleted
2.E.3.b.1.c., 2.E.3.b.2.c.	- 'Direct-acting hydraulic pressing' changed from global to local definition (new Technical Note 1)
2.E.3.b.2.d.	- 'Hot isostatic densification' changed from global to local definition (new Technical Note 2)
2.E.3.d.	- deleted
Category 3	
3.A. Notes 1 & 2 and N.B.	- entries corrected to restore reference to 3.A.1.a.13. (3.A.1.a.12. ***to*** 3.A.1.a.14.)
3.A.1.a.2.	- EEPROMs, flash memories, MRAMs deleted from entry - 'non-volatile memories' added (new Technical Note)
3.A.1.a.5.a. and Technical Notes	- output rate replaced by "sample rate" in paras. 1 to 5 - new definition for "sample rate" - Technical Notes are amended including deletion of 3, 6, 7, 8 and 9 - "multiple channel ADCs" changed from a local to a global definition - "interleaved ADCs" changed from a local to a global definition
3.A.1.a.5.b.2.a.	- «arrive at or within» added
3.A.1.a.7. Note	- Simple Programmable Logic Devices (SPLDs) deleted
3.A.1.a.14.	- chapeau amended - input sample rate replaced by "sample rate" in paras. a.1 to 5 - new Technical Notes 1 to 4
3.A.1.b.2. Notes 2 and 3	- editorial correction: double quotes added to "MMIC"
3.A.1.b.4.	- new N.B.3.
3.A.1.b.11.	- 'Frequency synthesiser' changed from global to local definition (new Technical Note)
3.A.1.e.	- para. a. amended including new sub-paras. 1 and 2 - new local definition for 'continuous power density' (new Technical Note 5)
3.A.1.i.	- new entry for electro-optic modulators including a Note and Technical Note
3.A.2.c.1.	- 10 MHz replaced by 40 MHz
3.A.2.c.4.	- 'Real-time bandwidth' changed from global to local definition in para. a. (new Technical Note 1) - 'frequency mask trigger' changed from global to local definition in para. b.2. (new Technical Note 4)
3.A.2.h.	- input sample rate replaced by "sample rate" in paras. 1.a. to e. - new Technical Notes 1 to 4
3.B.1.j.	- new entry for mask "substrate blanks" - new local definition for 'Extreme Ultraviolet (EUV)' (new Technical Note)
3.B.2.	- paras. a. and c. amended
3.C.2.a.1.	- 245 nm changed to 193 nm
3.C.5.	- new para. b.
3.C.6.	- amended

3.E.1.	- new Note 3 and new Technical Note for local definition of 'Process Design Kit' ('PDK')
Category 4	
introductory Note 2	- 'main storage' changed from global to local definition (new Technical Note)
4.A.3.b.	- 16 WT changed to 29 WT
4.A.4.	- global definitions (double quotes) changed to local definitions (single quotes) in entries a. to c. (new Technical Notes 1 to 3)
4.D.1.b.1.	- 8.0 WT changed to 15 WT
4.D.4.	- new decontrol Note
4.E.1.	- new Notes 1 and 2 - new Technical Notes 1 and 2 for the local definitions 'vulnerability disclosure' and 'cyber incident response' - new Statement of Understanding
Technical Note on 'APP'	- in the Note to para. 1, «and» is deleted after «floating point additions»
Category 5 – Part 1	
5.A.1.a.	- para. 3 is now written in two paras – 5.A.1.a.3. and 4. - the corresponding Notes are amended and numbered 1 and 2
5.A.1.d. and Note 1	- 'Electronically steerable phased array antennae' changed from global to local definition (new Technical Note) - new decontrol Note 2 (existing Note numbered 1)
Category 5 – Part 2	
5.A.2.a.	- amended
5.A.2.b.	- amended
5.D.2.b.	- amended
5.E.2.b.	- amended
Category 6	
6.A.2.f.	- new entry for 'Read-out integrated circuits' ('ROIC') - new Technical Note for the local definition of 'ROIC' - new decontrol Note
6.A.3.a.1. and 2.	- deleted (mechanical high-speed cameras)
6.A.3.a.3.	- chapeau and para. a. deleted
6.A.4.a.1.	- 'Deformable mirrors' changed from global to local definition (new Technical Note)
6.A.4.f.	- new entry for dynamic wavefront measuring equipment - new Technical Note for the local definition of 'frame rate'
6.A.5.a.6.b. Note 1	- «and» deleted after «beam conditioning»
6.A.5.d.5.c.	- 'Transfer lasers' changed from global to local definition (new Technical Note)
6.A.5.f.1.	- deleted - new N.B.
6.A.5.f.2.	- amended including «capable of» replaced by «specially designed for»
6.A.5.f.3.	- amended including new sub-paras. a. and b.
6.A.8.e.	- «steerable» replaced by «scanned» - new Technical Note
6.A.8.l.1.	- 'Automatic target tracking' changed from global to local definition (new Technical Note)
6.A.8.l.4.	- 'geographically dispersed' changed from global to local definition (new Technical Note)

