Don't Let This HAPPEN TO YOU!

Actual Investigations *of* Export Control *and* Antiboycott Violations

MARCH 2024

U.S. DEPARTMENT OF COMMERCE
Bureau of Industry and Security
Export Enforcement

DON'T LET THIS HAPPEN TO YOU!!!

An Introduction to the Consequences of Violating U.S. Export Control Law

Actual Investigations of Export Control and Antiboycott Violations

MARCH 2024

EXPORT ENFORCEMENT

BUREAU OF INDUSTRY AND SECURITY

U.S. DEPARTMENT OF COMMERCE

Summary Table of Contents

Dear Members of the Exporting Community,

Export controls have never been more important to our collective security interests than they are today. In the current climate of growing threats by nation-state actors, the agents and analysts of the Bureau of Industry and Security's (BIS) Export Enforcement team are dedicated to keeping our country's most sensitive items out of the world's most dangerous hands. Since December 2021, working under the leadership of President Biden and Secretary Raimondo, I have had the distinct honor of overseeing these efforts as the Assistant Secretary for Export Enforcement.

Last month marked the start of the third year of Russia's full-scale invasion of Ukraine, a brutal assault reliant on illicit acquisitions of western technologies like semiconductors and machine tools, as well as military alliances with pariah states like Iran and North Korea. So far, the full-scale invasion has resulted in the continued indiscriminate killing of Ukrainian soldiers and citizens as well as the destruction of hospitals, schools, and critical infrastructure. At the same time, the People's Republic of China continues its destabilizing activities, leveraging advanced technologies like artificial intelligence (AI) to modernize its military, enable human rights abuses against minorities, threaten its neighbors, and supplant U.S. interests in the Indo-Pacific. In addition to its support of Russia's war effort, Iran supplies weapons containing Western components to terrorist proxies such as Hamas, Hezbollah, the Houthis, and others who are bent on attacking U.S. forces stationed in Iraq, destabilizing the Middle East, and disrupting the free flow of commerce vital to global trade.

To meet these challenges, Export Enforcement has taken decisive action over the past year to prioritize its enforcement efforts in collaboration with interagency and international partners. These efforts were exemplified by our establishment in February 2023 of the Disruptive Technology Strike Force with the Department of Justice. The Strike Force, which includes partners from the Federal Bureau of Investigation, Homeland Security Investigations, and, as of February 2024, the Defense Criminal Investigative Service, aims to vigorously protect advanced technologies – like AI, quantum computing, and biotechnology – from being unlawfully acquired by foreign adversaries. Together, Strike Force agencies have taken an all-tools approach to aggressively pursue criminal and administrative enforcement, along with regulatory actions, against illegal procurement networks and to prevent nation-state actors from illicitly acquiring our most sensitive technology.

Forging international partnerships is another priority for us. Recent highlights include establishing a Disruptive Technology Protection Network with Japan and the Republic of Korea and establishing enforcement coordination mechanisms with partners in the G7 and in the "Export Enforcement Five" (or "E5") countries of Australia, Canada, New Zealand, and the United Kingdom. We've also implemented new data sharing arrangements, including with the European Anti-Fraud Office (OLAF), to allow closer coordination on export enforcement.

But no partnership is more important than our partnership with the private sector. While we are always prepared to enforce against those who break our rules, our strong preference is

for companies to invest in compliance upfront. That way, the national security harm that results when our rules are broken can be avoided.

Over the past year, we implemented policy changes, including changes to our Voluntary Self-Disclosure program, designed to ease the administrative burden for industry, promote compliance, and create a level playing field. We also issued a series of joint red-flag guidance documents, best practices, and alerts with interagency and international partners, including the Departments of Justice, Homeland Security, State, the Treasury, and the E5, to educate financial institutions, transportation industries, and the exporting community on global export control evasion tactics.

