www.t-b.com

U.S. EXPORT CONTROLS PAST, PRESENT AND FUTURE (2018 Edition)

Introduction – Looking Back at 2018

The US Government implemented significant changes to export control laws and regulations in 2018, including the Department of Commerce's Bureau of Industry and Security (BIS), Department of the Treasury's Office of Foreign Assets Control (OFAC), the Department of State and the Office of the US Trade Representative (USTR):

- The President signed the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (H.R. 5515). The NDAA includes export control reform provisions requiring the Commerce Department to establish export controls on emerging and foundational technologies, which are still being defined. BIS has since published an Advanced Notice of Proposed Rulemaking (ANPRM) in the Federal Register which sought public comment on criteria for identifying emerging and foundational technologies, which are due on January 10, 2018. The NDAA is also designed to strengthen the current Committee on Foreign Investment in the United States process, which reviews proposed foreign investments in the U.S. in order to determine the effect of such transactions on the national security of the U.S.

- Throughout the year, the USTR announced multiple rounds of new import tariffs on Chinese-origin items pursuant to a Section 301 action. The tariffs impact a wide range of goods that range from an additional 10% to 25% duty on the import of Chinese-origin goods into the U.S. The first 3 lists of items subject to the Section 301 tariffs have been finalized and the tariffs are now implemented. The changes included some reorganization of the Harmonized Tariff Schedule (HTS), including subheading 8517.62, which covers several types of telecommunications equipment.

- There were significant enforcement actions in 2018. The ZTE case was settled this year, and resulted in more than a $1 billion fine and other compliance measures. BIS also issued the largest civil penalty to be paid by an individual in BIS history. There were also penalties assessed to companies for a failure in third-party screening software, as well as a failure to screen against entities blocked under OFAC's "50% rule."

- There have been several changes to the sanction's programs implemented by OFAC and the State Department. The U.S. officially ceased its participated in the Joint Comprehensive Plan of Action (Iran Nuclear Deal), and certain sanctions against Iran were re-imposed under OFAC's Iranian Transactions and Sanctions Regulations. There were also additional sanctions implemented against Russia and Venezuela, as well as the removal of OFAC's Sudanese Sanctions Regulations.

- BIS revised several Export Control Classification Numbers to reflect changes to the control lists various multilateral regimes, including the Wassenaar Arrangement, Australia Group, Missile Technology Control Regime, and Nuclear Suppliers Group.

Additional information describing these changes is included below.

2018 Export Control Reform Updates

In recent years, we have focused this summary on the "broad-based interagency" review of U.S. export control regulations ordered by President Obama in 2009, 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.

Since the introduction of the Export Control Reform (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 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.

There were not many updates this year to the ECR Initiative. We did see proposed revisions to Categories I (Firearms), II (Artillery Projectors) and III (Ammunition) of the ITAR, as described in more detail below.

However, 2018 brought the Export Control Reform Act (ECRA), which established permanent statutory authority for current U.S. export controls implemented through the EAR. The ECRA repeals and replaces the Export Administration Act of 1979, which was the statutory authority for dual-use export controls until it lapsed in 1994, and which has been continued every year since by Executive Order of the President under the International Emergency Economic Powers Act (IEEPA). The ECRA was only one act under the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019, which was signed into law in August. The NDAA also included the Foreign Investment Risk Review Modernization Act (FIRRMA), which is designed to strengthen the Committee on Foreign Investment in the United States (CFIUS) review process.

Export Controls Act of 2018

The Export Controls Act of 2018 in the NDAA provides permanent statutory authority for the existing Export Administration Regulations. The EAR has been operating under emergency authority of the International Emergency Economic Powers Act for many years, ever since the Export Administration Act of 1979 lapsed. The ECRA does not expire, and replaces the EAR until the EAR is resolved or amended. The ECRA adds several noteworthy changes:

- New export controls on "emerging and foundational technologies," which are not specifically identified in the legislation.
- Commerce will revise the duties of the Emerging Technology and Research Advisory Committee to help identify "emerging and foundational technologies" that may be developed over a period of 5 or 10 years.
- License applications are now required to be reviewed for impact on the US defense industrial base. Transactions that would have a "significant impact on that defense industrial base can be denied.
- The government is required to publish export license details for licenses involving certain terrorism-supporting countries.
- Increased civil penalties per violation to $300,000 or twice the value of the transaction

Identifying "emerging and foundational technologies" is an important part of this legislation. BIS solicited comments on criteria for identifying emerging technologies that are essential to US national security, which were initially due on December 19, 2018, but the date has now been extended until January 10, 2019. This process will be determined by an interagency process that will consider both public and classified information, and information

from the Emerging Technology Technical Advisory Committee and the Committee on Foreign Investment in the United States. The process will consider:

- The development of emerging and foundational technologies in foreign countries;
- The effect export controls may have on the development of such technologies in the US; and
- The effectiveness of export controls on limiting the proliferation of emerging and foundational technologies in foreign countries.

There are several categories of technology that the Commerce Department wants to determine if there are specific emerging technologies that are essential to the national security of the US. These categories include:

1. Biotechnology: nonbiology synthetic biology, genomic and genetic engineering, or neurotech
2. Artificial intelligence (AI) and machine learning: such as Neural networks and deep learning (e.g., brain modelling, time series prediction, classification), evolution and genetic computation (e.g., genetic algorithms, genetic programming), reinforcement learning, computer vision (e.g., object recognition, image understanding), export systems (e.g., decision support systems, teaching systems), speech and audio processing (e.g., speech recognition and production), natural language processing (e.g., machine translation), planning (e.g., scheduling, game playing), audio and video manipulation technologies (e.g., voice cloning, deepfakes), AI cloud technologies, or AI chipsets;
3. Position, Navigation, and Timing (PNT) technology
4. Microprocessor technology: systems-on-Chip (SoC) or Stacked Memory on Chip
5. Advanced computing technology: memory-centric logic
6. Data analytics technology: visualization, automated analysis algorithms or context-aware computing
7. Quantum information and sensing technology: quantum computing, quantum encryption, or quantum sensing
8. Logistics technology: mobile electric power, modeling and simulation, total asset visibility or Distribution-based Logistics Systems (DBLS)
9. Additive manufacturing: 3-D printing
10. Robotics: micro-drone and micro-robotic systems, swarming technology, self-assembling robots, molecular robotics, robot compilers, or smart dust
11. Brain-computer interfaces: neural-controlled interfaces, mind-machine interfaces, direct neural interfaces, or brain-machine interfaces
12. Hypersonics: flight control algorithms, propulsion technologies, thermal protection systems, or specialized materials (for structures, sensors, etc.)
13. Advanced Materials: camouflage, functional textiles (e.g., advanced fiber and fabric technology), or biomaterials; and
14. Advanced surveillance technologies: faceprint and voiceprint technologies

BIS also welcomed comments on:

1. How to define emerging technology to assist identification of such technology in the future
2. Criteria to apply to determine whether there are specific technologies within these general categories that are important to US national security
3. Sources to identify such technologies
4. Other general technology categories that warrant review to identify emerging technology that are important to US national security
5. The status of development of these technologies in the US and other countries
6. The impact specific emerging technology controls would have on US technological leadership; and
7. Any other approaches on the issue of identifying emerging technologies important to US national security, including the stage of development or maturity level of an emerging technology that would warrant consideration for export control

Foreign Investment Risk Review Modernization Act

The Foreign Investment Risk Review Modernization Act (FIRRMA) strengthens the Committee on Foreign Investment in the United States (CFIUS) review process. CFIUS is the US Government's existing foreign investment review authority, determining if foreign investments threaten national security. The US Department of the Treasury, as chair of the CFIUS, issued temporary regulations implementing the first step of the FIRRMA legislation, which can be addressed in two parts:

1. Treasury made limited updates to CFIUS's existing regulations, effectively immediately. These limited updates are primarily to implement provisions of FIRRMA that became immediately effective upon its enactment.
2. Effective November 10, 2018, the Treasury Department implemented its pilot program, which had two key provisions:
    a. It puts into effect the first mandatory filing requirements ever imposed by the CFIUS, with a potential civil monetary penalty up to the value of the transaction for failure to file notice under the new regulations.
    b. It expands the scope of transactions subject to CFIUS review to include certain non-controlling investments in US businesses involved in critical technologies related to specific industries.

FIRRMA Pilot Program

CFIUS's jurisdiction is being expanded to give the Committee the authority to review "other investments" made by any foreign persons in Pilot Program US Businesses.

- Types of investments covered: For an investment to be covered under the pilot program, it would have to give the foreign investor:
    - Access to any material nonpublic technical information in the possession of the target US business;
    - Membership or observer rights on the board of directors or equivalent governing body of the US business, or the right to nominate an individual to a position on the board of directors or equivalent governing body of the US business; or
    - Any involvement, other than through voting of shares, in substantive decision making of the US business regarding the use, development, acquisition, or release of critical technology.
- Foreign persons covered: The pilot program covers all foreign persons and is not country-specific
- US businesses covered: The pilot program covers any US business that produces, designs, tests, manufactures, fabricates, or develops a critical technology that is 1) utilized in connection with the US businesses' activity in one or more Pilot Program Industries or 2) designed by the US business specifically for use in one or more Pilot Program Industries.
- Critical technologies covered: The pilot program covers all critical technologies, as defined by FIRRMA, including items on the US Munitions List, some items on the Commerce Control List controlled for reasons specified in the pilot program regulations, and emerging and foundational technologies controlled pursuant to the Export Control Reform Act of 2018. The emerging and foundational technologies have yet to be defined.
- Industries covered: The pilot program covers 27 industries, identified by their respective North American Industry Classification System (NAICS) code (Pilot Program Industries). The US Government carefully developed the list of pilot program industries for which certain strategically motivated foreign investment could pose a threat to US technological superiority and national security. The list of pilot program industries includes aircraft manufacturing, optical instrument and lens manufacturing, computer storage device manufacturing, wireless communications equipment manufacturing, semiconductor manufacturing, and semiconductor machinery manufacturing, among other industries.
- Mandatory declarations: The pilot program establishes mandatory declarations (i.e., abbreviated notices that generally should not exceed five pages in length) for foreign transactions involving Pilot Program US

Businesses that are within the purview of CFIUS (i.e., both controlling investments and "other investments").

- Declarations must be filed at least 45 days prior to a transaction's expected completion date. The Committee will have 30 days to take action.
- Parties may choose to file a notice under CFIUS's standard procedures rather than a declaration.
- Parties that are required to file with CFIUS and do not do so can be assessed a civil monetary penalty up to the value of the transaction.

As stated above, the pilot program commenced on November 10, 2018. It will end no later than the date on which the final FIRRMA regulations are implemented.

Additional ECR Updates

BIS and DDTC publish proposed rules to amend USML Categories I, II and III

The proposed rule described how articles the President determines no longer warrant control under United States Munitions List Category I--Firearms, Close Assault Weapons and Combat Shotguns; Category II--Guns and Armament; and Category III--Ammunition/Ordnance, would be controlled on the Commerce Control List and by the Export Administration Regulations. This proposed rule is being published in conjunction with a proposed rule from the Department of State, Directorate of Defense Trade Controls, which would amend the list of articles controlled by USML Category I (Firearms, Close Assault Weapons and Combat Shotguns), Category II (Guns and Armament), and Category III (Ammunition/Ordnance) of the USML to describe more precisely items warranting continued control on that list.

The changes described in the proposed rule on Categories I, II, and III of the USML are based on a review of those categories by the Department of Defense, which worked with the Departments of State and Commerce in preparing the amendments. The review was focused on identifying the types of articles that are now controlled on the USML that are either (i) inherently military and otherwise warrant control on the USML or (ii) if of a type common to non-military firearms applications, possess parameters or characteristics that provide a critical military or intelligence advantage to the United States, and are almost exclusively available from the United States. If an article satisfies one or both of those criteria, the article remains on the USML. If an article does not satisfy either criterion, it has been identified in the new Export Control Classification Numbers (ECCNs) included in this proposed rule. Thus, the scope of the items described in this proposed rule is essentially commercial items widely available in retail outlets and less sensitive military items.

BIS has created ECCNs, referred to as the "600 series," to control items that would be removed from the USML and controlled under the CCL, or items from the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies Munitions List (Wassenaar Arrangement Munitions List or WAML) that are already controlled elsewhere on the CCL.

These ECCNs are referred to as the "600 series" because the third character in each of the new ECCNs is "6." The first two characters of the "600 series" ECCNs serve the same function as any other ECCN as described in §738.2 of the EAR. The first character is a digit in the range 0 through 9 that identifies the Category on the CCL in which the ECCN is located. The second character is a letter in the range A through E that identifies the product group within a CCL Category. With few exceptions, the final two characters identify the WAML category that covers items that are the same or similar to items in a particular "600 series" ECCN. Category II of the USML and category ML2 of the WAML cover large caliber guns and other military weapons such as: Howitzers, cannon, mortars, anti-tank weapons, projectile launchers, military flame throwers and recoilless rifles.

In this proposed rule, items that are currently controlled in Category II of the USML would be controlled on the CCL under four new "600 series" ECCNs. Placement of the items currently in USML Category II into the CCL's 600 series would be consistent with existing BIS practice of using 600 series ECCNs to control items of a military nature.

Items currently controlled in Categories I and III of the USML would be controlled in new ECCNs in which the third character is a "5." These items are not appropriate for 600 series control because, for the most part, they have civil, recreational, law enforcement, or other non- military applications. As with 600 series ECCNs, the first character would represent the CCL category, the second character would represent the product group, and the final two characters would represent the WAML category that covers items that are the same or similar to items in the ECCN.

DDTC's proposed rule detailed the specific changes to the ITAR, including:

Revision of Category I

This proposed rule revises USML Category I, covering firearms and related articles, to control only defense articles that are inherently military or that are not otherwise widely available for commercial sale. In particular, the revised category will not include non-automatic and semi-automatic firearms to caliber .50 (12.7mm) inclusive, currently controlled under paragraph (a), and all of the parts, components, accessories, and attachments specially designed for those articles. Such items will be subject to the new controls in Export Control Classification Numbers 0A501, 0A502, 0A503, 0A504, 0A505, 0B501, 0B505, 0D501, 0D505, 0E501, and 0E502. Such controls in Category 0 of the CCL will be published in a separate rule by the Department of Commerce.

Paragraph (a) of USML Category I will cover firearms that fire caseless ammunition. Paragraph (b) will continue to cover fully automatic firearms to caliber .50 (12.7mm) inclusive. Paragraph (c) will cover firearms specially designed to integrate fire control, automatic tracking, or automatic firing systems, and all weapons previously described in paragraph (c) that remain on the USML will be covered by paragraph (a), (b) or (c) of this category or by Category II. Paragraph (d) will cover fully automatic shotguns. Paragraph (e) will continue to cover silencers, mufflers, sound suppressors, and specially designed parts and components; flash suppressors will be subject to the EAR. Paragraph (f) will be reserved, as riflescopes and other firearms sighting devices may be controlled in USML Category XII if they have night vison or infrared capabilities, and other riflescopes will be subject to the EAR. Paragraph (g) will continue to cover barrels, receivers (frames), bolts, bolt carriers, slides, or sears, specially designed for the firearms in Category I. Paragraph (h) will cover high capacity (greater than 50 rounds) magazines, and parts and components to convert a semi-automatic firearm into a fully automatic firearm, and accessories or attachments specially designed to automatically stabilize aim (other than gun rests) or for automatic targeting. Paragraph (i) will continue to cover the technical data and defense services.

A new (x) paragraph will be added to USML Category I, allowing ITAR licensing for commodities, software, and technology subject to the EAR, provided those commodities, software, and technology are to be used in or with defense articles controlled in USML Category I and are described in the purchase documentation submitted with the license application.

The note to Category I will be retained, with conforming revisions. A new second note will be added to clarify the terms "firearm," "fully automatic," and "caseless ammunition".

Revision of Category II

This proposed rule revises USML Category II, covering guns and armament, establishing a bright line between the USML and the CCL for the control of these articles. Most significantly, paragraph (j), controlling parts and components, will be revised to enumerate the articles controlled therein.

Paragraph (a) will be revised to enumerate the articles controlled in that paragraph. The articles currently covered in paragraph (c) (apparatus and devices for launching or delivering ordnance) still warranting control on the ITAR will be included in new paragraph (a)(4). A new paragraph (a)(5) will be added for developmental guns and armaments funded by the Department of Defense and the specially designed parts and components of those developmental guns and armaments. The articles currently controlled in paragraph (f), engines for self-propelled guns and howitzers in paragraph (a), will be on the CCL in ECCN 0A606. Tooling and equipment for the production of articles controlled in USML Category II, currently in paragraph (g), will be on the CCL in ECCN 0B602. Test and evaluation

equipment, currently in paragraph (h), will be on the CCL in ECCN 0B602. Certain autoloading systems controlled in paragraph (i) will be moved to paragraphs (j)(9) and (11).

A new (x) paragraph will be added to USML Category II, allowing ITAR licensing for commodities, software, and technology subject to the EAR, provided those commodities, software, and technology are to be used in or with defense articles controlled in USML Category II and are described in the purchase documentation submitted with the application.

Revision of Category III

This proposed rule revises USML Category III, covering ammunition and ordnance, to establish a bright line between the USML and the CCL for the control of these articles and to be consistent with the changes to Category I.

Most significantly, paragraphs (a) and (d) will be revised to remove broad catch-alls and enumerate the articles to be controlled therein. For example, paragraph (a), which controls ammunition for articles in USML Categories I and II, will be revised to specifically list the ammunition that it controls. A new paragraph (a)(10) will be added for developmental ammunition funded by the Department of Defense and the parts and components specially designed for such developmental ammunition. Ammunition not enumerated in paragraph (a) will be subject to the EAR. Likewise, revised paragraph (d), which controls parts and components, will enumerate the articles it controls; those articles not identified but currently captured via the catch-all will be subject to the EAR.

Additionally, paragraph (c), which controls production equipment and tooling, will be removed and placed into reserve. The articles currently covered by this paragraph will be subject to the EAR.

A new (x) paragraph will be added to USML Category III, allowing ITAR licensing for commodities, software, and technology subject to the EAR, provided those commodities, software, and technology are to be used in or with defense articles controlled in USML Category III and are described in the purchase documentation submitted with the application.

Conforming ITAR Changes

Additionally, conforming changes will be made to several sections of the ITAR that refer to the current controls in USML Category I(a). These sections will be amended because they all refer to firearms that will be controlled on the CCL. Section 123.16(b)(2) will be revised to remove reference to the firearms exemptions at §123.17(a) through (e), which describe the firearms exemptions, because the paragraphs will be removed as a consequence of the control of non-automatic and semi-automatic firearms on the CCL. For the same reason, §123.16(b)(6) will be revised to describe only the remaining exemption at §123.17 (personal protective gear), and §123.16(b)(7) will be reserved. §123.17 will be amended to remove paragraphs (a) through (e), consistent with changes made to the USML. Section 123.18, as it describes exemptions for firearms that will be controlled for export by the Department of Commerce, will be removed and placed into reserve. Revision of §124.14(c)(9) will remove the example of "sporting firearms for commercial resale." The policy guidance on Zimbabwe in §126.1(s) will be revised to remove reference to the firearms exemption in §123.17.