6.D.3.h.2.	- «and» deleted - in para. a., "electronically steerable phased array antennae" has been replaced by electronically scanned array antennae
Category 7	
7.A.6.a.	- 'Power management' changed from global to local definition (new Technical Note)
7.E.4.a.5.	- 'primary flight control' changed from global to local definition (new Technical Note)
7.E.4.a.6.	- 'Flight control optical sensor array' changed from global to local definition (new Technical Note)
7.E.4.b.5. Note	- 'flight path optimisation' changed from global to local definition (new Technical Note)
7.E.4.c.3.	- 'variable geometry airfoils' changed from global to local definition (new Technical Note)
rewritten (references replace descriptions)	
Very Sensitive List	
1.A.2.a.1.	- replaces former 1.A.2.a. for "Composite" structures or laminates
1.C.1.	- consequential change following amendment to corresponding entry in the Dual-Use List
6.A.1.a.2.c. and 6.A.1.a.2.f.	- editorial correction: hyphen added in "user-accessible programmability"
Munitions List	
ML1.d.	- positive text replaces decontrol Note
ML8.a.42	- new entry for an explosive
ML8.c.1.	- new Note 1 (existing Note numbered 2)
ML8.c.10.b. Note	- «JP-4, JP-8,» deleted – Note now applies to all fuels for civil use aviation
ML8.e.16.	- editorial correction: parenthesis added before (nitratomethylmethyloxetane)
ML8.e.21.	- new entry for an energetic material
ML8.f.5.	- copper beta-resorcylate added
ML9.b.1.	- paras. a. and b. deleted (performance parameters)
ML13.a. N.B.	- editorial: «s» added to «plate»
ML15. Note 1	- list of components deleted
ML17.l.	- amended
ML17.o.	- «and» replaced by «or» in parenthetical example
ML20.b.	- «and» replaced by «or» in parenthetical example
Definitions	

"Automatic target tracking" "Carbon fibre preforms" "Commingled" "Comminution" "Compound rotary table" "Deformable mirrors" "Direct-acting hydraulic pressing" "Effective gram" "Electronically steerable phased array antenna" "Flight control optical sensor array" "Flight path optimization" "Frequency mask trigger" "Frequency synthesiser" "Gas atomisation" "Geographically dispersed" "Hot isostatic densification" "Linearity" "Main storage" "Mechanical alloying" "Melt extraction" "Melt spinning" "Neural computer" "Optical computer" "Plasma atomisation" "Power management" "Previously separated" "Primary flight control" "Real-time bandwidth" "Resolution" "Rotary atomisation" "Settling time" "Solidify rapidly" "Splat quenching" "Systolic array computer" "Transfer laser" "Vacuum atomisation" "Variable geometry airfoils"	- these global definitions have been deleted from the Definitions section of the Lists. They have been replaced by local definitions in the form of Technical Notes
"Compensation systems"	- editorial correction: double quotes added to "magnetometers" (Cat 6)
"Cryptographic activation"	- «specifically» added before «activates» (Category 5 – Part 2) - «secure» deleted before «mechanism»
"Interleaved Analogue-to-Digital Converter (ADC)"	- new definition (Category 3)
"Multiple channel Analogue- to-Digital Converter (ADC)"	- new definition (Category 3)
"Sample rate"	- new definition (Category 3)
"Steady state mode"	- new definition (Category 9)
"User-accessible programmability"	- reference to Categories 4 and 5 have been deleted
Acronyms and Abbreviations	No amendments were made to the Acronyms and Abbreviations
Statements of Understanding and Validity Notes	
4.E.1.	- new SOU
9.A.4.f.	- new Validity Note until 31 December 2019