Export Enforcement's efforts in 2023 resulted in the highest number ever of convictions, temporary denial orders, and post-conviction denial orders, as well as the largest standalone administrative penalty in BIS history. You can read examples of these outcomes in this publication, aptly titled "Don't Let This Happen to You." The publication is intended to highlight the seriousness of administrative and criminal enforcement outcomes as a reminder to the exporting community of what can happen when there's a failure to comply with our rules. You do not want to become one of the case examples listed here – and we do not want you to become one either. We encourage you to work with your local Office of Export Enforcement field offices to help you understand our rules and how to comply with them.

Preventing our most sensitive goods and technologies from falling into the wrong hands is a shared endeavor. We look forward to continuing to partner with you in this critically important effort.

Sincerely,

Matthew S. Axelrod
Assistant Secretary for Export Enforcement

Introduction to Enforcement of U.S. Export Controls

Mission and Organization

The U.S. Department of Commerce's Bureau of Industry and Security (BIS) administers and enforces export controls on dual-use and certain munitions items for the Department of Commerce through the Export Administration Regulations (EAR) under the authority of the Export Control Reform Act of 2018 (ECRA).[1] Dual-use items are commodities, software, or technology that have both commercial and military or proliferation applications. These include items related to supercomputing and exascale computing, artificial intelligence, advanced manufacturing equipment and materials, quantum computing, and biosciences, along with firearms and related materiel. Since they are items on the Wassenaar Arrangement Munitions List (WAML) or were formerly on the U.S. Munitions List (USML), controlled items listed under 600 series Export Control Classification Numbers (ECCNs) are enumerated on the Commerce Control List (CCL). Likewise, certain satellite-related items formerly listed on the USML are now enumerated on the CCL in the 9x515 ECCNs, while certain firearms and ammunition transferred to the CCL from the USML are listed under the 0x5zz series ECCNs.

Other federal agencies with a role in administering U.S. export controls include the Department of State, which controls the export of defense articles and defense services subject to the International Traffic in Arms Regulations (ITAR); the Department of Energy, which controls exports and reexports of technology related to the production of special nuclear materials; the Nuclear Regulatory Commission, which controls the export of certain nuclear materials and equipment; and the Department of the Treasury, which administers economic sanctions programs.

BIS Export Enforcement protects and promotes U.S. national security, foreign policy, and economic interests by investigating violations, interdicting illegal exports, conducting end-use checks, helping companies to improve export compliance practices and to identify suspicious inquiries, supporting the licensing process by evaluating the bona fides of transaction parties, aggressively pursuing violators of export control regulations and initiating criminal prosecution or administrative enforcement actions, promoting U.S. strategic technology leadership, and partnering with counterparts throughout the U.S. government and internationally. By prioritizing its enforcement mission, BIS Export Enforcement has evolved over the past four decades into a sophisticated law enforcement agency with criminal investigators and enforcement analysts who are singularly focused on export enforcement and work closely together with licensing officers within a single bureau of the government.

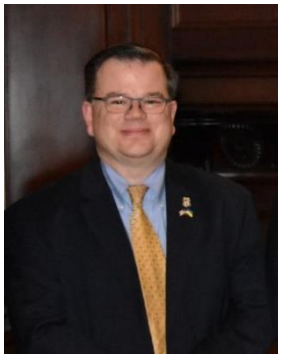
Deputy Assistant Secretary for Export Enforcement Kevin Kurland

[1] The Export Administration Regulations originally issued pursuant to the Export Administration Act (50 U.S.C. §§ 4601- 4623 (Supp. III 2015)) (EAA). On August 21, 2001, the EAA lapsed and the President, through Executive Order 13222 of August 17, 2001 (3 C.F.R., 2001 Comp. 783 (2002)), which was extended by successive Presidential Notices, the most recent being that of August 13, 2020 (85 Fed. Reg. 49,939 (Aug. 14, 2020)), continued the Regulations in effect under the International Emergency Economic Powers Act (50 U.S.C. § 1701, et seq. (2012)) (IEEPA). On August 13, 2018, the President signed into law the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which includes the Export Control Reform Act of 2018, 50 U.S.C. §§ 4801-4852 (ECRA). Section 1768 of ECRA provides, in pertinent part, that all rules and regulations that were made or issued under the EAA, including as continued in effect pursuant to IEEPA, and were in effect as of ECRA's date of enactment (August 13, 2018), shall continue in effect until modified, superseded, set aside, or revoked through action undertaken pursuant to the authority provided under ECRA.