Section 129.1(b) of the ITAR will be revised to clarify that the regulations on brokering activities in part 129 apply to those defense articles and defense services designated as such on the USML and those items described on the USMIL (27 CFR 447.21). Section 129.4 of the ITAR will also be revised to clarify brokering requirements for items on the USMIL that are subject to the brokering requirements of the AECA. The items that will move to the CCL for export control purposes, yet are in the USMIL for permanent import purposes, remain subject to the brokering requirements of part 129 with respect to all brokering activities, including facilitation in their manufacture, export, permanent import, transfer, reexport, or retransfer. The revisions also clarify that foreign defense articles that are on the USMIL require brokering authorizations.

Request for Comments for Military Items

BIS also sought public comments to perform a complementary review of items on the Commerce Control List concurrent with the Department of State's review of the controls implemented in its recent revisions of parts of the United States Munitions List (which control explosives and energetic materials, propellants, incendiary agents and their constituents; personal protective equipment; and military electronics), to ensure that the descriptions of these items on the CCL are clear, items for normal commercial use are not inadvertently controlled as military items on the USML, technological developments are accounted for on the control lists, and controls properly implement the national security and foreign policy objectives of the United States. This Notice of Inquiry also furthers the regulatory reform agenda directed by the President in Executive Order 13777. Comments must be received by BIS no later than April 13, 2018.

Specifically, BIS is solicited comments on the clarity, usability and any other matters related to implementation of the "600 series" ECCNs that control the following items, as well as certain items related thereto: energetic materials (ECCNs 1B608, 1C608, 1D608 and 1E608); armored and protective "equipment" (ECCNs 1A613, 1B613, 1D613, 1E613); military electronics (ECCNs 3A611, 3B611, 3D611 and 3E611); and cryogenic and superconducting equipment (ECCNs 9A620, 9B620, 9D620 and 9E620).

A core element of the transfer of certain articles on the USML to "600 series" ECCNs on the CCL has been the streamlining of categories on the USML, resulting in the control on the CCL of items that the President determines do not warrant USML control. On December 10, 2010, the Department of State provided notice to the public of its intent to revise the USML to create a more "positive list" that describes controlled items using, to the extent possible, objective criteria rather than broad, open-ended, subjective, or design intent-based criteria (see 75 FR 76935). As a practical matter, this meant revising USML categories so that, with some exceptions, the descriptions of defense articles that continued to warrant control under the USML did not use catch-all phrases to control unspecified items. With limited exceptions, the defense articles that warranted control under the USML were those that provided the United States with a critical military or intelligence advantage. All other items were to become subject to the export licensing jurisdiction of the EAR. Since that time, the Department of State has published final rules setting forth revisions for eighteen USML categories, each of which has been reorganized into a uniform and more "positive list" structure. In coordination with the Department of State, the Department of Commerce has published final rules that made corresponding revisions to the CCL by controlling items that the President has determined do not warrant control on the USML.

The advantage of revising the USML into a positive list is that its controls can be tailored to satisfy the national security and foreign policy objectives of the U.S. Government by maintaining control over those defense articles that provide a critical military or intelligence advantage, or otherwise warrant control under the ITAR, without inadvertently controlling items in normal commercial use. However, this approach requires that the USML and the CCL be regularly reviewed and updated to account for the following: technological developments; issues identified by exporters and reexporters involving the practical application of these controls; and changes in the military and commercial applications of items affected by the USML or by the corresponding "600 series" ECCNs on the CCL.

Consistent with the approach described above, this NOI requests public comments as part of a review of changes to the EAR that complements a similar review the Department of State is performing with respect to the ITAR. As discussed above, the Departments of State and Commerce reviews are being undertaken to follow up on sets of rules published by the Departments of State and Commerce. These rules implemented revisions to the following categories of the USML: Category V (explosives and energetic materials, propellants, incendiary agents and their constituents), effective July 1, 2014 (see 79 FR 34); Category X (protective personnel equipment), effective July 1, 2014 (see 79 FR 34); and Category XI (military electronics), effective December 30, 2014 (see 79 FR 37536). These rules also added the following "600 series" ECCNs to the CCL: ECCNs 1B608, 1C608, 1D608, 1E608, 1A613, 1B613, 1D613 and 1E613, effective July 1, 2014 (see 79 FR 264), and ECCNs 3A611, 3B611, 3D611, 3E611, 9A620, 9B620, 9D620 and 9E620, effective December 30, 2014 (see 79 FR 37551). The Department of State is seeking comments from the public on the condition and efficacy of the revised Categories V, X, and XI and whether they are meeting the objectives for the list revisions. BIS will make any changes to the CCL that it determines are necessary to complement revisions to the USML by the Department of State. In addition, through this NOI, BIS is independently seeking comments on how to improve the implementation of these "600 series" ECCNs on the CCL.

BIS also sought comments on potential cost savings to private entities from shifting control of specific commercial items from USML to the CCL. To the extent possible, please quantify the cost of compliance with USML control of commercial items, to include the time saved, the reduction in paperwork, and any other cost savings for a particular change.

The Department of State also requested comments from the public to inform its review of the controls implemented in recent revisions to Categories V, X, and XI of the United States Munitions List (USML). The Department periodically reviews USML categories to ensure that they are clear, do not inadvertently control items in normal commercial use, account for technological developments, and properly implement the national security and foreign policy objectives of the United States. The Department will accept comments on the Notice of Inquiry up to April 13, 2018.

The Department requested public comment on USML Categories V, X and XI. Commenters were encouraged to provide comments that are responsive specifically to the prompts set forth below:

1. Emerging and new technologies that are appropriately controlled by one of the referenced categories, but which are not currently described in subject categories or not described with sufficient clarity.
2. Defense articles that are described in subject categories, but which have entered into normal commercial use since the most recent revisions to the category at issue. For such comments, be sure to include documentation to support claims that defense articles have entered into normal commercial use.
3. Defense articles for which commercial use is proposed, intended, or anticipated in the next 5 years.
4. Drafting or other technical issues in the text of all of the referenced categories.
5. Comments regarding USML Category XI paragraph (b) modification.
6. Potential cost savings to private entities from shifting control of specific commercial items from USML to the Export Administration Regulations. To the extent possible, please quantify the cost of compliance with USML control of commercial items, to include the time saved, the reduction in paperwork, and any other cost savings for a particular change.

The Department will review all comments from the public. If a rulemaking is warranted based on the comments received, the Department will respond to comments received in a proposed rulemaking in the Federal Register.

Section 301 China Tariffs

On August 18, 2017, the Office of the United States Trade Representative (USTR) initiated an investigation under Section 301 of the Trade Act of 1974 into the government of China's acts, policies, and practices related to technology transfer, intellectual property, and innovation. Based on this investigation, the USTR imposed additional import duties on three lists of Chinese products based on the HTS codes of these products. These tariffs, implemented in three rounds (so far), impact a wide range of goods and are at different places in their implementation. We have provided below a summary of the different tariff actions and some potential options available to reduce the impact of the tariffs on U.S. importers.

Round 1

- Total import value of $34 billion
- 25% ad valorem duty
- Impacted items in Annex B to 83 FR 28710
- Became effective July 6, 2018

Round 2

- Total import value of $16 billion
- 25% ad valorem duty
- Impacted items in Annex C to 83 FR 28710
- Became effective August 23, 2018

Round 3

- Total import value of $200 billion
- 10% ad valorem duty (will be increased to 25% on March 2, 2019)
- Impacted items in 83 FR 55608
- Became effective September 24, 2018

Round 4?

- The Trump administration announced on September 17, 2018, that if China "takes retaliatory action against our farmers or other industries" it will initiate a process aimed at increasing tariffs on an additional $267 billion worth of goods from China, but nothing further has been announced.

Under the Notice of Modification of Action providing for the imposition of additional import duties on a third list of Chinese products published on September 21, 2018 (Round 3), USTR announced changes to heading 8517.62, which have had a significant impact on our clients. These changes include:

- 8517.62.0050 was removed from HTSUS subheading 8517.62.00;
- 8517.62.0020 was added to HTSUS subheading 8517.62.00 for "Switching and Routing Apparatus."
- 8517.62.0090 was also added to HTSUS subheading 8517.62.00 as a residual classification for "Other" apparatus.

Importers have had to decide if their products classified under HTS 8517.62.0050 are now under 8517.62.0020 as switching and routing apparatus, and subject to the additional tariffs, or under 8517.62.0090, which is exempt from the Section 301 tariffs. We are now seeing Customs rulings classifying imports under these two classifications.

In general, companies impacted by these new tariffs have several options to help reduce the impact, including:

- Adjust supply chain operations such that the items are substantially transformed in a country other than China, prior to their import into the United States.
- Import sub-assemblies, rather than finished products, if those sub-assemblies have an HTS classification not impacted by the new tariffs. Perform final assembly in the United States after importation.
- For any new developments to the tariff lists, submit comments to the USTR requesting that particular proposed HTS codes be removed from the final list, or submit a request to the USTR that particular products be excluded from the tariffs once the final list has been published.
- For products that are imported into the United States for future export, utilize a bonded warehouse or a drawback program.

2018 Sanctions Update

There were several changes to U.S. sanctions programs this year, most of which expand the sanctions programs, including Iran, Russia and Venezuela. Below is a summary of the noteworthy changes:

Iran

On May 8, President announced his decision to cease the United States' participation in the Joint Comprehensive Plan of Action (JCPOA), and to begin re-imposing the U.S. nuclear-related sanctions that were lifted to effectuate the JCPOA sanctions relief, following a wind-down period. In conjunction with this announcement, the President issued a National Security Presidential Memorandum (NSPM) directing the U.S. Department of the Treasury and other Departments and Agencies to take the actions necessary to implement his decision.

The JCPOA implementation in January 2016 lifted selective nuclear-related secondary sanctions, financial and banking related sanctions, as well as sanctions related to insurance, Iran's energy and petrochemicals sectors, Iran's shipping and shipbuilding sectors, gold and other precious metals, and Iran's automotive sectors.

According to **OFAC's Press Release** in May, Departments and Agencies began the process of implementing 90-day and 180-day wind-down periods for activities involving Iran that were consistent with the U.S. sanctions relief specified in the JCPOA. Now that the wind-down periods are completed, the applicable sanctions have come back into full effect, and OFAC revoked or amended, as appropriate, general and specific licenses issued in connection with the JCPOA.

Some of the significant changes that resulted from the re-imposition of sanctions include:

1. OFAC revoked General License H, which previously had permitted foreign-organized companies owned or controlled by U.S. persons to engage in certain dealings with Iran. This makes Iran and Cuba the only sanctions programs that treats foreign subsidiaries of a U.S. company as a U.S. person.
2. OFAC also re-imposed secondary sanctions targeting critical Iranian industries; and
3. OFAC re-designated hundreds of Iranian parties on OFAC's List of Specially Designated Nationals and Blocked Persons

OFAC also published **FAQs** in May covering the re-imposition of the secondary sanctions.

Even with the news about the U.S. exit from the JCPOA, OFAC highlighted existing guidance to underscore the U.S. Government's ongoing commitment to ensure that the Iranian people can exercise their universal right to freedom of expression and can freely access information via the Internet. OFAC's guidance, authorizations, and licensing policies support the Administration's continued commitment to promote the free flow of information to citizens of Iran - which the Iranian regime has consistently denied to its people.

OFAC continues to foster and support the free flow of information to the Iranian people through the following authorizations and licensing policies:

- *General Licenses*. OFAC has two Iran-related general licenses that authorize the provision of certain hardware, software, and services incident to the exchange of personal communications over the Internet, such as instant messaging, chat and email, and social networking software and services, as well as certain apps for mobile operating systems, anti-censorship tools, anti-tracking software, mobile phones, and other devices.
    - Section 560.540 of the Iranian Transactions and Sanctions Regulations (ITSR), 31 C.F.R. Part 560, authorizes the exportation from the United States or by U.S. persons, wherever located, to persons in Iran of certain publicly available, no-cost services incident to the exchange of personal communications over the Internet and certain publicly available, no-cost software necessary to enable such services.
    - General License D-1 (GL D-1), which is broader than the general license in section 560.540 of the ITSR, authorizes the export and reexport of fee-based services and software incident to the exchange of personal communications over the Internet, as well as the export, reexport, or provision of certain software and hardware incident to personal communications. The Annex to GL D-1 provides a list of services, software, and hardware that are considered "incident to personal communications" and eligible for export or reexport to Iran under this general license.
- *Guidance*. OFAC has provided extensive guidance on its website on these general licenses, including " Interpretive Guidance and a Statement of Licensing Policy on Internet Freedom in Iran " (describing the authorization in Section 560.540 of the ITSR and OFAC's policy for reviewing specific licenses in this area) and multiple "Frequently Asked Questions" (FAQs) on GL D-1 (FAQs 337-348 and FAQs 434-443).
- *Licensing Policies*. OFAC will consider applications to provide products and services outside the scope of these authorizations on a case-by-case basis based on U.S. foreign policy and national security interests. Section 560.540 includes a specific licensing policy for the export of other services and software

incident to information-sharing over the Internet, subject to certain conditions. Additionally, GL D-1 also includes a specific licensing policy for the export of other services, software, or hardware incident to personal communications that are outside the scope of the general license.

As the Iranian people seek to exercise their universal right to freedom of expression and continue to seek access to information via the Internet, OFAC remains committed to engaging with the private sector to provide guidance on the range of activities authorized by section 560.540 and GL D-1 of the ITSR. If you require assistance with interpreting the authorizations contained in section 560.540 and GL D-1 of the ITSR or assessing how they apply to your situation, or need guidance on how to apply for a specific license, please contact OFAC's Licensing Division online, by phone at 202-622-2480 , or by email at ofac_feedback@do.treas.gov.

Russia/Ukraine

OFAC and the State Department introduced additional sanctions against Russian individuals and entities, including the following actions throughout the year:

The President issued a new Executive Order (E.O.) "Authorizing the Implementation of Certain Sanctions Set Forth in the Countering Americas Adversaries Through Sanctions Act" to further the implementation of certain sanctions in the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA) with respect to the Russian Federation. In addition, the Secretary of State is taking two actions to implement his delegated authorities pursuant to section 231 of CAATSA and to further impose costs on the Russian Government for its malign activities.

First, the Secretary of State added 33 additional persons – a person is either an entity or an individual – to the CAATSA section 231 List of Specified Persons (LSP) for being a part of, or operating for or on behalf of, the defense or intelligence sectors of the Government of the Russian Federation. This action increases the number of persons identified on the LSP to 72. Any person who knowingly engages in a significant transaction with any of these persons is subject to mandatory sanctions under CAATSA section 231.

Second, in consultation with the Secretary of the Treasury, the Secretary of State imposed sanctions on the Chinese entity Equipment Development Department (EDD) and its director, Li Shangfu, for engaging in significant transactions with persons on the LSP. These transactions involved Russia's transfer to China of Su-35 combat aircraft and S-400 surface-to-air missile system-related equipment.

According to the **Press Release**, Section 231 of CAATSA and these actions are not intended to undermine the military capabilities or combat readiness of any country, but rather to impose costs on Russia in response to its interference in the United States election process, its unacceptable behavior in eastern Ukraine, and other malign activities. These actions further demonstrate the Department of State's continuing commitment to fully implement CAATSA section 231, which has already deterred billions of dollars-worth of potential arms exports from Russia. State encourages all persons to avoid engaging in transactions with entities on the LSP that may risk sanctions, including high-value, major transactions for sophisticated weapons systems.

OFAC, in consultation with the State Department, designated seven Russian oligarchs and 12 companies they own or control, 17 senior Russian government officials, and a state-owned Russian weapons trading company and its subsidiary, a Russian bank. These actions were pursuant to authority provided under E.O. 13661 and E.O. 13662, authorities codified by CAATSA, as well as E.O. 13582. These actions follow the Department of the Treasury's issuance of the CAATSA Section 241 report in late January. In the Section 241 report, Treasury identified senior Russian government officials and oligarchs. These actions target a number of the individuals listed in the Section 241 report, including those who benefit from the Putin regime and play a key role in advancing Russia's malign activities.

These actions also include the designation of two entities and six individuals pursuant to section 224 of CAATSA, which targets cyber actors operating on behalf of the Russian government. The CAATSA listing includes the Federal Security Service (FSB), a Russian intelligence organization, knowingly engages in significant activities that undermine cybersecurity on behalf of the Russian government. Specifically, the FSB has utilized its cyber tools to

target Russian journalists and politicians critical of the Russian government; Russian citizens and government officials; former officials from countries bordering Russia; and U.S. government officials, including cyber security, diplomatic, military, and White House personnel. Additionally, in 2017, the U.S. Department of Justice indicted two FSB officers for their involvement in the 2014 hacking of Yahoo that compromised millions of Yahoo accounts. OFAC previously sanctioned the FSB under E.O. 13694, as amended, on December 28, 2016.

The State Department also implemented the plans that it **announced** to impose Chemical and Biological Weapons Control and Warfare Elimination Act sanctions on Russia ("CBW Act"). The sanctions are in response to a determination by the U.S. government that the Russian government used "Novichok", a nerve agent, in an attempt to assassinate UK citizen Sergei Skripal and his daughter Yulia Skripa. The sanctions under the CBW act are implemented in two phases. The State Department has imposed the first round of sanctions through notice in the **Federal Register** after a 15-day review period. These sanctions include:

- a prohibition of exports of national security-sensitive goods and technology,
- the termination of foreign assistance,
- suspension of sales of defense articles or services, and
- the denial of credit or other financial assistance by the US government.

Based on the State Department's **background briefing** , we believe that the prohibition on the export of national security-sensitive goods and technology applies to items requiring an export license to Russia and not to items eligible for export under a license exception. From the background briefing:

We notified Congress today that pursuant to this act we intend to impose sanctions against the Russian Federation in a number of respects, the most significant of which is the imposition of a presumption of denial for all national security sensitive goods or technologies that are controlled by the Department of Commerce pursuant to the Export Administration Regulations. These goods are currently subject to a license – a case-by-case license determination, but we are – henceforth, when these sanctions go into effect, we will be presumptively denying such applications.

The second phase of the sanctions were scheduled to be implemented on approximately November 8th . The second phase was to be imposed if the executive branch cannot certify that Russia: (a) is no longer using chemical or biological weapons, (2) has provided reasonable assurances that it will not in the future use such weapons, and (3) that on-site inspections or other reliable means can be used to verify compliance. The State Department told law makers in November that Russia did not meet these certifications.

Under the CBW Act, the President must impose 3 of the following 6 sanctions:

- Further export restrictions including a prohibition on exports to Russia of all other goods and technology (excluding food and other agricultural commodities and products).
- Import restrictions on articles that are the growth, product, or manufacture of Russia.
- Prohibiting U.S. banks from making any loan or providing any credit to the government of Russia, except for loans or credits for the purpose of purchasing food or other agricultural commodities or products.
- Downgrading or suspending diplomatic relations between the United States and the government of Russia.
- Suspending air carriers owned by the government of Russia from transporting to or from the United States and terminating any air service agreement between the United States and Russia (with an exception for emergencies.

The State Department noted that it was looking at carve outs and waivers for the second phase of sanctions. The carve outs will be a policy of case by case licensing, rather than a presumption of denial for licenses for:

- the provision of foreign assistance to Russia and to the Russian people,
- the safety of commercial passenger aviation,
- space flight activities,
- purely commercial end users for civilian end uses, and

- exports to wholly-owned subsidiaries of U.S. companies and other foreign companies in Russia.