9.A.12.	- SOU deleted
9.B.1.c.	- Validity Note extended until 31 December 2020

Although the U.S. is a member of the Wassenaar Arrangement, it has not implemented these amendments into the Export Administration Regulations (EAR). It is BIS's custom to implement these changes between the spring and fall of the following year, and they do not become effective until they are published as a final rule in the Federal Register. For example, the Wassenaar control list changes agreed to at the December 2015 Plenary were not implemented into the EAR until they were published in the Federal Register in September 2016.

Online Resources:

- The Wassenaar Arrangement Home Page
- Summary of Changes to the Dual Use List
- New 2017 Dual Use List

The next regular Wassenaar Arrangement Plenary meeting will take place in Vienna in December 2018. The United Kingdom will assume the Chair of the Plenary for 2018, and has designated Ambassador Leigh Turner to assume this role. Additional information can be found on the Wassenaar website.

Missile Technology Control Regime

In October 2017, the Missile Technology Control Regime (MTCR) held its 31th Plenary Meeting in Dublin, Irelan. The MTCR, which includes 35 member states, is an informal and voluntary association of countries which share the goals of non-proliferation of unmanned delivery systems capable of delivering weapons of mass destruction, and which seek to coordinate national export licensing efforts aimed at preventing their proliferation. The aim of the MTCR is to restrict the proliferation of missiles, complete rocket systems, unmanned air vehicles, and related technology for those systems capable of carrying a 500 kilogram payload at least 300 kilometers, as well as systems intended for the delivery of weapons of mass destruction (WMD).

The MTCR's controls are applicable to certain complete rocket systems (to include ballistic missiles, space launch vehicles (SLVs), and sounding rockets) and unmanned air vehicle (UAV) systems (to include cruise missiles, drones, UAVs, and remotely piloted vehicles (RPVs)). Partners also recognize the importance of controlling the transfer of missile-related technology without disrupting legitimate trade and acknowledge the need to strengthen the objectives of the Regime through cooperation with countries outside the Regime.

The MTCR's 35 members are Argentina, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, India, Italy, Ireland, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, the Russian Federation, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom and the United States of America.

The main purpose of the Plenary Meeting was to review and evaluate the MTCR's activities over the last 12 months and to intensify the efforts of Partners to prevent the proliferation of unmanned delivery systems capable of delivering WMD. In this regard Partners devoted increased attention to Intangible Technology Transfer (ITT), Unmanned Aerial Vehicles (UAVs), Catch All Controls, Regional Proliferation and strategic outreach to non-MTCR countries.

In this year's Plenary, Partners recalled that the proliferation of WMD (nuclear, chemical and biological weapons) and their means of delivery remain a threat to international peace and security. They reiterated their commitment to limit the risks of proliferation by controlling international transfers that can contribute to delivery systems for WMD. They held a thorough exchange of information on missile proliferation developments since the last Plenary Meeting in Busan.

Partners welcomed the fact that the MTCR Guidelines and control lists in the Annex constitute an international best practices benchmark for controlling exports of missile-related items and technologies, and noted that these standards are adhered to by an increasing number of non-Partners and are included in some UN Security Council resolutions.

Partners also called on all states to exercise extreme vigilance to prevent the transfer of goods and technology which could contribute to WMD missile programs, in accordance with their national legislation and consistent with international law. They confirmed their commitment to inform and assist interested parties that are supportive of the MTCR's objectives and purposes.