BIS's jurisdiction has expanded to cover tens of thousands of munitions items transferred from the ITAR to the EAR (see below for additional information on the Export Control Reform (ECR) initiative). These transfers have enhanced U.S. Government oversight on such munitions exports because the specialized resources and authorities of Export Enforcement augment the existing enforcement resources of other federal agencies dedicated to protecting U.S. national security. ECR has also created interagency information sharing and coordination mechanisms to leverage U.S. Government export enforcement and compliance resources more effectively.

Export Enforcement has three program offices: the Office of Export Enforcement (OEE), the Office of Enforcement Analysis (OEA), and the Office of Antiboycott Compliance (OAC). Export Enforcement blends the unique talents of its program offices to channel enforcement efforts against current and emerging threats to U.S. national security and foreign policy. Those unique talents are described in the following paragraphs.

Office of Export Enforcement



Office of Export Enforcement Director John D. Sonderman

The Office of Export Enforcement (OEE) maintains Special Agents at offices across the United States, including its headquarters in Washington, DC, nine field offices located in Boston, Chicago, Dallas, Los Angeles, Miami, New York, Northern Virginia, Phoenix, and San Jose, and resident offices in Atlanta, Houston and Portland. In addition, OEE Special Agents have been deployed to FBI field offices in Boise, Charlotte, Cincinnati, Detroit, Huntsville, Las Vegas, Memphis, Minneapolis, New Haven, Pittsburgh, Rapid City, Salt Lake City, San Diego, Savannah, Seattle, St. Louis, and Tampa, as well as to Defense Criminal Investigative Service (DCIS) offices in Denver and San Antonio, and the Homeland Security Investigations (HSI) Field Office in Baltimore to provide enhanced coverage for investigating export violations.

OEE Special Agents are sworn federal law enforcement officers with authority to bear firearms, make arrests, execute search warrants, serve subpoenas, search, inspect, detain, seize, and administratively forfeit items about to be illegally exported, reexported, or transferred (in-country), as well as conveyances involved in such exports, reexports, and transfers (in-country), and order the redelivery to the United States of items exported in violation of U.S. law. OEE is the only federal law enforcement agency exclusively dedicated to the enforcement of export control laws, and that singular focus allows for the development of the requisite subject matter expertise to be able to effectively enforce a complex regulatory regime. Some cases may require years of thorough investigation to bring a matter to a successful completion. OEE investigations are initiated on information and intelligence obtained from a variety of sources, including routine review of export documentation, overseas end-use monitoring, and industry information. OEE investigates both export violations by U.S. persons and the unauthorized reexport or transfer (in-country) by foreign persons of items subject to the EAR to prohibited end uses, end users, or destinations. OEE also has the authority to enforce restrictions on specific activities of U.S. persons, including those unrelated to shipments of items subject to the EAR, such as brokering, servicing, financing, or freight forwarding in connection with certain foreign weapons of mass destruction and military-intelligence end uses and end users. OEE works closely with other federal law enforcement agencies to identify and act on export violations and with industry to raise awareness of compliance best practices and "red flag" indicators of potential illicit activities.[2] For example, OEE works with U.S. Customs and Border Protection to train outbound officers on EAR requirements to identify suspicious cargoes for detention.

[2] An illustrative list of indicators of possible unlawful diversion is found in Supplement No. 3 to Part 732 of the Export Administration Regulations (EAR), 15 C.F.R. Parts 730 – 774.