It is likely that if the President must impose the second set of sanctions, he will impose the least restrictive ones: opposing multilateral bank loans, prohibiting U.S. bank loans, and downgrading diplomatic relations.

These developments in 2018 suggest that the U.S. government intends to continue to pursue economic sanctions against Russia, and U.S. companies will face significant Russian sanctions risks.

Sudan

OFAC has removed from the Code of Federal Regulations the Sudanese Sanctions Regulations as a result of the revocation of certain provisions of one Executive Order and the entirety of another Executive Order on which the regulations were based. OFAC also amended the Terrorism List Government Sanctions Regulations to incorporate a general license authorizing certain transactions related to exports of agricultural commodities, medicines, and medical devices, which has, until now, appeared only on OFAC's website.

U.S. persons and non-U.S. persons will still need to obtain any licenses required by BIS to export or reexport to Sudan certain items (commodities, software, and technology) that are on the Commerce Control List of the EAR.

There are some exemptions for narrow cases. For example, items designated as EAR99 are outside of the scope of BIS's licensing requirements to Sudan. There are also some License Exceptions available for exports to Sudan, including License Exception CCD, which authorizes the export of certain mass-market communications-related devices to Sudan.

The removal of OFAC-administered sanctions on Sudan will have a greater impact on businesses that either do not export controlled products, that only operate a service from the United States (e.g., a cloud-based web service), or that are foreign companies reexporting certain U.S.-origin items.

North Korea

The U.S. Department of State, along with OFAC and other U.S. Government agencies issued an advisory to highlight sanctions evasions tactics used by North Korea that could expose businesses – including manufacturers, buyers, and service providers – to sanctions compliance risks under U.S. and/or United Nations sanctions authorities. This advisory also assists businesses in complying with the requirements under Title III, the Korean Interdiction and Modernization of Sanctions Act of CAATSA. According to the advisory, businesses should be aware of deceptive practices employed by North Korea in order to implement effective due diligence policies, procedures, and internal controls to ensure compliance with applicable legal requirements across their entire supply chains.

The Guidance:

1. Clarifies that the US is not seeking to disrupt the efforts of North Korean refugees and asylum seekers and says that if North Koreans gain another citizenship they are no longer considered North Korean for purposes of US sanctions, in particular, Title III, the Korean Interdiction and Modernization of Sanctions Act of the Countering America's Adversaries through Sanctions Act;
2. Provides a list of industries and countries in which North Korean laborers working on behalf of the North Korean Government were present in 2017-18 (at page 3). While the list of countries is long, it at least narrows somewhat the supply chain sourcing concerns to certain parts of Asia, Africa, and the Middle East;
3. Provides in Annex 3 a sectoral breakdown of where North Korean laborers are working on behalf of the North Korean Government overseas by sector. While Annex 3 states that it is NOT a comprehensive list of all countries, jurisdictions and industries, it is helpful in highlighting some higher risk jurisdictions by sector. For example, the Information Technology sector is warned about Angola, Bangladesh, China, Laos, Nigeria, Uganda, and Vietnam; and

4. Provides in Annex 2 a list of joint ventures that have operated or are currently operating in North Korea established prior to 2016, organized by industry sector. Again, this is not a comprehensive list, nor is it an SDN or blocked parties list, but it is a list that companies evaluating suppliers in Asia and China in particular may wish to check as they evaluate potential suppliers.

The full document can be found on **OFAC's website**.

Additional Regulatory Updates

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

Wassenaar Arrangement Implementation

BIS published amendments to the EAR to include changes agreed upon by the Wassenaar Arrangement at the 2017 Plenary meeting advocating implementation of effective export controls on strategic items. We have included several noteworthy changes to the EAR, highlighted below.

Changes to Category 2: Materials Processing

2B007. This control on in paragraph .a on "[Robots] capable in real-time of full three-dimensional image processing or full three-dimensional "scene analysis" to generate or modify "programs" or to generate or modify numerical program data" is removed and reserved because of insufficient connection to military capabilities. Robots of national security concern are controlled under 2B007.b, .c and .d.

Changes to Category 3: Electronics

3A001.a.5.a . This control on analog-to-digital converters (ADCs) is revised. The ADC control thresholds were not updated, but there were amendments to the language and definitions in the control parameters and corresponding technical notes.

3A002. The frequency parameter for electronic assemblies is raised from "exceeding 10 MHz" to "exceeding 40 MHz" for certain signal analyzers. BIS estimates that this change will reduce the annual license application submissions.

Changes to Category 4: Computers

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 16 to 29 Weighted TeraFLOPS (WT) in Items paragraph 4A003.b.

4D001 "Software" and 4E001 "Technology" are amended as follows:

1. The TSR paragraph in the List Based License Exceptions section is revising the APP from 16 to 29 WT, and
2. Items paragraph .b.1 in the List of Items Controlled section is amended by revising the APP from 8.0 to 15 WT.

Changes to Category 5, Part 1: Telecommunications

5A001.d**.** The control on 'electronically steerable phased array antennae' is revised to include the following exclusion note, as phased array antennae are increasingly being developed for civil telecommunications applications, including cellular, WLAN, 802.15, and wireless HDMI:

Note 2: 5A001.d does not apply to antennae specially designed for any of the following:

a. Civil cellular or WLAN radio-communications systems;
b. IEEE 802.15 or wireless HDMI; or
c. Fixed or mobile satellite earth stations for commercial civil telecommunications.

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.

Changes to Category 5, Part 2: Information Security

5A002**.** 5A002 is amended to clarify controls on products with dormant encryption. The revision clarifies that an item is controlled if:

1. the 'cryptography for data confidentially' is usable from the beginning regardless of "cryptographic activation" (i.e., not dormant),
2. the cryptographic capability was previously dormant but is now usable (whether by "cryptographic activation" or by other means; or
3. the "cryptographic activation" mechanism is not secure (i.e., the cryptographic capability is not securely kept dormant).

Changes to Category 6: Sensors and Lasers

6A008**.** This control on Radar systems, equipment and assemblies is amended by replacing "steerable array antennas" with "scanned array antennae" as well as adding a Technical Note to make people aware that electronically scanned array antennae are also known as electronically steerable array antennae. This revision uses more current, and standard, language to describe E-scan radar.

In total, 50 ECCNs were 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:

- 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.
- Review the updates on "dormant" encryption items to determine whether your classifications for dormant encryption items and cryptographic activation mechanisms are consistent with the regulatory clarifications.

Australia Group Implementation

BIS also published a final rule amending the EAR to implement the recommendations presented at the February 2017 Australia Group (AG) Intersessional Implementation Meeting, and later adopted pursuant to the AG silent approval procedure, and the recommendations made at the June 2017 AG Plenary Implementation Meeting and adopted by the AG Plenary.

The changes to the EAR include:

- Removal of Chemical/Biological CB2 controls on India;

- New controls at ECCN 2B350.c for certain prefabricated repair assemblies for designed for glass-lined reaction vessels and reactors controlled under 2B350.a or glass-lined storage tanks, containers and receivers controlled under 2B350.c;
- Expands ECCN 2B351 (Toxic Gas Monitoring Systems) to cover certain portable toxic gas monitors (e.g., small handheld detectors) and other monitors;
- New interpretive note for ECCN 2B352.b.1 fermenters, stating the "total internal volume" of the fermenter must be measured to determine whether it exceeds 20 liters.
- New controls at ECCN 2B352.j to cover certain nucleic acid assemblers and synthesizers;
- New controls at ECCN 1C350 on precursor chemical hydrochloride salt (C.A.S. #41480–75–5) N,N-Diisopropylaminoethanethiol hydrochloride.
- ECCN 1C353 (Genetic Elements and Genetically Modified Organisms) was rewritten;
- Technical corrections to ECCN 1C351;
- Reduction in the 45-day advance export notification requirement for 5 milligrams or less of saxitoxin (for medical or diagnostic purposes only) to a 3-day notice.

There is also a savings clause applicable to "deemed exports" of technology or source code that, because of this new rule, creates a new license requirement. Exporters may continue to release such items to a foreign person under the previous authorization (i.e., license exception or NLR) until May 17, 2018.

Missile Technology Control Regime Implementation

BIS also published a final rule amending the EAR to reflect changes to the Missile Technology Control Regime (MTCR) Annex that were agreed to by MTCR member countries at the October 2017 Plenary in Dublin, Ireland, and the May 2017 Technical Experts Meeting (TEM) in Stockholm, Sweden. This final rule revises seventeen ECCNs 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.

The Missile Technology Control Regime is an export control arrangement among 35 nations, including most of the world's suppliers of advanced missiles and missile-related equipment, materials, software and technology. The regime establishes a common list of controlled items (the Annex) and a common export control policy (the Guidelines) that member countries implement in accordance with their national export controls. The MTCR seeks to limit the risk of proliferation of weapons of mass destruction by controlling exports of goods and technologies that could make a contribution to delivery systems (other than manned aircraft) for such weapons.

This final rule revises the EAR to reflect changes to the MTCR Annex agreed to at the October 2017 Plenary in Dublin, Ireland, and changes resulting from the May 2017 Technical Experts Meeting in Stockholm, Sweden. This rule also makes changes to the Commerce Control List to conform with the MTCR Annex. All of the changes in this final rule align the MT controls on the CCL with the MTCR Annex.

The ECCNs affected by this rule include 1B117, 1B118, 1C111, 1C118, 2B109, 2B120, 2B121, 2B122, 6A107, 7A105, 7A107, 7A116, 9A012, 9A101, 9A115, 9A515, 9A610.

License Requirements based on Nuclear Suppliers Group Agreements

BIS also implemented a final rule amending the EAR to impose a license requirement on exports and reexports of specified target assemblies and components for the production of tritium under new ECCN 1A231, and for the related "production" technology for 1A231 commodities covered under ECCNs 1E001 and 1E201. The items identified in this rule are controlled for nuclear nonproliferation (NP) Column 1 and anti-terrorism (AT) Column 1 reasons. These new classifications are the result of a U.S. Government proposal submitted and agreed to by members of the relevant multilateral regime, the Nuclear Suppliers Group (NSG), in June 2017. This final rule, as required under the 0Y521 procedure and in fulfillment of multilateral commitments, implements the multilateral control for the items adopted by the NSG.

BIS Eases Restrictions on Exports to India

BIS amended the EAR to formally recognize and implement India's membership in the Wassenaar Arrangement. Further, BIS removes India from Country Group A:6 and places it in Country Group A:5. This action befits India's status as a Major Defense Partner and recognizes the country's membership in three of the four export control regimes: Missile Technology Control Regime, Wassenaar and Australia Group. This rule is another in the series of rules that implement reforms to which the United States and India mutually agreed to promote global nonproliferation, expand high technology cooperation and trade, and ultimately facilitate India's full membership in the four multilateral export control regimes (Nuclear Suppliers Group, MTCR, WA, and AG). This rule also makes conforming amendments.

BIS Increases Restrictions on Export to South Sudan

BIS also amended the EAR to conform to the Department of State's amendment of February 14, 2018 to the ITAR that placed restrictions on exports of defense articles (and defense services) to the Republic of South Sudan (South Sudan). The State action reflected a policy determination by the Secretary of State that it was in the best interests of U.S. foreign policy to impose such restrictions. Consistent with the State action, in this amendment, BIS updated the EAR to restrict the export and reexport of certain items on the Commerce Control List to South Sudan. Pursuant to established procedure, BIS added South Sudan to the list of U.S. embargoed countries under Country Group D:5-U.S. Embargoed Countries, a list drawn from the list of arms embargoes in the ITAR and State Federal Register notices, and adopts a restrictive license application review policy consistent with State's review policy set forth in the ITAR.

Enforcement Actions

There were some significant enforcement actions in 2018. The ZTE case was settled this year, and resulted in more than a $1 billion fine and other compliance measures. BIS also issued the largest civil penalty to be paid by an individual in BIS history. There were also penalties assessed to companies for a failure in third-party screening software, as well as a failure to screen against entities blocked under OFAC's "50% rule." We have included a summary of these cases, below. Additional resources can be found on the BIS, OFAC and DOJ websites:

- 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 7 penalties and settlements in 2018 for a total of $71,510,561.
- 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 January of this year.

In Appendix A, we have also included a summary other enforcement actions that occurred during 2018.

ZTE Enforcement Update

On July 13, 2018, the Bureau of Industry and Security (BIS) lifted its Denial Order on ZTE Corporation and ZTE Kangxun allowing these entities to receive US-origin goods and services. The other ZTE entities subject to the enforcement action, ZTE Parsian (Iran) and Beijing 8-Star International Co. (China), remained restricted parties. This Denial Order lifting is pursuant to a settlement agreement reached by BIS and ZTE, where ZTE agreed, among other things, to pay a $1 billion civil penalty for export control-related violations, deposit $400,000 in escrow, retain a team of special compliance coordinators, and completely replace its Board of Directors and senior leadership.

As way of background, in March 2017, after a five-year U.S. Government investigation, 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. ZTE agreed to a combined civil and criminal penalty and forfeiture of $1.19 billion after illegally shipping telecommunications equipment to Iran and North Korea, making false statements, and obstructing justice including through preventing disclosure to and affirmatively misleading the U.S. Government.

In addition to these monetary penalties, ZTE also agreed a seven-year suspended denial of export privileges, which could be activated if any aspect of the agreement was not met and/or if the company committed additional violations of the EAR.

The Department of Commerce then determined that ZTE made false statements to BIS in 2016, during settlement negotiations, and in 2017, during the probationary period, related to senior employee disciplinary actions the company said it was taking or had already taken. ZTE's false statements only were reported to the U.S. Government after BIS requested information and documentation showing that employee discipline had occurred.

As a result, BIS activated ZTE's Denial Order and placed the following restrictions on the company:

ZTE was unable to directly or indirectly, participate in any way in any transaction involving any commodity, software or technology exported or to be exported from the United States that is subject to the EAR, or in any other activity subject to the EAR, including:

- Applying for, obtaining, or using any license, license exception, or export control document;
- Carrying on negotiations concerning, or ordering, buying, receiving, using, selling, delivering, storing, disposing of, forwarding, transporting, financing, or otherwise servicing in any way, any transaction involving any item exported or to be exported from the United States that is subject to the Regulations, or engaging in any other activity subject to the Regulations; or
- Benefiting in any way from any transaction involving any item exported or to be exported from the United States that is subject to the Regulations, or from any other activity subject to the Regulations.

The Denial Order also included restrictions on any person acting on behalf of ZTE.

Largest Penalty Paid by Individual in BIS History

Eric Baird, the former owner and CEO of a Florida-based package consolidation and shipping service, has pleaded guilty to one count of felony smuggling and admitted to 166 administrative violations of U.S. export control laws as part of a global settlement with the U.S. Department of Justice and the U.S. Department of Commerce's Bureau of Industry and Security.

On December 12, 2018, Baird's criminal plea was accepted by a federal judge in the U.S. District Court for the Middle District of Florida, and BIS issued an Order outlining the administrative violations and imposing civil penalties of $17 million, with $7 million suspended, and a 5-year denial of export privileges, of which one year is suspended. **The civil penalty is the largest to be paid by an individual in BIS history**. In February 2017, Access USA settled with BIS and agreed to an administrative civil penalty of $27 million, with $17 million suspended.

As part of the administrative settlement, Baird admitted to violations of the Export Administration Regulations committed from August 1, 2011, through January 7, 2013, during his tenure as CEO of Access USA Shipping, LLC d/b/a MyUS.com (Access USA). Baird founded Access USA and developed its business model, which provided foreign customers with a U.S. address that they used to acquire U.S.-origin items for export without alerting U.S. merchants of the items' intended destinations. Under Baird's direction, Access USA developed practices and policies which facilitated concealment from U.S. merchants. Access USA would regularly change the values and descriptions of items on export documentation even where it knew the accurate value and nature of the items. Among the altered descriptions were some for controlled items listed on the Commerce Control List (CCL). For example, laser sights for firearms were described as "tools and hardware," and rifle scopes were described as "sporting goods" or "tools, hand tools."

Additionally, Baird established and/or authorized Access USA's "personal shopper" program. As part of this program, Access USA employees purchased items for foreign customers from a shopping list while falsely presenting themselves to U.S. merchants as the domestic end-users of the items. In some cases, Baird directed or authorized Access USA employees to use his personal credit card information, and in others Baird personally asked Access USA employees to apply for and use personal credit cards of their own to make such purchases and have the items sent to their personal addresses. As a result, in addition to being misled to believe that a domestic customer and end-user was involved when the items were in fact intended for export, the U.S. merchant would be misled to believe that Access USA itself was not involved in the transaction.

The activities that Baird knowingly authorized and/or participated in resulted in unlicensed exports of controlled items to various countries, as well as repeated false statements on Automated Export System (AES) filings. As early as September 2011, Baird was made aware that undervaluing violated U.S. export laws, including the EAR. In fact, Baird received e-mails on this subject from his Chief Technology Officer, who stated, "I know we are WILLINGLY AND INTENTIONALLY breaking the law." In the same email chain, Baird suggested that Access USA could falsely reduce the value of items by 25% on export control documentation submitted to the U.S. government and if "warned by [the U.S.] government," then the company "can stop ASAP."

Screening Failures Result in OFAC Penalties

Cobham Holdings, Inc. (Cobham), a company based in Arlington, Virginia, on behalf of its former subsidiary, Aeroflex/Metelics, Inc. (Metelics), has agreed to pay $87,507 to settle potential civil liability for three apparent violations of the Ukraine Related Sanctions Regulations, 31 C.F.R. part 589 (the URSR). Specifically, between July 31, 2014 and January 15, 2015, Metelics appears to have violated Section 589.201 of the URSR when it sold 3,400 LM 102202-Q-C-301 switch limiters, 6,900 MSW 2061-206 switches, and 20 silicon diode switch limiter samples through distributors in Canada and Russia to a person whose property and interests in property are blocked pursuant to Executive Order 13661 of March 17, 2014, “Blocking Property of Additional Persons Contributing to the Situation in Ukraine”.

Prior to December 14, 2015, Metelics was a subsidiary of Cobham, a global provider of technology and services in aviation, electronics, communications, and defense. During negotiations to sell Metelics, the purchaser identified a July 31, 2014 shipment of silicon diode switches and switch limiters to a Metelics distributor in Canada for end-use by Almaz Antey Telecommunications LLC (AAT) in Russia. Cobham investigated the shipment and discovered that in December 2014 and January 2015, Metelics made two additional shipments through a Russian distributor for end-use by AAT. **At all relevant times, although AAT was not explicitly identified on OFAC’s List of Specially Designated Nationals and Blocked Persons, it was 51 percent owned by Joint-Stock Company Concern Almaz-Antey (JSC Almaz-Antey), which OFAC had blocked and added to the SDN List on July 16, 2014, two weeks before the July 31, 2014 shipment**. As a result, AAT was blocked pursuant to §§ 589.201 and 589.406 of the URSR at the time Metelics engaged in the three shipments described below. These shipments arose out of two separate transactions – one taking place between June and July 2014, and the other taking place between October 2014 and January 2015.

On June 18, 2014, Metelics agreed to ship an order of 6,900 switches and 6,900 switch limiters through a Canadian distributor to AAT. The total value of the order was $1,123,182. On June 19, 2014, Metelics performed a denied party screening for the order that returned warnings for Russia generally but not AAT specifically, as JSC Almaz-Antey had not yet been added to the SDN List. Metelics did not have sufficient stock to fill the order, so it arranged to split the order into two shipments.