In the interests of regional and international security, Partners appealed to all states to support the non-proliferation aims of the Regime by observing its Guidelines and establishing appropriate national legislation and law enforcement mechanisms. From this perspective, partners emphasized that observance of the MTCR Guidelines by as many states as possible will contribute substantially to limiting the risks of proliferation of delivery systems for WMD and to fostering international security. Partners invited states to declare, on a voluntary basis, adherence to the MTCR Guidelines and formally notify the MTCR Point of Contact in writing of their political commitment to control all of the items on the MTCR Annex according to the MTCR Guidelines, including any subsequent changes to the Annex/Guidelines. Current MTCR adherents include Estonia and Latvia.

Partners underlined that the MTCR Guidelines are not designed to impede technological advancement and development, including space programs, as long as such activities could not contribute to delivery systems for WMD.

Partners conducted extensive discussions on and expressed concern about global missile proliferation activities, in particular ongoing missile programs in the Middle East, Northeast Asia, and South Asia, which might fuel missile proliferation activities elsewhere. Partners also encouraged relevant regional bodies and institutions to pay attention to the role of export controls in preventing the proliferation of missiles capable of carrying WMD.

Within the framework of the MTCR mandate, Partners confirmed their commitment to implement fully UN Security Council resolutions 1695, 1718, 1874, 2087, 2094, 2270, 2321, 2356, 2371 and 2375, having in mind the ballistic missile-related provisions of the resolutions, in particular resolution 2371. Bearing in mind the grave international situation due to DPRK missile development, partners reiterated their firm commitment to exercise extreme vigilance when controlling transfers that could contribute to the DPRK's ballistic missile program, in response to the drastic escalation of ballistic missile launches and significant missile technology development by the DPRK since February 2016. With regard to Iran, Partners noted the continuing process of implementation of the Joint Comprehensive Plan of Action (JCPOA) endorsed by UN Security Council resolution 2231. Partners confirmed their commitment to implement this resolution, having in mind the ballistic missile-related provisions in Annex B of this resolution. Partners agreed to continue exchanging views on missile program developments.

Partners expressed particular appreciation for the outreach activities conducted by the outgoing MTCR Chairman Director General Ham Sang-wook of the Republic of Korea. The new MTCR Chairs were encouraged to follow up and conduct further outreach activities and contacts in order to increase transparency about the Regime, to promote its objectives and to maintain the momentum of dialogue with the visited countries. Partners also encouraged the continuation of individual, collective and regional efforts to assist non-Partner states and other interested parties in implementing missile-related export controls, and to inform the Chair about these activities.

Partners reaffirmed the critical importance of the MTCR's on-going technical work. They underlined that the rapid technological development and changes in proliferant procurement practices related to sensitive items and technologies continue to require great awareness and effective actions to address these developments. They recognized that the Equipment, Software, and Technology Annex is a cornerstone of the work done by the MTCR to prevent missile proliferation and expressed deep appreciation for the accomplishments of the MTCR's Technical Experts Meeting (TEM).

Partners also expressed their deep appreciation for the work of the MTCR's Licensing and Enforcement Experts Meeting (LEEM), and the Information Exchange Meeting (IEM). In the IEM and LEEM, Partners continued discussions on a number of issues, including proliferation trends, procurement activities and strategies in support of

programs for WMD delivery means; serious risks and challenges posed by intangible technology transfers (ITT); key technology trends in missile programs; catch-all controls for non-listed items; and brokering, transit and transhipment issues, and efforts to exploit them to evade export controls. These discussions showed that constant awareness; sharing of information, including best practices; and updating of MTCR countries' export control systems and enforcement efforts are of great importance and have a significant impact on their work aimed at curbing proliferation of WMD means of delivery.

Further information on the MTCR is available on its website.