Metelics prepared the first shipment associated with the June 18, 2014 order for June 27, 2014 and performed nother denied party screening that day with similar results to the first screening. Knowing the shipment was destined for Russia, Metelics forwarded the end-use certificates to its Director of Global Trade Compliance to confirm that required compliance procedures had been followed and for final approval. After completing its global trade compliance review, Metelics shipped the first part of the order on June 27, 2014. The value of the shipment was $377,860. On July 16, 2014, OFAC designated JSC Almaz-Antey and added it to the SDN List.

Metelics prepared the second shipment on July 31, 2014 and again performed a denied party screening. **Although OFAC had designated JSC Almaz-Antey and added it to the SDN List approximately two weeks before, and despite the inclusion of two uncommon terms in the names of both the SDN and the specific end-user for the subject transaction (Almaz and Antey), Metelics' denied party screening produced no warnings or alerts for AAT. After the Director of Global Trade Compliance, in reliance on the results of the screening software, approved the transaction, Metelics shipped the second part of the order on July 31, 2014.** The total value of the second shipment was $745,322.

In October 2014, Metelics received an order for 10 samples of two different silicon diode switch limiters from a Russian distributor for end-use by AAT. On October 27, 2014, Metelics performed a denied party screening for the parties involved in the transaction (including AAT) which did not return any matches. Metelics subsequently shipped the samples in two separate shipments following the same procedures of performing a denied party search just prior to shipment and seeking approval from its Director of Global Trade Compliance (similar to the July 2014 transaction). The first shipment occurred on December 19, 2015 and the second on January 15, 2015. The value for each of these two shipments listed on the commercial invoices was $10. **Cobham determined that its screening software failed to generate an alert because JSC Almaz-Antey (the entity identified on the SDN List) did not include the word "telecom." The third-party screening software relied on by Cobham used an all word match criteria that would only return matches containing all of the searched words, even though Cobham had set the search criteria to "fuzzy" to detect partial matches. This meant that the software failed to match "Almaz Antey" when Cobham searched for "Almaz Antey Telecom."**

International Export Control Agreements and Regimes

Wassenaar Arrangement

The 24th Plenary Meeting of the Wassenaar Arrangement (WA) was held in Vienna on December 5 - 6, 2018. 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 2018, 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);
- continued work on export control lists, including:
    - adopted new export controls for quantum-resistant cryptography algorithms, air-launch platforms for space-launch vehicles, electromagnetic pulse (EMP)-resistant software, and explosives;
    - clarified existing controls for cryptographic activation, underwater sensors, pre-1946 aircraft engines, non-magnetic diesel engines, water tunnels, naval nuclear equipment, and production items for integrated circuits; and

  - relaxed controls for industrial Internet-of-Things, high-performance continuous-wave lasers, and infrared cameras, where performance thresholds were updated due to the fast evolution of the civil market.
- agreed to continue a comprehensive and systematic review of the WA Control Lists to ensure their ongoing relevance;
- approved new tools to further promote consistency among their licensing and enforcement authorities in the interpretation and application of the WA Control Lists;
- shared experiences in licensing and enforcement practices and discussed how to strengthen national export control implementation, including exchanging information on intangible transfer of technology (ITT) controls;
- considered a number of proposals for new best practices guidelines and identified other existing guidelines for updating as appropriate in 2019 as part of a regular review cycle;
- gave attention to measures to strength two-way engagement with industry, universities and the research community, including promotion of internal compliance programs;
- 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;
- 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.B.3.c.	- extra full stop deleted at the end of the para. (editorial)
1.C.1.a. Note 1	- new para. e. and new Technical Note for the local definition of 'open-cell foams'
1.C.10.d.1.a.	- full stop added after 1.C.8.a. (editorial)
Annex – "Explosives" List, entry 6	- hyphen added between FOX and 7 (editorial)
Category 2	
2.A.1. Note	- 2001 added after ISO 3290 - «G» added before 5
2.A.1.a.	- «or Class 2» added after Class 4
2.B.2.d.4.	- single quotation mark added to the end of the local definition (editorial)
2.B.3.	- entry amended including a cascaded structure for the control criteria
2.B.6.b.1.	- entry amended including a new Technical Note 2 for the local definition of 'measuring range'
Table – Deposition Techniques – Tech. Note b.4.	- full stop changed to a semi-colon at the end of the para. (editorial)
Category 3	
3.A., Note 2	- comma added after 3.A.1.a.14. to ensure that the description applies to ICs in all entries referenced (editorial)
3.A.	- new Note 3

Category/Item	Comments
3.A.1.a.	- Note 1 deleted (replaced by new Note 3 under 3.A.) - Note 2 renamed Note
3.A.1.a.2., Note	- «designed» added after integrated circuits
3.A.1.a.5.b.	- entry amended to avoid overlapping of the controls between 3.A.1.a.5.b.1. and 3.A.1.a.5.b.2. (editorial)
3.A.1.b., Technical Note 2	- deleted since the local definition of 'vacuum electronic devices' has become a global definition - Technical Note 1 renamed Technical Note
3.A.1.b.1. and Notes 1 & 2; 3.A.1.b.1.a., b., c., d. and Technical Note; 3.A.1.b.8.; 3.A.1.b.9.; 3.E.3.g.	- all instances of 'vacuum electronic device(s)' now have double quotation marks
3.A.1.b.2.b.1.	- space added between 10 and «W» (editorial)
3.A.1.b.2.b.2.	- space added between 5 and «W» (editorial)
3.A.1.b.3.f.	- new entry; - «or» moved from the end of 3.A.1.b.3.d. to the end of 3.A.1.b.3.e. (consequential change)
3.A.1.b.3., Note 1	- «in 3.A.1.b.3.a. through 3.A.1.b.3.e. » added after transistor
3.A.2.a.6.b.	- entry amended to clarify signal processing
3.A.2.d.5.	- entry expanded including sub-paras. a., b. and c. plus a Technical Note for the local definition of 'RF modulation bandwidth'
3.A.2.d.6.	- new entry - «or» moved from the end of 3.A.2.d.4.b. to the end of 3.A.2.d.5.c. (consequential change)
3.B.1.h.	- «having any of the following» is deleted
3.B.1.h.1.	- entry deleted; - former 3.B.1.h.2. becomes part of the 3.B.1.h. chapeau
3.D.5.	- new entry
Category 4	No amendments were made to Category 4
Category 5 – Part 1	
5.E.1.d.4.	- 0.1 nW – parameter written correctly (editorial)
Category 5 – Part 2	
5.A.2., N.B.	- "satellite navigation system" replaces Global Navigation Satellite Systems (GNSS)
5.A.2.a. & Technical Note 2; 5.A.2.a.4. 5.A.2.a., Note 2.a.1.a.1.b.	- 'described security algorithm' replaces 'in excess of 56 bits of symmetric key length, or equivalent'
5.A.2.a. Technical Note 2.c.	- new entry for "asymmetric algorithm" including sub-paras 1., 2. & 3. and a Technical Note - «or» moved from the end of Technical Note 2.a. to the end of TN 2.b.3. (consequential change)
5.A.2.a., Note 2.j.	- new entry for items specially designed for a 'connected civil industry application' including sub-paras. 1. & 2. and Technical Notes 1 & 2

Category/Item	Comments
5.A.2.b.	- entry rewritten including a Technical Note for the local definition of 'cryptographic activation token'
5.D.2.b.	- entry rewritten
5.E.2.b.	- entry rewritten
Category 6	
6.A.1.a.2.	- Note referring to receiving equipment is moved from the end of the 6.A.1.a.2. entries to under the chapeau
6.A.1.a.2.a.	- new Technical Note 2; existing TN numbered 1
6.A.1.a.2.a.6.	- 'hydrophone sensitivity' parameter added
6.A.3.b.4.b., Note 3.b.1.	- parameter changed from 10 to 2 mrad
6.A.5.	- new Note 6 defining 'Single transverse mode' and 'Multiple transverse mode'
6.A.5.a.3.a. & b.; 6.A.5.a.5.a. & b.; 6.A.5.a.6.a. & b.; 6.A.5.a.6.b. Note 1 and Note 2 chapeau; 6.A.5.a.7.a. & b.; 6.A.5.a.9.a. & b.; 6.A.5.b.3.a. & b.; 6.A.5.b.5.a., b. & c.; 6.A.5.b.6.c. & d.; 6.A.5.b.7.a. & b.; 6.A.5.b.9.a. & b.	- single quotation marks placed around 'Single transverse mode' and 'Multiple transverse mode' in these entries
6.A.5.a.6.a.	- entry amended including new sub-paras. 1. and 2.
6.A.5.a.6.b.1.	- parameter changed from 500 to 1,000 W
6.A.5.a.6.b., Note 2	- sub-paras. a., f. and g. deleted; - sub-para. e – parameter changed from 4 to 6 kW
6.A.5.d.1.b.	- comma deleted after Individual
6.B.2.	- new entry for masks and reticles
Category 7	
7.A.2.a.1. & 2.	- «angular» added before rate range
7.A.3., Technical Note a.; 7.A.5. chapeau; 7.A.5.b., Note; 7.D.3.b.2.; 7.D.5.	- "Satellite navigation system" replaces Global Navigation Satellite Systems (GNSS) in these entries
Category 8	
8.A.1.c.	- entry entirely rewritten
8.A.1.d.	- entry deleted
8.A.2.d.	- entry written with a cascading structure for greater clarity
8.B.1.	- entry amended
Category 9	
9.A.4.	- air-launch platforms added in the chapeau
9.A.4.g.	- new entry for air-launch platforms

Category/Item	Comments
9.A.10.d.	- 'response time' made into a local definition with corresponding Technical Note
9.B.1.	- entry amended
9.E.3.a.7.	- entry deleted
Sensitive List	
3.A.1.b.2.	- new entry for "MMIC" amplifiers
3.A.1.b.3.	- new entry for discrete microwave transistors
6.A.2.a.3.	- Notes 7 and 8 are combined as Note 7; - Note 8 no longer used
8.A.1.c.	- «tethered» deleted from the entry
8.A.1.d.	- entry deleted
Very Sensitive List	
8.A.1.c.1.	- new entry for unmanned submersible vehicles
8.A.1.d.	- entry deleted
Munitions List	
ML4.a., Note b.	- addition of «or» between Missile and rocket nozzles
ML5. chapeau and para. b.	- entry amended and para. b. has a cascaded structure
ML6.	- entry amended and restructured
ML8.a.6.	- a hyphen has been added between «FOX» and «7» (editorial)
ML8.a.33.	- double quotation marks around "Explosives" (editorial correction)
ML8.a.36 & 37	- a semi-colon at the end of these entries (editorial)
ML8.a.43.	- new entry
ML8.c.12.	- new Note
ML9.a.1.	- new Note for diver delivery vehicles
ML9.a.2.; ML17.h.; ML17.m.; ML17.p.	- «other than those» replaced by «not»
ML9.b.3.	- Non-magnetic deleted before diesel engines; - in sub-para. b. single quotation marks around 'Non-magnetic'; - new Technical Note added for the local definition of 'non-magnetic'
ML9.h.	- new entry for naval nuclear equipment including a Technical Note and a Note
ML10., Note 5	- or "lighter-than-air vehicles" added to the chapeau
ML10., Note 6	- new Note for vintage aero-engines
ML11.b.	- "Satellite navigation system" replaces Global Navigation Satellite Systems (GNSS)
ML13., Note 4	- «c.» is added to ML13 reference
ML17.g.and Note	- «not specified elsewhere» is added after «propulsion equipment»; - «including "nuclear reactors"» moved to a new Note
ML21.c.	- full stop added between «ML21» and «b» (editorial)
Definitions	
"Cryptography"	- new Note 2 added; - existing Note renumbered 1
"Radiant sensitivity"	- full stop at the end of the definition (editorial)

Category/Item	Comments
"Satellite navigation system"	- new definition
"Stability"	- Statement of Understanding amended
"Vacuum electronic devices"	- new global definition
Acronyms and Abbreviations	
ENOB	- new entry
EUV	- new entry
GNSS	- entry deleted
GVWR	- new entry
HEMT	- «s» deleted from «Transistors»
PDK	- new entry
QE	- new entry
ROIC	- new entry
Statements of Understanding and Validity Notes	No amendments were made to the Statements of Understanding and Validity Notes

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 2019. Greece will assume the Chair of the Plenary for 2019. Additional information can be found on the Wassenaar website.

Australia Group

The Australia Group (AG) held its 33rd plenary meeting in June 2018. 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 33rd Plenary were:

- issuing a consensus statement expressing the Group's grave concerns about the re-emergence of the use of chemical weapons, in Syria, Iraq, the United Kingdom and Malaysia;
- agreement to several amendments to the Syria Specific Control List for use by AG participants;
- 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, with non-AG members such as China 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.

Several AG participants urged the Chair to issue a consensus statement from the Group, highlighting the significant risks to the CWC from recent events and the need to protect and uphold the international rules-based order. In response, AG participants expressed their grave concern and alarm at the re-emergence of the use of chemical weapons, in violation of, and in challenge to the international laws and norms prohibiting the use of these abhorrent, indiscriminate weapons.

Participants again urged the Syrian regime to respect its obligations under international law, to cease chemical weapons use and to fully declare and completely destroy its chemical weapons program pursuant to its obligations under the CWC. AG participants also urged all countries to fully respect their obligations under international law, not to use chemical weapons, and to fully declare and completely destroy their chemical weapons programs pursuant to their obligations under the CWC.

Participants expressed grave concern at the attack using a nerve agent in March 2018 in the United Kingdom, as confirmed by the OPCW Technical Assistance Visit report, putting innocent people and responding emergency services personnel in grave danger. AG participants welcomed the UK's presentation of its thorough analysis of the incident, and looked forward to the further conclusions of the ongoing police investigation. AG participants again voiced concerns 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 2017 demonstrated the need for action to address the threat of chemical weapons.

AG participants welcomed the convening of a Special Session of the Conference of the States Parties to the CWC on 26-27 June 2018 in The Hague, to allow all States Parties to be able to discuss and express their views on possible additional, stronger measures for upholding the CWC, and reinforcing the effectiveness of the OPCW and its Technical Secretariat in carrying out their mandate.

AG participants also stressed the CWC Review Conference in November 2018, would be crucial to ensuring no erosion of the global prohibition on any use of chemical weapons. AG participants expressed their support and appreciation for the professional, impartial and independent work of the OPCW Director-General and Technical Secretariat in upholding the CWC. AG participants were also briefed on the International Partnership Against Impunity for the Use of Chemical Weapons. Those not yet Participating States were invited to join the Partnership. Many AG participants expressed support for the efforts made by Participating States to the Partnership to ensure that all those who develop or use these weapons are held accountable.

All AG participants reaffirmed their steadfast commitment and determination to continue working collectively and collaboratively, including to ensure that exports from their territories do not contribute to the development or use of chemical or biological weapons, and on other measures to help safeguard and strengthen the global non-proliferation arrangements that are intended to keep all countries more secure and safe. All AG participants agreed that the use of any chemical weapons by anyone, anywhere, cannot be tolerated under any circumstance.

France will host the 2019 Plenary in Paris in June 2019.

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

Nuclear Suppliers Group

The 28th Plenary Meeting of the Nuclear Suppliers Group (NSG) took place in Jurmala, Latvia in June 2018. 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.

On the Democratic People's Republic of Korea (DPRK), the Participating Governments noted the developments in the DPRK since the 2017 NSG Plenary in Bern, and reconfirmed their commitment to the United Nations Security Council resolutions 2371(2017), 2375(2017), 2397(2017) and previous relevant UNSC resolutions, which, inter alia, reaffirm that the DPRK shall immediately abandon all nuclear weapons and existing nuclear programs in a complete, verifiable and irreversible manner. Participating Governments noted with encouragement the recent Inter-Korean summits and the DPRK-US summit. Within the framework of the NSG's mandate, the Participating Governments noted that the supply of all controlled items to the DPRK is prohibited according to the above-mentioned resolutions.

On Iran, the Participating Governments took note of the continued implementation by the E3/EU+2 and the Islamic Republic of Iran of the Joint Comprehensive Plan of Action (JCPOA). Participating Governments reconfirmed their commitment to the 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. Participating Governments expressed interest in receiving further briefings.

The Group noted that discussions were continuing on the requests for participation that had been submitted.

The Group noted that discussions were continuing on the issue of "Technical, Legal and Political Aspects of the Participation of Non-NPT States in the NSG" initiated at the 2016 Seoul Plenary.

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;
- strengthened the NSG's policies regarding transparency and confidentiality;
- discussed and exchanged information and best practices on licensing and enforcement as well as national experiences in implementing the NSG Guidelines;
- welcomed the growing number of States that have harmonized their national export control systems with the NSG Guidelines and Control Lists;
- took note of an outreach event with the World Association of Nuclear Operator (WANO) and the World Nuclear Association (WNA) on 10 April 2018 and welcomed the interest of industry in future outreach
- decided to revise and update the NSG website, adding new content and sections
- 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.

Missile Technology Control Regime

The Missile Technology Control Regime (MTCR) held its 32nd Plenary meeting this year. However, unlike prior years, the MTCR has yet to issue a public statement summarizing objectives and actions taken at this year's Plenary meeting 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 (including 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.

Further information on the MTCR is available on its website, and will include updates from the 32nd Plenary meeting, if they are published.

Recommendations for 2019

We anticipate the following actions in 2019, which you can begin preparing for now:

- We are likely to see the impact of the NDAA's Export Control Reform Act early in the New Year. BIS has solicited comments on the criteria for defining emerging and foundational technologies in the areas of biotechnology, artificial intelligence and machine learning, microprocessor technology, data analytics technology, robotics, and more. This could lead to export licensing requirements for these technologies, even if they are not currently controlled under the EAR. Since the comment period has been extended until January 10th, we recommend providing comments to BIS, even if your company's technology is not included in the initial categories of emerging technologies. The comment may address how to define and identify emerging technologies and the impact these controls would have on U.S. technological leadership.

- The NDAA's Foreign Investment Risk Review Modernization Act will also be addressed in the New Year. FIRRMA's Pilot Program already expands the CFIUS review process of foreign investments in the U.S., and creates mandatory filing requirements, and includes certain non-controlling investments in US businesses involved in critical technologies related to specific industries. We are likely to see further clarifications on the definition of critical technologies early in the New Year, but U.S. companies should already be reviewing any possible foreign investment under the expanded scope of FIRRMA.

- The Section 301 tariffs have already had a significant impact on U.S. importers of Chinese-origin items, and we anticipate changes to the tariffs in 2019. The List 3 tariff rate on the $200 billion worth of Chinese-origin items is set to increase to 25% on March 1st. List 3 includes telecommunications routing and switching apparatus under HTS code 8517.62.0090. There have also been discussions about adding a List 4 of items to the China import tariffs, although nothing has been formally announced. We recommend reviewing the HTS classification of all Chinese-origin imports to determine if your items are already subject to the Section 301 tariffs or future tariffs. If so, you should consider ways of mitigating the impact of the tariffs including adjusting supply chain operations or utilizing a bonded warehouse or drawback program.

- Based on our review of enforcement actions in 2018, we recommend that exporters review their internal screening process to mitigate the risk of an export violation. The Cobham/Metelics case included a failure in the third-party screening software to detect a partial match of a denied party, as well as the failure to

identify a party that was blocked pursuant to OFAC's 50% rule, which blocks transactions with entities majority-owned by a denied party, even if the entity, itself, is not included on the denied party list. This requires enhanced due diligence by exporter, who can no longer solely rely on the third-party screening results. Exporters should consider an internal audit of its existing screening process, and enhanced end-user/end-use certifications for transactions with countries of concern.

- There have been continued developments in the export/import control regulations of various foreign governments. The focus in 2018 was on China, which introduced retaliatory tariffs against U.S.-origin items, and implemented its cybersecurity law. We have also continued to see enforcement of foreign governments' import controls on encryption products. Many of these issues will be addressed at the annual American Conference Institute's *Advanced Industry Forum on Global Encryption, Cloud & Cyber Export Controls*. The 9th year of the conference will be held on March 27 - 28 in San Francisco, California, and will once again be co-chaired by Roz Thomsen. In addition to foreign importers and 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.

- Finally, a reminder to exporters of encryption products that the end of the year marks the close of the reporting period for annual encryption and semi-annual ENC reports. As we continue to see streamlining changes being made to encryption products, many items no longer require reporting. This is a good time to prepare required reports, which are due no later than February 1, 2019 and to analyze current products to determine if reporting is no longer required.

We look forward to working with you on these recommendations and other trade compliance issues in the New Year!

Appendix A – Additional Enforcement Actions

PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage

The Department of Commerce took action to restrict exports to Fujian Jinhua Integrated Circuit Company, Ltd. (Jinhua) by adding them to the Entity List (Supplement No. 4 to Part 744 of the Export Administration Regulations), because Jinhua poses a significant risk of becoming involved in activities that are contrary to the national security interests of the United States. Jinhua is nearing completion of substantial production capacity for dynamic random access memory (DRAM) integrated circuits. The additional production, in light of the likely U.S.-origin technology, threatens the long term economic viability of U.S. suppliers of these essential components of U.S. military systems.

The Justice Department later announced the indictment of Jinhua and United Microelectronics Corporation and three individuals charging them with crimes related to a conspiracy to steal, convey, and possess stolen trade secrets of an American semiconductor company for the benefit of a company controlled by the PRC government.

According to the indictment, the defendants were engaged in a conspiracy to steal the trade secrets of Micron Technology, Inc. (Micron), a leader in the global semiconductor industry specializing in the advanced research, development, and manufacturing of memory products, including dynamic random-access memory (DRAM). DRAM is a leading-edge memory storage device used in computer electronics. Micron is the only United States-based company that manufactures DRAM. According to the indictment, Micron maintains a significant competitive advantage in this field due in large part from its intellectual property, including its trade secrets that include detailed, confidential information pertaining to the design, development, and manufacturing of advanced DRAM products.

Prior to the events described in the indictment, the PRC did not possess DRAM technology, and the Central Government and State Council of the PRC publicly identified the development of DRAM and other microelectronics technology as a national economic priority. The criminal defendants are United Microelectronics Corporation (UMC), a Taiwan semiconductor foundry; Fujian Jinhua Integrated Circuit, Co., Ltd. (Jinhua), a state-owned enterprise of the PRC; and three Taiwan nationals: Chen Zhengkun, a.k.a. Stephen Chen; He Jianting, a.k.a. J.T. Ho; and Wang Yungming, a.k.a. Kenny Wang.

UMC is a publicly listed semiconductor foundry company traded on the New York Stock Exchange; is headquartered in Taiwan; and has offices worldwide, including in Sunnyvale, California. UMC mass produces integrated-circuit logic products based on designs and technology developed and provided by its customers. Jinhua is a state-owned enterprise of the PRC, funded entirely by the Chinese government, and established in February 2016 for the sole purpose of designing, developing, and manufacturing DRAM.

According to the indictment, Chen was a General Manager and Chairman of an electronics corporation that Micron acquired in 2013. Chen then became the president of a Micron subsidiary in Taiwan, Micron Memory Taiwan (MMT), responsible for manufacturing at least one of Micron's DRAM chips. Chen resigned from MMT in July 2015 and began working at UMC almost immediately. While at UMC, Chen arranged a cooperation agreement between UMC and Fujian Jinhua whereby, with funding from Fujian Jinhua, UMC would transfer DRAM technology to Fujian Jinhua to mass-produce. The technology would be jointly shared by both UMC and Fujian Jinhua. Chen later became the President of Jinhua and was put in charge of its DRAM production facility.

While at UMC, Chen recruited numerous MMT employees, including Ho and Wang, to join him at UMC. Prior to leaving MMT, Ho and Wang both stole and brought to UMC several Micron trade secrets related to the design and manufacture of DRAM. Wang downloaded over 900 Micron confidential and proprietary files before he left MMT and stored them on USB external hard drives or in personal cloud storage, from where he could access the technology while working at UMC.

Société Générale S.A. Settles Potential Civil Liability for Apparent Violations of Multiple OFAC Sanctions Programs

Société Générale S.A., a financial institution headquartered in Paris, France, has agreed to remit $53,966,916.05 to settle its potential civil liability for the 1,077 apparent violations of the Cuban Assets Control Regulations; the Iranian Transactions and Sanctions Regulations; and the Sudanese Sanctions Regulations.

For at least five years up to and including 2012, Société Générale S.A. processed transactions to or through the United States or U.S. financial institutions that involved countries or persons (individuals and entities) subject to the sanctions programs administered by OFAC. Société Générale S.A. often processed these transactions in a non-transparent manner that removed, omitted, obscured, or otherwise failed to include references to OFAC-sanctioned parties in the information sent to the U.S. financial institutions that were involved in the transactions.

For more information regarding the conduct that led to the Apparent Violations.

Société Générale S.A. processed 796 transactions involving Cuba totaling approximately $5,503,813,992.25 between July 11, 2007 and October 26, 2010, in apparent violation of the CACR. The total base penalty for this set of apparent violations was $25,870,000.00. Société Générale S.A. processed 30 transactions involving Iran totaling approximately $34,152,962.50 between November 20, 2008 and January 20, 2009, in apparent violation of the ITSR. The total base penalty for this set of apparent violations was $34,152,962.50. Société Générale S.A. processed 251 transactions involving Sudan totaling $22,486,039.61 between July 9, 2007 and March 19, 2012, in apparent violation of the SSR. The total base penalty for this set of apparent violations was $41,656,278.22.

Two Los Angeles-Area Men Charged with Conspiring to Illegally Obtain Technology and Computer Chips that Were Sent to China

Yi-Chi Shih, 62, an electrical engineer who is a part-time Los Angeles resident, and Kiet Ahn Mai, 63, of Pasadena, were arrested on federal charges that allege a scheme to illegally obtain technology and integrated circuits with military applications that were exported to a Chinese company without the required export license.

The complaint alleges that Shih and Mai conspired to illegally provide Shih with unauthorized access to a protected computer of a United States company that manufactured specialized, high-speed computer chips known as monolithic microwave integrated circuits (MMICs). The conspiracy count also alleges that the two men engaged in mail fraud, wire fraud and international money laundering to further the scheme.

According to the affidavit in support of the criminal complaint, Shih and Mai executed a scheme to defraud the U.S. company out of its proprietary, export-controlled items, including technology associated with its design services for MMICs. As part of the scheme, Shih and Mai accessed the victim company's computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mail allegedly concealed Shih's true intent to transfer the U.S. company's technology and products to the People's Republic of China.

The victim company's proprietary semiconductor technology has a number of commercial and military applications, and its customers include the Air Force, Navy and the Defense Advanced Research Projects Agency. MMICs are used in electronic warfare, electronic warfare countermeasures and radar applications.

The computer chips at the heart of this case allegedly were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese company that established a MMIC manufacturing facility in Chengdu. Shih was the president of CGTC, which in 2014 was placed on the Commerce Department's Entity List, according to the affidavit, "due to its involvement in activities contrary to the national security and foreign policy interest of the United States – specifically, that it had been involved in the illicit procurement of commodities and technologies for unauthorized military end use in China." Because it was on the Entity List, a license from the Commerce Department was required to export U.S.-origin MMICs to CGTC, and there was a "presumption of denial" of a license.

The complaint outlines a scheme in which Shih used a Los Angeles-based company he controlled – Pullman Lane Productions, LLC – to funnel funds provided by Chinese entities to finance the manufacturing of MMICs by the victim company. The complaint affidavit alleges that Pullman Lane received financing from a Beijing-based

company that was placed on the Entity List the same day as CGTC "on the basis of its involvement in activities contrary to the national security and foreign policy interests of the United States."

Mai acted as the middleman by using his Los Angeles company – MicroEx Engineering – to pose as a legitimate domestic customer that ordered and paid for the manufacturing of MMICs that Shih illegally exported to CGTC in China, according to the complaint. It is the export of the MMICs that forms the basis of the IEEPA violation alleged against Shih. The specific exported MMICs also required a license from the Commerce Department before being exported to China, and a license was never sought or obtained for this export.

Turkish Banker Convicted of Conspiring to Evade U.S. Sanctions Against Iran and Other Offenses

Mehmet Hakan Atilla, a resident of Turkey, was found guilty of conspiring with others, including Reza Zarrab, a/k/a "Riza Sarraf," who previously pled guilty to evading U.S. sanctions among other offenses, to use the U.S. financial system to conduct transactions on behalf of the Government of Iran and other Iranian entities, which were barred by U.S. sanctions, and to defraud U.S. financial institutions by concealing these transactions' true nature.

According to the evidence introduced at trial, other proceedings in this case, and documents previously filed in Manhattan federal court:, Atilla, Zarrab, and others used deceptive measures to provide access to international financial networks, including U.S. financial institutions, to the Government of Iran, Iranian entities, and entities identified by the Department of the Treasury Office of Foreign Assets Control as Specially Designated Nationals. They did so by, among other things, using Halk Bank, at which Atilla acted as Deputy General Manager of International Banking, to engage in transactions that violated U.S. sanctions against Iran. In particular, they took steps to protect and hide Zarrab's supply of currency and gold to the Government of Iran, Iranian entities, and SDNs using Halk Bank, and in doing so, shielded the bank from U.S. sanctions. Atilla, Zarrab, and others conspired to create and use false and fraudulent documents to disguise prohibited transactions for Iran and make those transactions falsely appear as transactions involving food, thus falling within humanitarian exceptions to the sanctions regime. As a result of this scheme, the co-conspirators induced U.S. banks to unknowingly process international financial transactions in violation of the IEEPA.

Texas man sentenced for conspiring to illegally export radiation-hardened integrated circuits to Russia and China

A North Texas man was sentenced to 46 months in federal prison for 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.

According to the plea agreement, between about June 2015 and March 2016, Peter Zuccarelli, 62, of Plano, Texas, and his co-conspirators agreed to illegally export RHICs to China and Russia in violation of the International Emergency Economic Powers Act. 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 about $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.

Commerce Department Moves Against Illicit Iran Aircraft Network

BIS has acted against Turkish national Gulnihal Yegane and three affiliated Turkish companies who are involved in illicitly procuring and supplying Iranian airlines with U.S.-origin aircraft engines and spare parts. The action, called a "temporary denial order" (TDO), suspends the export privileges of Gulnihal Yegane (Yegane), Trigron Lojistik

Kargo Limited Sirketi ("Trigron"), Ufuk Avia Lojistik Limited Sirketi (Ufuk Avia), and RA Havacilik Lojistik Ve Tasimacilik Ticaret Limited Sirketi (RA Havacilik). Gulnihal Yegane was previously added to the BIS Entity List for smuggling parts to Iran's Mahan Air.

Yegane is actively involved in the illicit procurement of U.S.-origin aircraft engines and spare parts (ECCN 9A991) for Iranian airlines and has taken extensive steps to continue this activity while attempting to conceal her involvement after BIS added Yegane to the BIS Entity List in December 2013 for transactions involving Mahan Air (78 FR 75458). Mahan Air was designated by Treasury's Office of Foreign Assets Control (OFAC) as a Specially Designated Global Terrorist in October 2011 for providing financial, material, and technological support to Iran's Islamic Revolutionary Guard Corps-Qods Force. Yegane is now utilizing Trigron, which Yegane owns and operates, and Turkish logistics companies Ufuk Avia and RA Havacilik, with which Yegane is affiliated. The deceptive efforts to obtain U.S.-origin aircraft engines included re-structuring a transaction to Iran to conceal Yegane's involvement after the initial attempt was discovered by BIS.

Temporary Denial Orders are issued by the Assistant Secretary for Export Enforcement of the Bureau of Industry and Security, denying the export privileges of a company or individual to prevent an imminent or on-going export control violation. These orders are issued for a renewable 180-day period and cut off not only the right to export from the United States, but also the right to receive or participate in exports from the United States. BIS is the principal agency involved in the implementation and enforcement of export controls for commercial technologies and many military items. The BIS Office of Export Enforcement detects, prevents, investigates and assists in the sanctioning of illegal exports of such items.

Two Men Indicted for Scheme to Export Firearms to Kurds in Iraq

Two men were indicted by a federal grand jury in Seattle Wednesday for three federal felonies in connection with their scheme to smuggle dozens of firearms to Turkey and Iraq in violation of the Arms Export Control Act. Paul Stuart Brunt, 51, of Bellevue, Washington, and Rawnd Khaleel Aldalawi, 29, of Seattle, were arrested on a criminal complaint January 24, 2018.

According to records filed in the case, between October 2016 and November 2017, Brunt and Aldalawi engaged in a scheme to smuggle firearms from the U.S. to people associated with the Peshmerga military in Kurdistan, a part of Iraq. Brunt purchased the firearms at gun stores and gun shows around the Puget Sound region. The men then attempted to ship the guns from the Port of Seattle through Turkey and on to Iraq, hidden in the side panels of vehicles.

In the first shipment in February 2017, some 30 guns were hidden in three cars. In the second shipment in November 2017, 47 firearms were concealed in two vehicles. That second shipment was discovered by authorities in Turkey, and the shipment was traced back to Brunt and Aldalawi. The men had not obtained any export licenses for the firearms and smuggled them in violation of the Arms Export Control Act.

The conspiracy is punishable by up to five years in prison and a $250,000 fine. Violating the Arms Export Control Act is punishable by twenty years of imprisonment. The men are scheduled to be arraigned on the indictment on February 8, 2018.

Two Men Arrested and Charged With Illegally Exporting UAV Parts and Technology to Hizballah

The indictment of Usama Darwich Hamade, 53, Samir Ahmed Berro, 64, and Issam Darwich Hamade, 55, was announced for their conspiring to illegally export goods and technology from the United States to Lebanon and to Hizballah, a designated foreign terrorist organization, in violation of the International Emergency Economic Powers Act, the Export Administration Regulations, and the International Traffic in Arms Regulations. Defendants Usama Hamade and Issam Hamade are currently in custody in South Africa. Samir Ahmed Berro remains at large.

According to the Indictment, from 2009 through December 2013, Usama Hamade, Berro and Issam Hamade willfully conspired to export and attempted to export from the United States to Lebanon, and specifically to

Hizballah, goods and technology without obtaining the required export licenses from the U.S. Department of Commerce and the U.S. Department of State, in violation of IEEPA, the Export Administration Regulations, the Arms Export Control Act, and the International Traffic in Arms Regulations. According to the Indictment, those goods included inertial measurement units (IMUs) suitable for use in unmanned aerial vehicles (UAVs), a jet engine, piston engines and recording binoculars.

Port St. Lucie Man Indicted on Weapons Charges

A Port St. Lucie man was indicted on charges related to the illegal exportation of firearms, firearms accessories and ammunition. Frederik Barbieri, 36, of Ft. Pierce, Florida, was charged with one count of conspiracy to commit offenses against the United States, one count of delivering firearms to a contract carrier without notification, that shipment contained firearms, one count of smuggling firearms and fire accessories from the United States to Brazil and one count of exporting firearms and firearms accessories without a license. According to court documents, Barbieri entered into a conspiracy to illegally export firearms to Brazil without a license, which lasted from May 2013 to June 2017. Barbieri and his co-conspirators purchased firearms, firearms accessories and ammunition, obliterated the serial numbers and concealed the weapons, the accessories and the ammunition in different packages.

Barbieri and his co-conspirators would then ship the packages to Brazil, where Barbieri and his co-conspirators would sell such firearms, firearm accessories, and ammunition at a profit. It is further alleged that on May 26, Barbieri shipped a package concealing firearms and firearms accessories to Brazil without obtaining a license to export those items and without notifying the contract carrier that the package contained firearms.

If convicted, Barbieri faces a maximum statutory sentence of five years on Counts 1 and 2, a maximum statutory sentence of 10 years on Count 3, and a maximum statutory sentence of 20 years on Count 4.

Connecticut Business Owners Admit to Profiting from Unlawful Exports to Pakistan

Muhammad Ismail and Kamran Khan of Connecticut pleaded guilty in federal court to money laundering in connection with funds they received for the unlawful export of goods to Pakistan. A third defendant, Imran Khan previously pleaded guilty to violating U.S. export laws.

According to court documents and statements made in court, from at least 2012 to December 2016, Ismail, and his two sons, Kamran and Imran Khan, were engaged in a scheme to purchase goods that were controlled under the Export Administration Regulations and to export those goods without a license to Pakistan, in violation of the EAR. Through companies conducting business as Brush Locker Tools, Kauser Enterprises-USA and Kauser Enterprises-Pakistan, the three defendants received orders from a Pakistani company that procured materials and equipment for the Pakistani military, requesting them to procure specific products that were subject to the EAR. When U.S. manufacturers asked about the end-user for a product, the defendants either informed the manufacturer that the product would remain in the U.S. or 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 the defendants in Connecticut. The products were then shipped to Pakistan on behalf of either the Pakistan Atomic Energy Commission ("PAEC"), the Pakistan Space & Upper Atmosphere Research Commission (SUPARCO), or the National Institute of Lasers & Optronics (NILOP), all of which were listed on the U.S. Department of Commerce Entity List. The defendants never obtained a license to export any item to the designated entities even though they knew that a license was required prior to export. The defendants received the proceeds for the sale of export controlled items through wire transactions from Value Additions' Pakistan-based bank account to a U.S. bank account that the defendants controlled.

BIS Penalizes Trilogy International for Russian Export Violations

On or about January 23, 2010, April 6, 2010, and May 14, 2010, respectively, Trilogy International engaged in conduct prohibited by the Regulations by exporting items subject to the Regulations and controlled on national security grounds to Russia without the required BIS export licenses.

The items involved were an explosives detector and a total of 115 analog-to-digital converters. The items were classified under Export Control Classification Numbers 1A004 and 3A001, respectively, controlled as indicated above on national security grounds, and valued in total at approximately $76,035. Each of the items required a license for export to Russia pursuant to Section 742.4 of the Regulations.

BIS issued $200,000 in penalties and 10-year export bans to Trilogy International Associates and its president for exporting an explosives detector and other equipment to Russia without the required licenses.

Iranian national sentenced in Minnesota to 15 months in federal prison for conspiring to illegally export restricted technology to Iran

An Iranian national, who was arrested in New York City, was sentenced in Minneapolis to 15 months in prison for his role in illegally exporting restricted technology to his home country. Aliereza Jalali, 39, was sentenced before U.S. District Judge Joan N. Ericksen in the District of Minnesota, on one count of conspiracy to defraud the United States. He pleaded guilty to the charge on Nov. 29, 2017.