Australia Group

The Australia Group (AG) held its 32nd plenary meeting in June 2017. The Australia Group is a cooperative and voluntary group working to counter the spread of technologies and materials that may facilitate the development or acquisition of chemical and biological weapons (CBW) by states of concern and terrorists. Among the measures agreed by the Group at the 32nd Plenary were:

- issuing a statement on the 20th anniversary of the entry into force of the Chemical Weapons Convention, expressing the Group's grave concerns about the resurgence in the use of chemical weapons;
- reinforcing efforts to stay ahead of potential proliferators by increasing awareness of emerging technologies, the potential exploitation of the cyber sphere, and scientific developments that could be used for chemical and biological weapons production and delivery;
- intensifying Australia Group focus on preventing the proliferation of goods, technologies and information to terrorists and non-state actors that could enable the production or delivery of chemical and biological weapons or attacks;
- sharing approaches to challenges posed by intangible technology transfers, proliferation financing, procurement, transhipment and broader proliferation networks, including through enhanced engagement with industry and academia;
- renewed commitment to work collaboratively and cooperatively, both domestically and internationally, and to share experiences in enforcing export controls, information, outcomes of investigations and operational activity; and
- agreement to enhance outreach to non-members through more regular Australia Group Dialogues and continued efforts to encourage all states to implement robust export controls and to adopt Australia Group export controls as the model for international best practice.

Recognizing the 20th anniversary of the entry into force of the CWC, the Australia Group issued on June 30th a statement expressing grave concern and regret at the evidence and allegations of chemical weapons use in Syria and Iraq and condemning the threat that this poses to international norms against the use of chemical weapons. Members highlighted the important work of the OPCW in implementing the CWC over the past 20 years, which was recognized with the awarding of the Nobel Peace Prize in 2013.

Australia Group members expressed concern about the DPRK's chemical and biological weapons capability. The use of VX nerve gas to kill Kim Jong-nam in the Kuala Lumpur International Airport in February this year adds urgency to the need for action to address the threat of chemical weapons.

Members emphasized the importance of all countries fully implementing the restrictions on the transfer of chemical and biological weapons-related items, materials, equipment, goods, and technology to the DPRK, established in relevant UN Security Council Resolutions, including 1718, 2270, 2321 and 2356.

The Australia Group reaffirmed its view that the horrific use of chemical weapons against the people of Syria and Iraq underlines the necessity to uphold the complete prohibition on the use of chemical weapons by anyone,

anywhere at anytime, through universal adherence to and effective implementation of the CWC. Members noted the release of the OPCW Fact Finding Mission (FFM) report on 29 June, and the statement by the Director-General of the OPCW that "the OPCW FFM has confirmed the use of sarin, a nerve agent, at the 4 April incident in Khan Shaykhun in Syria".

The Australia Group urged Syria to facilitate the complete and verified destruction of its entire chemical weapons program and to resolve all ambiguities in its declaration to the OPCW, and to cooperate fully with the OPCW's Fact Finding Mission and OPCW-United Nations Joint Investigative Mechanism, so that the international community will have confidence that Syria is meeting its obligations under UN Security Council Resolutions 2118, 2209, 2235, 2314, 2319 and the CWC in full.

Additional information on the AG can be found on its website.

Nuclear Suppliers Group

The 27th Plenary Meeting of the Nuclear Suppliers Group (NSG) took place in Bern, Switzerland in June 2017. The NSG is a Group of 48 nuclear supplier countries that seeks to contribute to the non-proliferation of nuclear weapons through the implementation of two sets of Guidelines for nuclear exports and nuclear-related exports.

Participating Governments reiterated their firm support for the full, complete and effective implementation of the NPT as the cornerstone of the international non-proliferation regime. Within the framework of the NSG's mandate, the Group exchanged information on and expressed its concerns regarding continued global proliferation activities and reaffirmed its determination to continue to cooperate closely in order to deter, hinder and prevent the transfer of controlled items or technology that could contribute to nuclear weapons or other nuclear explosive devices.

The Participating Governments reconfirmed their commitment to UNSCRs 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) and 2356 (2017), which strongly condemned the DPRK's nuclear tests. Within the framework of the NSG's mandate, the Participating Governments noted that the supply of all NSG controlled items to the DPRK is prohibited according to the abovementioned resolutions.