According to the defendant's guilty plea, from 2009 through December 2015, Jalali was a part-time employee of Green Wave Telecommunication, Sdn Bhn, (Green Wave) a Malaysian company located in Kuala Lumpur, Malaysia. Since its incorporation in 2009, Green Wave operated as a front company for Fanavar Moj Khavar (Fana Moj), an Iran-based company that specializes in both broadcast communications and microwave communications.

As part of this conspiracy, Green Wave was used to acquire unlawfully sensitive export-controlled technology from the United States on behalf of Fana Moj. In order to accomplish these acquisitions, Jalali and his co-conspirators concealed the ultimate unlawful destination and end users of the exported technology through false statements, unlawful financial transactions, and other means.

The defendant's co-conspirators contacted producers of the sought-after technology, solicited purchase agreements, and negotiated the purchase and delivery of the goods with the seller. When the goods were received by Green Wave in Malaysia, Jalali repackaged and unlawfully exported the items from Malaysia to Fana Moj in Tehran, Iran. In 2017, the U.S. Department of the Treasury placed Fana Moj on its list of "Specially Designated Nationals" for providing financial, material, technological or other support for, or goods or services in support of, the IRGC.

Florida Man Pleads Guilty to Conspiracy to Illegally Export Defense Articles to Russia

Vladimir Nevidomy, 31, of Hallandale Beach, Florida, pleaded guilty, to conspiring to illegally export military-grade night vision and thermal vision devices and ammunition primers to Russia. According to information contained in court documents, from as early as April 2013 through November 2013, customers in Russia contacted Nevidomy by email requesting night vision rifle scopes, thermal monoculars and ammunition primers, all of which were on the U.S. Munitions List and subject to export control by the U.S. Department of State. Nevidomy proceeded to obtain at least three ATN MARS 4x4 night-vision rifle scopes and an ODIN 61BW thermal multi-purpose monocular from U.S. vendors by falsely representing to the vendors that the items were not for export.

On or about April 16, 2013, a co-defendant caused a wire transfer from a Shanghai, China bank account in the amount of $11,755 for the purchase and shipment of two ATN MARS 4x4 night-vision rifle scopes. That same day, Nevidomy paid $9,599 to a U.S. vendor for the purchase of those two night-vision rifle scopes. On or about May 2, 2013, Nevidomy also caused a wire transfer in the amount of $10,000 to be sent to a U.S. vendor for the purchase of the ODIN 61BW thermal multi-purpose monocular.

Later, Nevidomy's co-defendant caused a wire transfer from a bank account in Riga, Latvia in the amount of $18,036, part of which was for the purchase of a third ATN Mars 4X4 night-vision rifle scope. On the same day,

Nevidomy caused a wire transfer in the amount of $9,599 to a U.S. vendor, part of which was for the purchase of the third ATN Mars 4X4 night-vision rifle scope.

After the U.S. vendors sent the night vision devices to Nevidomy in South Florida, he exported them to the co-defendant in Russia by either concealing the defense articles in household goods shipments sent through a freight forwarding company or using a private Russian postal service that operated in South Florida. In June 2013, Nevidomy aided and abetted the export of the ATN MARS 4x4 night-vision rifle scopes from the U.S. to the co-defendant in Russia, and in August 2013, he exported the ODIN 61BW thermal multi-purpose monocular from the U.S. to the co-defendant in Russia.

On or about July 19, 2013, the same co-defendant sent an email to Nevidomy requesting 1,000 large-rifle ammunition primers to be shipped to Vladivostok, Russia. On or about Oct. 2, 2013, Nevidomy attempted to export 1,000 Sellier & Bellot ammunition primers from the U.S. to the co-defendant in Vladivostok, Russia. These ammunition primers were seized by U.S. Customs and Border Protection.

These night vision rifle scopes, thermal monocular, and ammunition primers required a license or other authorization from the U.S. Department of State before being exported from the U.S. since they were on the U.S. Munitions List. A certified license history check revealed that neither Nevidomy nor his associates ever applied or attempted to apply for an export license from the State Department for the night-vision equipment or ammunition primers.

U.S. Couple and Company Indicted for Conspiracy to Illegally Obtain U.S. Goods For Syria

A Massachusetts couple, their company, and a Syrian national were indicted today in federal court in Boston in connection with a scheme to smuggle goods out of the United States and to supply services to Syria. The company and the defendants also conducted business with EKT Electronics, which was involved in the acquisition and/or development of improved explosive devices used against U.S. troops in Iraq and Afghanistan.Anni Beurklian, a/k/a Anni Ajaka (Beurklian), 49, a naturalized U.S. citizen from Lebanon who resided in Waltham; her husband, Antoine Ajaka, a/k/a Tony Ajaka (Ajaka), 50, a lawful permanent resident from Lebanon who resided in Waltham; Amir Katranji, a/k/a Amir Hachem Katranji, a/k/a Amir Hachem Alkatranji, a/k/a Amir Katra (Katranji), 52, a Syrian national; and Top Tech US Inc., a U.S. company, which operated out of the Ajaka/Beurklian residence in Waltham, were indicted on conspiracy to violate U.S. export laws and regulations, conspiracy to defraud the United States, smuggling U.S. goods out of the United States, conspiracy to obstruct justice, and obstruction of justice. Beurklian, Ajaka, and Top Tech US Inc. are also charged with illegally providing services to persons located in Syria and mail fraud. Beurklian and Ajaka previously fled the U.S. and have not returned.

As alleged in the indictment, beginning no later than 2012 and continuing until Jan. 9, 2018, Beurklian and her husband operated an export business, Top Tech US Inc., out of their Waltham residence. The couple used their business to procure goods, including electronics, computer equipment, and electrical switches, from U.S. companies and export those goods out of the United States to customers in Lebanon and Syria. One of their customers was Amir Katranji, a citizen of Syria who operates and manages EKT Electronics (EKT), a company headquartered in Syria. In 2007, EKT and its founder, Mohammad Katranji, Amir Katranji's father, were added to the Department of Commerce's Entity List because the U.S. Government had determined that EKT and Mohammad Katranji were involved in activities related to the acquisition, attempted acquisition, and/or development of improvised explosive devices, which were being used against U.S. and Coalition troops in Iraq and Afghanistan. As a result, since 2007, no U.S. person has been permitted to export U.S. goods to EKT without first obtaining an export license from the Department of Commerce. As alleged in the indictment, no one has sought or obtained an export license to export any U.S. goods to EKT or Mohammad Katranji.

The indictment further alleges that in or about 2013, Ajaka and Beurklian began doing business with Katranji and supplying U.S. origin goods to EKT using Top Tech US. Ajaka and Beurklian knew that Katranji operated a business in Syria and that they were providing brokering services to Katranji and his Syrian company, EKT, by buying and shipping U.S. origin goods to EKT and its customers. EKT paid Ajaka and Beurklian more than $200,000 through Top Tech US bank accounts for their services. To conceal their illegal activity with EKT and

evade the mandatory export filing requirement, Ajaka and Beurklian, with the knowledge and agreement of Katranji, falsified shipping paperwork and undervalued goods being shipped overseas directly to, or on behalf of, EKT.

Additionally, the indictment alleges that, in or about 2016, after U.S. Government officials began detaining international shipments made by Top Tech US before they had exited the country, Beurklian, Ajaka, and Katranji conspired to obstruct justice and obstructed justice by manipulating, deleting, and falsifying records regarding shipments of U.S. goods overseas. The indictment further alleges that, on Jan. 9, 2018, after engaging in plea negotiations with the U.S. Government, Beurklian and Ajaka fled the United States to avoid prosecution. To date, they have not returned.

Pennsylvania Man Charged With Illegally Exporting Firearm Parts to Iraq

Ross Roggio, 49, of Stroudsburg, Pennsylvania, and Roggio Consulting Company, LLC, a firm with which Ross Roggio was associated, for alleged involvement in a conspiracy to illegally export firearm parts, firearm manufacturing tools, and "defense services," including items used to manufacture M4 rifles, from the United States to Iraq, in violation of the Arms Export Control Act and the International Emergency Economic Powers Act.

The indictment charges Ross Roggio and Roggio Consulting Company, LLC with criminal conspiracy, illegal export of goods, wire fraud and money laundering. Pursuant to regulations of the U.S. Department of Commerce, a license is required to export certain goods and services from the United States to Iraq for reasons of regional stability and national security. Similarly, defense services and defense articles may not be exported to Iraq without a license from the U.S. Department of State.

The indictment alleges that, beginning in January of 2013 until the date of the indictment, Ross Roggio conspired to export both items and services from the United States to Iraq, without the required U.S. Commerce Department and U.S. State Department licenses. The conspirators allegedly purchased firearms parts and manufacturing tools from the United States, illegally exported the items to Iraq where the items were utilized and incorporated in the manufacture and assembly of complete firearms in a firearms manufacturing plant constructed and operated in part by Ross Roggio. It is alleged that the items illegally exported included: M4 Bolt Gas Rings MIL; Firing Pin Retainers; Rifling Combo Buttons, and "defense services." The defense services allegedly provided by Ross Roggio and his firm include the furnishing of assistance to foreign persons in the manufacture of firearms.

In addition to the charges relating to export controls violations, the indictment also alleges that Ross Roggio and his firm committed wire fraud on at least three occasions by purchasing items from a United States company and providing said company with false information about the end-user of the items. Finally, the indictment charges Ross Roggio and his firm with 27 counts of money laundering in the form of bank transfers from Iraq to two accounts within the Middle District of Pennsylvania, in furtherance of their unlawful export conspiracy.

Russian Citizen Sentenced to 18 Months in Federal Prison for Attempting to Illegally Export More Than $100,000 in Firearm Parts and Accessories

A Russian citizen was sentenced to 18 months in federal prison for attempting to illegally export from the United States more than $100,000 in firearm parts, ammunition and accessories, including parts designed for assault rifles. Konstantin Checkovskoi was apprehended by Homeland Security Investigations (HSI) Special Agents at O'Hare International Airport in Chicago on April 26, 2017, as he attempted to board a flight for Stockholm, Sweden. In Chekhovskoi's eleven checked bags were the firearm parts, ammunition and accessories, including bullets, rifle magazines, triggers, stocks, muzzle brakes and scopes, many of which were designed for assault rifles such as AK-47s and M4s. Chekhovskoi lacked the required license for the export-controlled items. Chekhovskoi, 44, of St. Petersburg, Russia, pleaded guilty last year to one count of attempting to fraudulently and knowingly export firearm parts. U.S. District Judge Sara L. Ellis imposed the 18-month prison term and fined Chekhovskoi $100,000.

New Jersey Woman Charged With Smuggling American Aircraft Components To Iranian Airline Companies

A Morristown, New Jersey, woman appeared in federal court to face charges for her alleged role in an international procurement network that smuggled over $2 million worth of aircraft components from the United States to Iran in violation of export control laws.

Joyce Eliabachus is charged in a three-count criminal complaint with conspiracy to violate the Iranian Transactions and Sanctions Regulations, conspiracy to commit money laundering, and conspiracy to smuggle goods from the United States. According to the complaint, Eliabachus – the principal officer and operator of Edsun Equipments LLC, a purported New Jersey-based aviation parts trading company run out of her Morristown residence – is allegedly part of a sophisticated procurement network that has secretly acquired large quantities of license-controlled aircraft components from U.S. manufacturers and vendors, and exported those parts to Iran through freight-forwarding companies located in the United Arab Emirates and Turkey, in violation of U.S. export control laws.

From May 2015 through October 2017, Eliabachus and her conspirators facilitated at least 49 shipments containing a total of approximately 23,554 license-controlled aircraft parts from the U.S. to Iran, all of which were exported without the required licenses. Eliabachus conspired with the owner of an Iranian-based procurement firm, identified in the complaint as "CC-1," whose international network helped initiate the purchase of U.S.-origin aircraft components on behalf of CC-1's clients in Iran. The network's client list was comprised of Iranian airline companies, several of which have been officially designated by the U.S. government as posing a threat to the country's national security, foreign policy, or economic interests, including Mahan Air Co., Caspian Airlines, and Kish Air, among others.

Using Edsun Equipment in New Jersey, Eliabachus finalized the purchase and acquisition of the requested components from the various U.S.-based distributors. She then re-packaged and shipped the components to shipping companies in the UAE and Turkey, including Parthia Cargo and Reibel Tasimacilik Ve Tic A.S., where her Iranian conspirators directed trans-shipment of the components to locations in Iran.

In order to obscure the extent of the network's procurement activities, Eliabachus routinely falsified the true destination and end-user of the aircraft components she acquired. She also falsified the true value of the components being exported in order to evade the necessity of filing export control forms, which further obscured the network's illegal activities from law enforcement. The funds for the illicit transactions were obtained from the various Iranian purchasers, funneled through Turkish bank accounts held in the names of various shell companies controlled by the Iranian conspirators, and ultimately transferred into one of Edsun Equipments' U.S.-based accounts. The network's creation and use of multiple bank accounts and shell companies abroad was intended to conceal the true sources of funds in Iran, as well as the identities of the various Iranian entities who were receiving U.S. aircraft components.

The charge of conspiracy to violate the ITSR carries a maximum penalty of 20 years in prison and a $1 million fine. The charge of conspiracy to commit money laundering carries a maximum penalty of 20 years in prison and a $500,000 fine. The charge of conspiracy to smuggle goods carries a maximum penalty of five years in prison and a $250,000 fine.

Bulgarian National Arrested for Conspiracy to Defraud the United States and Illegally Export Prohibited Articles to Syria in Violation of U.S. Export Control Laws

Zhelyaz Andreev, a Bulgarian national, was arrested pursuant to an Interpol Red Notice based on an Indictment charging him with: conspiracy to defraud the U.S. Government and substantive violations of the Syria Trade Embargo as enforced through the International Emergency Economic Powers Act; and the U.S. Department of Treasury Office of Foreign Assets Control's designation of Syrian Arab Airlines, aka Syrian Air, as a Specially Designated National whose assets are blocked and with whom U.S. nationals are prohibited from transacting business.

Andreev was charged with conspiracy to violate IEEPA and the OFAC regulations by exporting dual-use goods, that is, articles that have both civilian and military application, to Syrian Arab Airlines, 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.

According to court documents, Andreev worked in the Bulgaria office of AW-Tronics, a Miami export company, which shipped and exported various aircraft parts and equipment to Syrian Arab Airlines. Andreev dealt directly with the Syrian Air principals who procured the parts.

Maine Resident Sentenced Two Years for Illegal Receipt and Shipment of Firearms

Iulian Petre, a/k/a "Julian Petre," 51, of Waterville, Maine, was sentenced in U.S. District Court by Judge John A. Woodcock, Jr. to two years in prison and three years of supervised release for illegally receiving and shipping firearms. He was convicted of these charges on August 28, 2017, following a six-day jury trial. Court records and trial evidence revealed that in 2012 and 2013, Petre purchased and received firearms from out-of-state sellers intending to unlawfully export them. He shipped some of these firearms to Romania. The export of these firearms required authorization from the U.S. Department of State, which the defendant knowingly failed to obtain.

Florida Resident Pleads Guilty to International Firearms Trafficking

A Port St. Lucie resident pled guilty to unlawfully exporting firearms, firearm accessories, and ammunition from South Florida to Rio de Janeiro, Brazil. Frederik Barbieri of Port St. Lucie, Florida pled guilty to one count of conspiracy to commit offenses against the United States, in violation of Title 18, United States Code, Section 371, and one count of unlicensed exportation of defense articles, in violation of Title 22, United States Code, Section 2778. Barbieri faces a possible maximum statutory sentence of 25 years in prison.

According to stipulated facts filed in court, from May of 2013 through February of 2018, Barbieri conspired with others to: possess firearms with obliterated serial numbers; deliver packages containing those firearms to contract carriers for international shipment without providing notice that the packages contained firearms; and smuggle firearms, firearm accessories, and ammunition from the United States to Rio de Janeiro, Brazil.

During this period, a shipment sent by Barbieri was intercepted in Rio de Janeiro by Brazilian law enforcement and found to contain approximately thirty AR-15 and AK-47 rifles and firearm magazines, all concealed in four 38-gallon Rheem water heaters. The water heaters were hollowed out and loaded with the contraband, and the serial numbers on each of the firearms had been obliterated. The same day that Brazilian authorities intercepted his shipment, Barbieri called and requested that the freight forwarder destroy the related paperwork.

Documentation provided by the freight forwarder revealed Barbieri's historical shipments. In addition to shipping the four Rheem water heaters in which he concealed approximately thirty rifles, Barbieri also shipped to Brazil an additional 120 Rheem water heaters, as well as 520 electric motors and 15 air conditioning units, from May of 2013 to May of 2017, using that freight forwarder. These items are all consistent with objects used to conceal the illegal international shipment of firearms and ammunition.

In February 2018, federal agents executed a warrant to search a storage unit rented by Barbieri in Vero Beach, Florida. In the storage unit, law enforcement discovered 52 rifles, 49 of which were wrapped for shipment with obliterated serial numbers. In addition, law enforcement discovered dozens of high capacity firearm magazines, over 2,000 rounds of ammunition, and packaging materials. Barbieri was arrested the following day.

It is illegal for civilians to possess firearms in Brazil. According to Brazilian law enforcement, AK and AR rifles have a black market value of approximately $15,000 to $20,000 in the black market. The retail cost of those firearms in the United States is approximately $700 to $1,000.

Neither Barbeiri, nor any of his coconspirators, obtained a license or written approval from the United States Department of State to export any defense articles. Non-automatic firearms, firearm accessories, and ammunition are articles designated as "defense articles," pursuant to federal regulations.

Turkish Banker Sentenced to 32 Months for Conspiring to Violate U.S. Sanctions Against Iran and Other Offenses

Mehmet Hakan Atilla, a resident and citizen of Turkey, was sentenced to 32 months for his participation in a scheme to violate U.S. economic sanctions imposed on the Islamic Republic of Iran involving billions of dollars' worth of Iranian oil proceeds held at Atilla's employer (Turkish Bank-1). On Jan. 3, after a five-week jury trial, Atilla was convicted of conspiring with others to use the U.S. financial system to conduct transactions on behalf of the government of Iran and other Iranian entities, which were barred by U.S. sanctions, and to defraud U.S. financial institutions by concealing these transactions' true nature.

Beginning in or about 1979, the president, pursuant to the International Emergency Economic Powers Act (IEEPA), has repeatedly found that the actions and policies of the government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States and has declared a national emergency to deal with the threat. In accordance with these presidential declarations, the United States has instituted a host of economic sanctions against Iran and Iranian entities. This sanctions regime, among other things, prohibits financial transactions involving the United States or U.S. persons that were intended directly or indirectly for the government of Iran or Iranian entities. Other U.S. sanctions in effect during this case's relevant time period also required foreign financial institutions to restrict the use of Iranian oil proceeds, if those foreign banks wished to continue to do business with the U.S. financial system.

Atilla and others conspired to provide access to restricted oil revenues through international financial networks, including U.S. financial institutions, to the government of Iran, Iranian entities, and entities identified by the Department of the Treasury Office of Foreign Assets Control as Specially Designated Nationals (SDNs). They did so by, among other things, using Turkish Bank-1, at which Atilla served as Deputy General Manager of International Banking, to engage in transactions involving billions of dollars' worth of petroleum revenues held by the Central Bank of Iran and the National Iranian Oil Company. In particular, they facilitated and protected Turkish Bank-1 customer, international gold trader Reza Zarrab's, ability to supply currency and gold to, and facilitate international financial transactions for, the Government of Iran, Iranian entities, and SDNs using Turkish Bank-1. Many of those financial transactions involved unwitting U.S. financial institutions, in violation of U.S. sanctions against Iran. The elaborate scheme established by Atilla and others also shielded Turkish Bank-1 from U.S. sanctions.

Atilla in particular lied to and deceived U.S. Treasury officials about Turkish Bank-1's activities and its purported compliance efforts in order to avoid subjecting the bank to U.S. sanctions. Additionally, Atilla, Zarrab and others conspired to create and use false and fraudulent documents to disguise prohibited transactions for Iran and make those transactions falsely appear as transactions involving food, thus falling within humanitarian exceptions to the sanctions regime. As a result of this scheme, Atilla and his co-conspirators induced U.S. banks unknowingly to process international financial transactions in violation of the IEEPA, and to launder through the U.S. financial system funds promoting the scheme.

Florida Man Sentenced to 26 Months for Conspiring to Illegally Export Defense Articles to Russia

Vladimir Nevidomy of Hallandale Beach, Florida was sentenced to 26 months in prison, to be followed by three years of supervised release, for conspiring to illegally export military-grade night vision and thermal vision devices, and ammunition primers to Russia. According to information contained in court documents, from as early as April 2013 through November 2013, customers in Russia contacted Nevidomy by email requesting night vision rifle scopes, thermal monoculars and ammunition primers, all of which were on the U.S. Munitions List and subject to export control by the U.S. Department of State. Nevidomy proceeded to obtain at least three ATN MARS 4x4 night-vision rifle scopes and an ODIN 61BW thermal multi-purpose monocular from U.S. vendors by falsely representing to the vendors that the items were not for export.

After the U.S. vendors sent the night vision devices to Nevidomy in South Florida, he exported them to his co-defendant in Russia by either concealing the defense articles in household goods shipments sent through a freight forwarding company or using a private Russian postal service that operated in South Florida. In June 2013,

Nevidomy aided and abetted the export of the ATN MARS 4x4 night-vision rifle scopes from the U.S. to the co-defendant in Russia, and in August 2013, he exported the ODIN 61BW thermal multi-purpose monocular from the U.S. to the co-defendant in Russia.

On or about July 19, 2013, the same co-defendant sent an email to Nevidomy requesting 1,000 large-rifle ammunition primers to be shipped to Vladivostok, Russia. On or about Oct. 2, 2013, Nevidomy attempted to export 1,000 Sellier & Bellot ammunition primers from the U.S. to the co-defendant in Vladivostok. These ammunition primers were seized by U.S. Customs and Border Protection.

These night vision rifle scopes, thermal monocular and ammunition primers required a license or other authorization from the U.S. Department of State before being exported from the U.S. since they were on the U.S. Munitions List. A certified license history check revealed that neither Nevidomy, a Ukraine-born naturalized U.S. citizen, nor his associates ever applied or attempted to apply for an export license from the State Department for the night-vision equipment or ammunition primers.

Ericsson, Inc. settles Potential Civil Liability for an Apparent Violation of the Sudanese Sanctions Regulations

Ericsson AB (EAB), located in Sweden, and Ericsson, Inc. (EUS), located in Texas, both of which are subsidiaries of Telefonaktiebolaget LM Ericsson ("Ericsson"), have agreed to pay $145,893 to settle potential civil liability for an apparent violation of the International Emergency Economic Powers Act (IEEPA) and the Sudanese Sanctions Regulations, 31 C.F.R. part 538 (SSR).

On or around September 22, 2011, EAB signed a letter of intent with the Sudanese subsidiary of a third-country telecommunications company in order to provide equipment and services to upgrade and expand telecommunications network coverage in Sudan starting with a test network. Ericsson opted to connect its test network in Sudan via satellite, as it had done in other underdeveloped areas. Ericsson hired BCom Offshore SAL (BCom) to assist with installing, configuring, and servicing the satellite equipment destined for Sudan.

In late 2011, the high temperatures in Sudan caused some of Ericsson's equipment to malfunction. In response, two now former EAB employees – a radio systems expert and project manager (EAB Employee #1), and a senior engagement director within EAB's business unit responsible for managing the implementation of the Sudanese project (EAB Employee #2) –contacted an EUS subject matter specialist and director of business development with EUS'sHosted Satellite Group (EUS Employee) to request assistance. The EUS Employee initially responded in a January 2, 2012 email to EAB Employee #1 and his manager (EAB Manager)among other EAB employees: "Please do not address any emails relating to this country [Sudan]to me. It is a serious matter and Ericsson can get fined and I can get fired."

Notwithstanding the email cited above, the EAB personnel continued to discuss how to repair the damaged equipment with the EUS Employee while no longer referencing Sudan by name. For example, on January 27, 2012, EAB Employee #1 sent an email referencing Sudan by name to the EAB Manager and EUS Employee, to which the EAB Manager responded in Swedish "do not use that word ;)." Additionally, on February 22, 2012, the EUS Employee sent an email with "East Africa" in the subject line advising EAB Employee #1 and EAB Employee #2 on how to move forward with the Sudan project given the heat constraints.

On or about February 28, 2012, the EUS Employee met with EAB Employee #2 and the Chief Operating Officer (COO) of Ericsson's principal subcontractor, BCom, in Barcelona, Spain at a sales conference to specifically discuss the overheating problem in Sudan. The group decided to solve the issue by purchasing an export controlled U.S.-origin satellite hub capable of withstanding the heat.

On March 22, 2012, at the direction of Employee #1, EAB purchased a satellite hub from a U.S.-based company for delivery to BCom's office in Geneva, Switzerland. On or about March 28, 2012, EAB Employee #1 exchanged emails with Ericsson's compliance department explaining what the satellite hub was for and why its purchase was

necessary. Ericsson's compliance department informed EAB Employee #1 that the supply of such a satellite hub to Sudan would violate Ericsson's internal policy regarding sanctions compliance.

Despite the information from Ericsson's compliance department, the EUS Employee, EAB Employee #1, and BCom's COO agreed to provide the location of the customer purchasing the satellite hub as "Botswana" if future questions arose. Subsequently, on or about April 2, 2012, EAB Employee #1 structured Ericsson's purchase of the satellite hub into a multistage transaction between EAB and BCom. The multistage transaction involved transshipping the hub through Switzerland and Lebanon, and ultimately to Sudan. Every stage of the transaction except the last was invoiced. BCom did not issue an invoice to EAB for the final stage of the transaction taking the satellite hub from Lebanon to Sudan. Ericsson has since terminated its relationship with BCom.

California Residents Plead Guilty to Scheme to Illegally Export Components for Production of Night Vision Rifle Scopes

Naum Morgovsky and Irina Morgovsky, both of Hillsborough, California, pleaded guilty for their respective roles in a scheme to export components for the production of night vision and thermal devices in violation of the Arms Export Control Act. Naum Morgovsky also pleaded guilty to laundering the proceeds of from the scheme.

According to their guilty pleas, Naum Morgovsky and Irina Morgovsky admitted that from April 2012 until Aug. 25, 2016, they conspired to export without the necessary license to a company in Moscow, Russia, numerous scope components, including image intensifier tubes and lenses. They further admitted a coconspirator in Russia communicated to them lists of components necessary for the Russian business to manufacture certain night vision devises. The couple used their U.S. business, Hitek International, to purchase these components and misrepresented to the sellers that the products would not be exported. The couple then shipped the products to Russia and other countries in Europe where an associate arranged for them to be hand-carried into Russia. Further, the couple admitted the scope components they exported were on the U.S. Munitions List and that they therefore were not permitted to export the items without a license from the Department of State, Directorate of Defense Trade Controls. The defendants admitted they knew a license was required to export the components and that they did not obtain a license.

In addition to exporting the components, Naum Morgovsky admitted he took steps to conceal his crimes so that the couple could continue to run the illegal export business undetected. Specifically, he admitted he laundered the proceeds of the export crimes and used the name of a deceased person to conceal the fact that he was the source and owner of a U.S.-based account.

On April 27, 2017, a federal grand jury issued a superseding indictment charging the Morgovskys, along with Mark Migdal, 72, of Portola Valley, California, for their respective roles in three related schemes — the illegal export scheme resolved by today's plea agreements, and two additional bank fraud schemes allegedly involving Naum Morgovsky. With respect to the illegal export scheme, the grand jury charged Naum Morgovesky with conspiracy to violate the Armed Export Control Act, and two counts of money laundering. The grand jury charged Irina Morgovesky with the conspiracy and with misuse of a passport. Pursuant to today's plea agreements, the couple pleaded guilty all the charges with the exception of the passport charge pending against Irina Morgovesky — that charge will be dismissed.

On Nov. 10, 2017, Judge Chhabria severed the case to allow the illegal export charges to be handled separately from the allegations regarding the bank fraud scheme alleged in the April 27, 2017, indictment. The bank fraud charges are still pending against Naum Morgovesky. According to the indictment, Naum Morgovesky conspired with Migdal to defraud two federally-insured banks, now Bank of America and EverBank, by seeking those banks' approval for a short sale of two condominiums. The condominiums were in Kihei, Maui, and were in the same building as a condominium that had been owned by Migdal. The indictment alleges Morgovsky and Midgal conspired to convince the banks to allow the properties to be sold in a short sale to an individual who was deceased. A short sale is a sale in which a lender allows a property to be sold at a price that is less than the amount owed on the loan. Morgovsky also is accused of submitting false statements to the banks about Midgal's

employment status and income. The indictment charges Naum Morgovsky and Migdal with conspiracy to commit bank fraud, and two counts of bank fraud, related to the sale of the Hawaii properties.

On July 25, 2017, Migdal pleaded guilty to his part in the conspiracy and to two counts of making false statements on loan and credit applications. On April 24, 2018, Judge Chhabria sentenced Migdal to 18 months in prison and ordered him to pay a $1,000,000 fine, to pay $460.215 in restitution, and to serve 3 years of supervised release.

Chinese National Arrested for Conspiring to Illegally Export U.S. Origin Goods Used in Anti-Submarine Warfare to China

A Chinese national was arrested and charged in connection with violating export laws by conspiring with employees of an entity affiliated with the People's Liberation Army (PLA) to illegally export U.S. origin goods to China, as well as making false statements to obtain a visa to enter the United States and to become a lawful permanent resident under the EB-5 Immigrant Investor Visa Program.

Shuren Qin, a Chinese national residing in Wellesley, Mass., was charged in a criminal complaint with one count of visa fraud and one count of conspiring to commit violations of U.S. export regulations. Qin was arrested today and will appear in federal court in Boston on June 22, 2018. According to charging documents, Qin was born in the People's Republic of China and became a lawful permanent resident of the United States in 2014. Qin operates several companies in China, which purport to import U.S. and European goods with applications in underwater or marine technologies into China. It is alleged that Qin was in communication with and/or receiving taskings from entities affiliated with the PLA, including the Northwestern Polytechnical University (NWPU), a Chinese military research institute, to obtain items used for anti-submarine warfare.

In 2001, the Department of Commerce designated NWPU on its Entity List because of the national security risks it poses to the U.S. NWPU has worked closely with the PLA on the advancement of its military capabilities. From at least July 2015 to December 2016, Qin allegedly exported approximately 78 hydrophones (devices used to detect and monitor sound underwater) from the United States to NWPU without obtaining the required export licenses from the Department of Commerce, in violation of U.S. export laws. Qin did so by concealing from the U.S. supplier that NWPU was the end-user and causing false information to be filed with the United States Government.

As alleged in court documents, in 2014, Qin made false statements on his visa application. Specifically, he falsely certified that he had never "engaged in export control violations or other unlawful activity." However, it is alleged that Qin engaged in numerous violations of U.S. export laws since 2012. In his petition to become a legal permanent resident of the U.S., Qin again falsely certified that he had never committed any crime. Furthermore, during a November 2017, interview with Customs and Board Patrol Officers, Qin stated that he "only" exported instruments that attach to a buoy. However, Qin had allegedly exported remotely-operated side scan sonar systems, unmanned underwater vehicles, unmanned surface vehicles, robotic boats, and hydrophones. These items have military applications and can be used for weapon delivery systems, anti-submarine warfare, mine counter-measures as well as intelligence, surveillance and reconnaissance activities.

The charge of conspiring to violate U.S. export laws provides for a sentence of no greater than 20 years in prison, three years of supervised release and a fine of $1 million. The charge of visa fraud provides for a sentence of no greater than 10 years in prison, three years of supervised release and a fine of $250,000. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Iranian Businessman Charged with Illegally Exporting Nuclear Nonproliferation-Controlled Materials from Illinois

An Iranian businessman schemed with the owner of a European company to illegally export nuclear nonproliferation-controlled materials to Iran from Illinois. Saeed Valadbaigi, also known as "Saeed Valad" and "Saeed Baigi," plotted in 2011 to illegally export U.S.-origin 7075 T6 Aluminum tubing from Illinois to Iran by way of Belgium and Malaysia, the indictment states. The size and type of the aluminum was used in the missile and aerospace industry and was subject to U.S. regulations for nuclear nonproliferation purposes, the indictment

states. Valadbaigi's smuggling plan was part of an effort to evade U.S. laws and export-control regulations, according to the charges.

In addition to the 7075 Aluminum tubing, the newly unsealed indictment accuses Valadbaigi of illegally exporting titanium sheets from a company in northern Illinois, to Iran, by way of the Republic of Georgia, the United Arab Emirates and Malaysia. At the time of that deal in 2009, Valadbaigi controlled various companies in all three of those countries, the indictment states. The charges further allege that Valadbaigi in 2012 ordered acrylic sheets from a company in Connecticut, and falsely claimed that the sheets would be used only in Hong Kong. He later allegedly arranged for the acrylic sheets to be transshipped to Iran.

The public is reminded that an indictment is not evidence of guilt. The defendant is presumed innocent and entitled to a fair trial at which the government has the burden of proving guilt beyond a reasonable doubt. Each count of wire fraud and attempting to violate the IEEPA carries a maximum sentence of 20 years in prison. The illegal export charge is punishable by up to ten years in prison, while the conspiracy and false statement counts are each punishable by up to five years. If convicted, the Court must impose a reasonable sentence under federal statutes and the advisory U.S. Sentencing Guidelines.

California Man Pleads Guilty to Conspiring to Violate U.S. Sanctions Against Syria

Rasheed Al Jijakl, a Syrian-born naturalized U.S. citizen of Walnut, California, pleaded guilty to a charge of conspiring to export U.S.-origin tactical gear to Syria in violation of the International Emergency Economic Powers Act and Syria Sanctions.

In the factual basis filed as part of the plea agreement, Jijakli admitted that from April 2012 through March 2013, he conspired with other individuals to export tactical gear, including U.S.-origin laser boresighters, day and night vision rifle scopes, and other items (Tactical Gear) from the United States to Syria. From June through July 2012, Jijakli and one of the co-conspirators (Co-conspirator 1) purchased the Tactical Gear. On July 17, 2012, Jijakli traveled from Los Angeles, California to Istanbul, Turkey with the Tactical Gear, with the intent that it would be provided to Syrian rebels training in Turkey and fighting in Syria. Jijakli provided some of the Tactical Gear, specifically the laser boresighters, to a second co-conspirator who Jijakli learned was a member of Ahrar Al-Sham. Jijakli also provided the goods to other armed Syrian insurgent groups in Syria and Turkey. In total, Jijakli and co-conspirators knowingly provided at least 43 laser boresighters, 85-day rifle scopes, 30 night vision rifle scopes, tactical flashlights, a digital monocular, 5 radios, and 1 bulletproof vest to Ahrar Al-Sham and other Syrian rebels in Syria, or with knowledge that the Tactical Gear was going to Syria. Also, in August and September 2012, Jijakli directed co-conspirators to withdraw thousands of dollars from Palmyra Corporation, where Jijakli was the Chief Executive Officer, to pay for Tactical Gear for Syrian rebels.

Canadian Man Sentenced to Prison for Conspiracy to Export Restricted Goods and Technology to Iran

Ghobad Ghasempour, a Canadian national, was sentenced to 42 months in prison for conspiracy to unlawfully export U.S. goods to Iran. Ghasempour was arrested on March 28, 2017 as he entered the United States at Blaine, Washington. An investigation revealed that Ghasempour had used front companies in China and co-conspirators in Iran, Turkey and Portugal to illegally export restricted technology products to Iran.

According to records filed in the case, between 2011 and 2017, Ghasempour and his co-conspirators illegally exported and attempted to export goods and technology to Iran that have both military and non-military uses. Ghasempour exported a thin film measurement system, manufactured by a California company, that is essentially a microscopic tape measure for liquid coatings and parts that are used in cell phones and missiles; he attempted to export an inertial guidance system test table, manufactured by a North Dakota company, used to test the accuracy of gyroscopes that assist in flying commercial and military airplanes; and the conspirators exported two types of thermal imaging cameras, manufactured by an Oregon company, that can be used in commercial security systems and military drones. Some of the items Ghasempour sought to export were intercepted by law enforcement. The conspirators falsified shipping documents and lied to U.S. manufacturers by claiming that the restricted items were being shipped to customers in Turkey and Portugal, knowing that the true destination of these

goods was Iran. The Iranian customers paid the Chinese front companies owned by Ghasempour and a co-conspirator.

Colorado woman sentenced to 3 years in federal prison for illegally exporting firearms to the Dominican Republic

A former member of the U.S. Army stationed at Fort Carson, Colorado, was sentenced to serve three years in federal prison following her criminal conviction for illegally exporting firearms to the Dominican Republic in 2015. On Sept. 1, 2015, a federal grand jury indicted Katherine O'Neal, 43, for numerous firearm and illegal financing-type criminal charges. A superseding indictment was handed down on Nov. 20, 2016, with a second superseding indictment returned on Dec. 5, 2017. A jury found O'Neal guilty of smuggling goods from the United States on March 6, 2018. O'Neal was acquitted on other counts alleging false information on firearm-purchase forms and money laundering.

At trial, the government introduced evidence showing that O'Neal made multiple trips to the Dominican Republic shortly after purchasing firearms in Denver and Colorado Springs, Colorado. On one trip she flew from Denver to the Dominican Republic with 11 firearms in her luggage in early June 2015. O'Neal declared the firearms to the airline, but did not obtain the required State Department export license. Her bags had been misdirected by the airline and were not on her flight. When the bags arrived later, Dominican Republic officials noticed the handguns while examining her baggage. When O'Neal arrived at the airport to claim her luggage, she was arrested. The Dominican Republic has a ban on all imported firearms. A Denver jury found O'Neal guilty of smuggling goods from the United States.

Connecticut Business Owner Sentenced for Export Violation

Imran Khan, of North Haven, was sentenced to three years of probation, the first six months of which Khan must serve in home confinement, for violating U.S. export law. Judge Underhill also ordered Khan to perform 100 hours of community service and pay a $3,000 fine.