The NSG welcomed the continued implementation of the Joint Comprehensive Plan of Action (JCPOA) concluded by the E3/EU+3 and the Islamic Republic of Iran and endorsed by UNSCR 2231 (2015). Since the last Plenary the NSG continued to receive briefings from the JCPOA Procurement Working Group Coordinator regarding the work of the Procurement Channel established in accordance with the JCPOA and UNSCR 2231. Participating Governments expressed interest in receiving further briefings.

At the Plenary meeting, the NSG also:

- maintained its focus on technical issues important to the implementation of the Control Lists by exchanging views and agreeing on a number of proposals to clarify and update the NSG Control Lists;
- discussed and reaffirmed the significance of updating the NSG Guidelines to keep pace with the evolving global security landscape and a fast-paced nuclear and nuclear-related industry;
- discussed the NSG's policies regarding transparency and confidentiality;
- discussed and exchanged information and best practices on licensing and enforcement;
- welcomed the growing number of States that have harmonized their national export control systems with the NSG Guidelines and Control Lists;
- took note of a report on outreach to non-NSG participants and agreed on the value of these outreach activities;
- discussed options for enhancing outreach and approved revised guidance for such outreach;
- continued to consider all aspects of the implementation of the 2008 Statement on Civil Nuclear Cooperation with India and discussed the NSG relationship with India.

Further information on the NSG is available on its website.

Recommendations for 2018

We anticipate the following actions in 2018, which you can begin preparing for now:

- There have been continued developments in the export/import control regulations of various foreign governments, including France, Israel, Hong Kong, India Russia and China, related to the control of cryptographic products and provision of cloud-related services. These requirements have presented challenges to U.S. exporters/importers of cryptographic products as foreign governments continue to implement these regulations.

  One significant change that already occurred is BIS's implementation of a reporting requirements for compliance with the Hong Kong TID import regulations. We also anticipate a more formal implementation of India's import and export regulations pursuant to its admission into various international organizations, including the Wassenaar Arrangement. We will keep you posted on updates to these requirements, but we recommend contacting resellers and distributors with a presence in these countries to ensure that your products are handled in compliance with these foreign regulations.

  We will also discuss these changes at the annual American Conference Institute's *Advanced Industry Forum on Global Encryption, Cloud & Cyber Export Controls*. The 8th year of the conference will be held on March 26 - 28 in San Francisco, California, and will once again be co-chaired by Roz Thomsen. In addition to foreign exporters and importers, this conference will be of interest to companies that are facing obstacles are the use and provision of cloud-based services becomes more widespread. Please let us know if you are interested in attending so you can take advantage of our registration discount code. Additional information can be found on the conference website.

- Participants of 23rd Plenary Meeting of the Wassenaar Arrangement agreed on several changes to the lists of dual-use goods, technologies, and munitions. One significant agreement that U.S. industry should keep an eye on is the clarifications related to the "cybersecurity" controls. The control on "intrusion software," for example, does not apply to vulnerability disclosure or cyber incident response, which was a concern of exporters in the prior controls. It will be interesting to see how the U.S. responds to these changes, and if they will pursue further clarification of the controls, draft a new export control rule.

- Another emerging technology, and potential area of export control, to keep an eye on in 2018 is "Artificial Intelligence." Both the U.S. President's National Security Advisor and Head of Secretariat at the Wassenaar Arrangement published statements on this topic in December, noting that "Artificial Intelligence," including self-driving cards to autonomous weapons, and the integration of advanced sensors, are emerging technologies of concern that the U.S. and Wassenaar Arrangement will continue to address.

- The major announcements this year related to the sanctions programs include State Department enforcement against certain entities in Cuba and Russia, and corresponding implementations into the BIS and OFAC sanctions programs regulations. We will update you on any changes, but you can begin to ensure that your export practices are consistent with the current BIS, OFAC and State Department sanctions program regulations.

- Exporters of encryption products should be aware that the end of the year marks the close of the reporting period for semi-annual ENC reports. With the elimination of the Encryption Registration Number and the streamlining changes made to Encryption items, many items no longer require reporting or the requirements have changed. This is a good time to prepare required reports, which are due no later than February 1, 2018 and to analyze current products to determine if reporting is no longer required.