According to court documents and statements made in court, from at least 2012 to December 2016, Khan and two of his family members engaged in a scheme to purchase goods that were controlled under the EAR and to export those goods without a license to Pakistan, in violation of the EAR. Through companies conducting business as Brush Locker Tools, Kauser Enterprises-USA and Kauser Enterprises-Pakistan, the three defendants received orders from a Pakistani company that procured materials and equipment for the Pakistani military, requesting them to procure specific products that were subject to the EAR. When U.S. manufacturers asked about the end-user for a product, the defendants either informed the manufacturer that the product would remain in the U.S. or 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 the defendants in Connecticut. The products were then shipped to Pakistan on behalf of either the Pakistan Atomic Energy Commission (PAEC), the Pakistan Space & Upper Atmosphere Research Commission (SUPARCO), or the National Institute of Lasers & Optronics ("NILOP"), all of which were listed on the U.S. Department of Commerce Entity List. The defendants never obtained a license to export any item to the designated entities even though they knew that a license was required prior to export. The defendants received the proceeds for the sale of export-controlled items through wire transactions to a U.S. bank account that the defendants controlled.

On June 1, 2017, Khan pleaded guilty to one count of violating the International Emergency Economic Powers Act. In pleading guilty, he specifically admitted that, between August 2012 and January 2013, he procured, received and exported to PAEC an Alpha Duo Spectrometer without a license to do so.

On March 5, 2018, Khan's father, Muhammad Ismail, and his brother, Kamran Khan, each pleaded guilty to one count of international money laundering, for causing funds to be transferred from Pakistan to the U.S. in connection with the export control violations. In pleading guilty, Ismail and Kamran Khan specifically admitted that, between January and July 2013, they procured, received and exported to SUPARCO, without a license to do so, certain

bagging film that is used for advanced composite fabrication and other high temperature applications where dimensional stability, adherence to sealant tapes and uniform film gage are essential. The proceeds for the sale of the bagging film was wired from Pakistan to the defendants in the U.S.

On July 18, 2018, Judge Underhill sentenced both Muhammad Ismail and Kamran Kahn to 18 months of imprisonment. Ismail and Kamran Khan are both citizens of Pakistan and lawful permanent residents of the U.S.

Chinese National Sentenced to Federal Prison in Scheme to Smuggle Restricted Space Communications Technology to China

A Chinese national who pleaded guilty to participating in a scheme that illegally exported sensitive space communications technology to China was sentenced to serve 46 months in federal prison. Si Chen, who used various aliases, included "Cathy Chen," pleaded guilty in July to conspiracy to violate 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 also pleaded guilty to money laundering and using a forged passport with her photo but a different name that appeared to have been issued by the People's Republic of China.

According to court documents, from March 2013 through the end of 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 included components commonly used in military communications "jammers." Additionally, Chen smuggled communications devices worth more than $100,000 that are commonly used in space communications applications. Chen falsely under-valued the items on the shipping paperwork to avoid arousing suspicion. Chen received payments for the illegally exported products through an account held at a bank in China by a family member.

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.

In addition to participating in the scheme to violate IEEPA, Chen used several aliases and a forged Chinese passport to conceal her smuggling activities. Chen 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, Chen shipped the devices to Hong Kong, and from there the items were transshipped to China. The parcels shipped to Hong Kong bore her false name, along with false product descriptions and monetary values, all done in an effort to avoid attracting law enforcement scrutiny.

Texas Resident Sentenced in South Florida to More Than 6 Years in Prison for Violations of the Cuban Embargo

A Texas resident was sentenced in the Southern District of Florida to 6.5 years in prison for unlawfully exporting to Cuba electronic devices that require a license to export due to national security controls. Bryan Evan Singer, of Bryan, Texas was convicted at trial for attempting to illegally smuggle electronics to Cuba in violation of the Cuban Embargo, in violation of Title 18, United States Code, Section 554, and for making false statements to federal law enforcement, in violation of Title 18, United States Code, Section 1001(a)(2).

On May 2, 2017, Singer intended to travel from Stock Island, Florida to Havana, Cuba aboard his vessel "La Mala." Prior to Singer's departure, law enforcement conducted an outbound inspection of the boat. During the inspection, Singer declared that he was only bringing to Cuba those items observable on the deck, and that the value of those items was less than $2,500. However, law enforcement conducting the search discovered a hidden compartment under a bolted down bed in the cabin of Singer's boat. In the hidden compartment, law enforcement discovered hundreds of electronic devices, valued at over $30,000. Included in those devices were over 300 Ubiquiti Nanostation Network devices, which are designed to provide highly encrypted connections between computer networks over long distances. These devices require a license for export to Cuba, under United States law, because

their capabilities threaten national security. Singer never sought or obtained a license to export to Cuba, prior to his offenses of conviction.

Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies

A Chinese Ministry of State Security (MSS) operative, Yanjun Xu, aka Qu Hui, aka Zhang Hui, has been arrested and charged with conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies. Xu was extradited to the United States.

Beginning in at least December 2013 and continuing until his arrest, Xu targeted certain companies inside and outside the United States that are recognized as leaders in the aviation field. This included GE Aviation. He identified experts who worked for these companies and recruited them to travel to China, often initially under the guise of asking them to deliver a university presentation. Xu and others paid the experts' travel costs and provided stipends.

OFAC Announces Settlement Agreement with JPMorgan Chase Bank under Cuban and Syrian Sanctions

OFAC announced a $5,263,171 settlement with JPMorgan Chase Bank, N.A., to settle potential civil liability for 87 apparent violations of the Cuban Assets Control Regulations; the Iranian Transactions and Sanctions Regulations and the Weapons of Mass Destruction Proliferators Sanctions Regulations. Specifically, the transactions were net settlement payments, of which a very small portion appears to have been attributable to interests of airlines that were at various times on OFAC's List of Specially Designated Nationals and Blocked Persons, blocked pursuant to OFAC sanctions, or located in countries subject to the sanctions programs administered by OFAC. These apparent violations do not include transactions that were exempt from the prohibitions of the International Emergency Economic Powers Act (IEEPA); for example, the apparent violations include transactions such as airline freight charges, which are not exempt. OFAC has determined that JPMC voluntarily self-disclosed the apparent violations, and that the apparent violations constitute a non-egregious case.

Separately, OFAC has issued a Finding of Violation to JPMC regarding violations of the Foreign Narcotics Kingpin Sanctions Regulation, and the Syrian Sanctions Regulations. Specifically, OFAC determined that from approximately 2007 to October 2013, JPMC processed 85 transactions totaling $46,127.04 and maintained eight accounts on behalf of six customers who were contemporaneously identified on the SDN List. OFAC determined that JPMC voluntarily disclosed the violations, and that the violations constitute a non-egregious case.

Chicago Resident Guilty of Trying to Illegally Export Guns and Ammunition to Haiti

A Chicago man has admitted in federal court that he tried to illegally export nearly two dozen guns and ammunition to Haiti from Illinois. Patrick Germain pleaded guilty to one count of knowingly and fraudulently attempting to export firearms contrary to the laws and regulations of the United States. In a written plea agreement, Germain admitted that in 2016 he planned to illegally export 16 handguns, five shotguns, a rifle and ammunition from Evanston to Haiti by way of Miami, Fla. Germain built a plywood container, filled it with the guns and ammunition, and then hid it inside a cargo van, the plea agreement states. The van was then delivered to a shipping company in Miami but law enforcement seized it before it could be transported to Haiti.

According to the plea agreement, Germain in June 2016 purchased the firearms and ammunition from dealers in Illinois. Germain also purchased three vehicles, including the cargo van that he would later use to transport the concealed firearms and ammunition. He then hired an Illinois company to deliver the three vehicles to Miami, where Germain had arranged for a Florida shipping company to transport the vehicles to Haiti. When asked by the Illinois company why the cargo van appeared to be overweight, Germain represented to the driver that the added weight was due to furniture in the backseat. Germain also misled the Florida shipping company by not notifying them that the cargo van was filled with guns and ammunition, according to the plea agreement.

Iranian National Pleads Guilty to Conspiring to Illegally Export Products From the United States to Iran

Arash Sepehri, a citizen of Iran, pleaded guilty on Nov. 7, to a federal charge stemming from his role in a conspiracy to cause the export of controlled goods and technology to Iran, in violation of U.S. Department of Commerce and military controls, as well as in contravention of sanctions imposed against Iran.

According to court documents filed in this case, Sepehri was an employee and a member of the board of directors of an Iranian company, Tajhiz Sanat Shayan, or Tajhiz Sanat Company (TSS). TSS and other companies involved in the conspiracy were listed by the European Union on May 23, 2011, as entities being sanctioned for their involvement in the procurement of components for the Iranian nuclear program. Through TSS and associated companies, Sepehri and others conspired to obtain high-resolution sonar equipment, data input boards, rugged laptops, acoustic transducers and other controlled technology from the United States without obtaining proper licenses and in violation of economic sanctions.

As stated in the court documents, Sepehri and his co-conspirators sought to evade legal controls through a variety of means, including the use of a variety of aliases, United Arab Emirates (UAE)-based front companies and an intermediary shipping company based in Hong Kong. Payments for the goods were arranged through the UAE.

Two Residents of Lebanon Arrested in Seattle in Connection with Scheme to Illegally Export Firearms to Lebanon

Hicham Diab, of Tripoli, Lebanon, and Nafez El Mir, a Canadian citizen residing in Lebanon, were arrested after they traveled to a Seattle warehouse and began hiding firearms in a vehicle they planned to ship to Lebanon. Diab and El Mir appeared in federal court this afternoon, charged with conspiracy to violate the Arms Export Control Act.

According to a criminal complaint unsealed today, in 2016, Diab began communicating with a person in the U.S. who Diab believed was willing to locate firearms for him to smuggle to Lebanon. The person in the U.S. alerted Homeland Security Investigations (HSI) about the contact. Over the course of 2017 and 2018, undercover HSI agents posed as people able and willing to supply firearms sought by Diab in furtherance of his smuggling scheme. In October 2018, Diab made plans to come to the U.S. and successfully wired funds for the purchase of firearms and a vehicle in which to hide the firearms. Diab arrived in Seattle on Nov. 7, and was accompanied by El Mir who, according to Diab, had experience smuggling firearms hidden in automobile panels.

On November 7 and 8, Diab went with the undercover agents to a warehouse containing firearms that had been secured by HSI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and inspected the firearms, which included: twenty Glock handguns, a Smith & Wesson .50 revolver, one FN Fiveseven pistol, an AR15 rifle kit and a M203 grenade launcher. Diab and El Mir, during their November 8 warehouse visit, began hiding the firearms in door panels and bumper space inside a sport-utility vehicle. El Mir also discussed ways to get the vehicle shipped to Lebanon with the hidden weapons. The men were arrested the evening of Nov. 8, as they exited the warehouse.

California Resident Sentenced to 9 Years in Prison and $1 Million Fine for His Scheme to Illegally Export Components for Production of Night Vision and Thermal Devices and Money Laundering

Naum Morgovsky, of Hillsborough, California, was sentenced to 108 months in prison and three years of supervised release for conspiring to illegally export components for the production of night-vision and thermal devices to Russia in violation of the Arms Export Control Act, and for laundering the proceeds of the scheme.

According to their guilty pleas, which occurred during the second day of jury selection on June 12, Naum Morgovsky and Irina Morgovsky admitted that from at least April 2012 until Aug. 25, 2016, they conspired to export without the necessary license to a company called Infratech in Moscow, Russia, numerous night and thermal vision components, including image intensifier tubes and lenses. The couple used their U.S. business, Hitek International, to purchase these components and misrepresented to the sellers that the products would not be exported. The couple then shipped the products to Russia using a variety of front companies and shipment methods. Further, defendants knew the night and thermal vision components they exported were on the U.S.

Munitions List and that they therefore were not permitted to export the items without a license from the Department of State, Directorate of Defense Trade Controls, which they never sought.

In addition to exporting the components, Judge Chhabria found that Naum Morgovsky, a naturalized U.S. citizen originally of Ukraine, had taken steps to conceal his crimes so that the couple could continue to operate the illegal export business undetected, and that Naum Morgovsky laundered the proceeds of the export crimes. As the government alleged, Naum Morgovksy used numerous front companies and the identity of at least one deceased person in furtherance of the scheme. In handing down the sentence, Judge Chhabria noted that this was a "very serious crime" and that "people who export night vision . . . need to know that there is a penalty."

For her part in the scheme, the grand jury charged Irina Morgovsky with conspiracy to violate the Armed Export Control Act and with misuse of a passport. She pleaded guilty to the charges and on Oct. 31, Judge Chhabria sentenced her to 18 months in prison for her role in the scheme.

California Man Sentenced to Nearly 4 Years in Federal Prison for Scheme to Smuggle Rifle Scopes and Tactical Equipment to Syria

Rasheed Al Jijakli, 57, a Syrian-born naturalized U.S. citizen who resides in Walnut, California, was sentenced to 46 months in prison for his role in a scheme to smuggle rifle scopes and other tactical gear to Syria in violation of the International Emergency Economic Powers Act and sanctions imposed on Syria by the United States. Jijakli pleaded guilty to the felony offense on Aug. 13 and admitted he conspired with others to export tactical gear from the United States to Syria. That tactical gear included U.S.-origin laser boresighters, and day- and night-vision rifle scopes.

From June through July of 2012, Jijakli and a co-conspirator purchased the tactical gear. On July 17, 2012, Jijakli traveled with the tactical gear from Los Angeles to Istanbul with the intent that it would be provided to Syrian rebels training in Turkey and fighting in Syria.

Jijakli provided some of the tactical gear, specifically the laser boresighters, to a second co-conspirator, who Jijakli learned was a member of the militant group Ahrar Al-Sham. Jijakli also provided the goods to other armed Syrian insurgent groups in Syria and Turkey.

Jijakli and his co-conspirators knowingly provided at least 43 laser boresighters, 85 day rifle scopes, 30 night-vision rifle scopes, tactical flashlights, a digital monocular, five radios, and one bulletproof vest to Ahrar Al-Sham and other Syrian rebels in Syria, or with knowledge that the tactical gear was going to Syria.

Additionally, in August and September 2012, Jijakli directed co-conspirators to withdraw thousands of dollars from Palmyra Corporation, where Jijakli was the chief executive officer, to pay for tactical gear that would be provided to Syrian rebels. In his plea agreement, Jijakli specifically admitted directing that $17,000 from Palmyra be used to purchase tactical gear intended for Syrian rebels.

Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Zoltek Companies, Inc.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced a $7,772,102 settlement with Zoltek Companies, Inc. ("Zoltek") and its subsidiaries worldwide. Zoltek — a holding company headquartered in Bridgeton, Missouri, and the owner of Zoltek Corporation ("Zoltek U.S."), located in the United States, and Zoltek Vegyipari ZRT ("Zoltek ZRT"), located in Hungary — has agreed to settle its potential civil liability for 26 apparent violations of the Belarus Sanctions Regulations, 31 C.F.R. part 548 (BSR). The apparent violations involve Zoltek U.S. approving 26 purchases of acrylonitrile — a chemical used in the production of carbon fiber — between Zoltek ZRT and J.S.C. Naftan ("Naftan"), a Belarusian entity OFAC designated on August 11, 2011 pursuant to Executive Order 13405 of June 16, 2006, "Blocking Property of Certain Persons Undermining Democratic Processes or Institutions in Belarus," and identified on OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"), in apparent violation of § 548.201 of the BSR. OFAC determined that Zoltek and Zoltek U.S. voluntarily self-disclosed the apparent violations and that the apparent violations that

occurred prior to February 2015 constitute a non-egregious case, and that the apparent violations that occurred after February 2015 constitute an egregious case.

Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Yantai Jereh Oilfield Services Group Co. Ltd.

OFAC announced a $2,774,972 settlement with Yantai Jereh Oilfield Services Group Co. Ltd. and its affiliated companies and subsidiaries worldwide (collectively referred to hereafter as the "Jereh Group"). The Jereh Group's settlement with OFAC is concurrent with a settlement agreement between the Jereh Group and the U.S. Department of Commerce's Bureau of Industry and Security. The Jereh Group, headquartered in the city of Yantai, China, has agreed to settle potential civil liability for 11 apparent violations of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560 (ITSR). The apparent violations involved the exportation or re-exportation, and attempted exportation or re-exportation of U.S.-origin goods ultimately intended for end-users in Iran by way of China. The Jereh Group also exported certain U.S.-origin items with knowledge or reason to know that the items were intended for production of, for commingling with, or for incorporation into goods made in China to be supplied, transshipped, or re-exported to end-users in Iran. Two of the 11 shipments were seized by U.S. Customs and Border Protection prior to exiting the United States. The goods in question include oilfield equipment such as spare parts, coiled tubing strings, and pump sets in violation §§ 560.203 and 560.204 of the ITSR. OFAC determined that the Jereh Group did not voluntarily self-disclose the apparent violations and that the apparent violations constitute an egregious case.

Lebanese Businessman Tied by Treasury Department to Hezbollah Pleads Guilty to Money Laundering Conspiracy in Furtherance of Violations of U.S. Sanctions

Kassim Tajideen, the operator of a network of businesses in Lebanon and Africa whom the U.S. Department of the Treasury designated as an important financial supporter to the Hezbollah terror organization, pleaded guilty to charges associated with evading U.S. sanctions imposed on him. Tajideen, 63, of Beirut, Lebanon, pleaded guilty before U.S. District Court Judge Reggie B. Walton in the U.S. District Court for the District of Columbia, to conspiracy to launder monetary instruments, in furtherance of violating the International Emergency Economic Powers Act (IEEPA). Tajideen was designated by the U.S. Department of the Treasury as a Specially Designated Global Terrorist in May 2009 as a result of his provision of significant financial support to Hezbollah, which was named a Foreign Terrorist Organization by the U.S. Department of State. This designation prohibited Tajideen from being involved in, or benefiting from transactions, involving U.S. persons or companies without a license from the Department of the Treasury.

According to the statement of facts signed by Tajideen in conjunction with his plea, after his designation, Tajideen conspired with at least five other persons to conduct over $50 million in transactions with U.S. businesses that violated these prohibitions. In addition, Tajideen and his co-conspirators knowingly engaged in transactions outside of the United States, which involved transmissions of as much as $1 billion through the United States financial system from places outside the United States.

Canadian Authorities Arrest CFO of Huawei Technologies at U.S. Request

Canadian authorities in Vancouver have arrested Huawei Technologies Co.'s chief financial officer at the request of the U.S. for alleged violations of Iran sanctions, the latest move by Washington against the Chinese cellular-technology giant. A spokesman for Canada's justice department said Meng Wanzhou was arrested in Vancouver on Dec. 1 and is sought for extradition by the U.S. A bail hearing has been tentatively scheduled for Friday, according to the spokesman. Ms. Meng, the daughter of Huawei's founder, Ren Zhengfei, also serves as the company's deputy chairwoman.

The arrest comes at a critical juncture in U.S.-Chinese relations. President Trump and Chinese President Xi Jinping last weekend agreed to a temporary truce in a trade spat to negotiate a settlement. The U.S. has raised other concerns with China, ranging from spying to intellectual-property theft to Beijing's military posture in the South China Sea. China has said its actions are appropriate.

The U.S. has undertaken a campaign against Huawei, which is viewed as a national-security threat because of its alleged ties to the Chinese government. In the past year, Washington has taken a series of steps to restrict Huawei's business on American soil and, more recently, launched an extraordinary international outreach campaign to persuade allied countries to enact similar curbs.

China strongly protests the arrest and has urged both U.S. and Canadian officials to free Ms. Meng, according to a statement released by the Chinese Embassy in Canada. The U.S. is seeking Ms. Meng's extradition so as to have her appear in federal court in the Eastern District of New York, according to people familiar with the matter.