Based on information gathered during an investigation, OEE works closely with attorneys from the Department of Justice to prosecute violators criminally, as well as with the Office of Chief Counsel for Industry and Security to bring administrative charges. Additionally, Export Enforcement acts where appropriate to place parties on the BIS Entity List, Unverified List, Denied Persons List, and Military End-User List. Export Enforcement is co-located in the same Department of Commerce bureau as Export Administration, allowing for close cooperation in the administration and enforcement of export controls. Export Enforcement provides advice and comments on the enforceability of new policies and regulations, and works closely with Export Administration to routinely review export transactions to ensure compliance with the EAR. Such review includes:

- Confirming whether exported items were properly classified;
- Verifying required export authorizations, if applicable (e.g., the required export license was obtained prior to the shipment and the transaction complies with the license conditions, a license exception was available and properly used, or the item did not require a license for export to the end user and destination); and
- Determining whether the transaction involved any apparent violations of the EAR (e.g., related to the ten General Prohibitions, end-use-based or end-user-based controls or proscribed parties).[3]

DISRUPTIVE TECHNOLOGY STRIKE FORCE

In February 2023, the U.S. Department of Justice and the U.S. Department of Commerce launched the Disruptive Technology Strike Force (DTSF), designed to bring together experts throughout the government – including the FBI, HSI, DCIS, and U.S. Attorney's Offices throughout the country – to target illicit actors, strengthen supply chains, and protect critical technological assets from being acquired or used by nation-state adversaries. The Strike Force uses an all-tools approach – i.e., criminal prosecutions, administrative penalties, Entity Listings – to prevent and deter violations involving advanced technologies that can be used in new or novel ways to enhance nation state adversaries' military capabilities or support mass surveillance programs that enable human rights abuses.

In the 12 months since its formation, the DTSF has:

- Charged 15 cases involving alleged sanctions and export control violations, smuggling conspiracies, and other offenses
- Issued Temporary Denial Orders against 29 entities
- Led to numerous parties being placed on Commerce's Entity List and Treasury's Specially Designated Nationals and Blocked Persons List

Export Enforcement Assistant Secretary Matthew S. Axelrod at a press conference announcing criminal charges in multiple cases in connection with the multi-agency Disruptive Technology Strike Force

[3] See Part 736 of the EAR for details on the ten General Prohibitions.

In fiscal year 2023, BIS investigations led to the criminal conviction of 67 individuals and businesses for export violations with penalties of $1,710,019 in criminal fines, $3,383,410 in forfeitures, $9,020,618 in restitution and 1,779 months of imprisonment. In addition, OEE and the Office of Chief Counsel for Industry & Security completed 147 administrative export matters, resulting in $303,401,583 in civil penalties. The convictions, restitution, months of imprisonment, and civil penalties all represent the highest in OEE's history.

In addition to our Headquarters at the Department of Commerce in Washington, DC, OEE has nine field offices located in Boston, Chicago, Dallas, Los Angeles, New York, Miami, Northern Virginia, Phoenix, and San Jose. There are three resident offices located in Atlanta, Houston, and Portland as well.

Office of Enforcement Analysis

The Office of Enforcement Analysis (OEA) supports the identification, prevention and investigation of illegal exports, reexports and transfers (in-country) of items subject to the EAR, as well as certain activities of U.S. persons related to the proliferation of weapons of mass destruction (WMD) or support to certain military-intelligence end uses and end users, and supports the prosecution of the parties responsible by: 1) analyzing the *bona fides* of foreign transaction parties to license applications (i.e., their reliability as recipients of U.S.-origin items); 2) monitoring end uses and end users of U.S.-origin exports; 3) identifying suspicious inquiries to alert U.S. companies; 4) developing investigative leads; 5) providing analytical case support; and 6) engaging with key trading partners. OEA accomplishes this mission through its Strategic Intelligence Division, International Operations Division, Export Control Officer Program, and Investigative Analysis Division.

OEA's Strategic Intelligence Division serves as the executive agent for the interagency Information Triage Unit, or "ITU," and vets the *bona fides* of foreign parties to license applications. The Strategic Intelligence Division is responsible for assembling and disseminating relevant all-source information from which to base informed decisions on proposed exports requiring a U.S. Government license.

OEA's International Operations Division screens BIS license applications and reviews export documentation to select candidates for pre-license checks (PLCs) and post-shipment verifications (PSVs), collectively referred to as end-use checks (EUCs). PLCs validate information on BIS export license applications, including end-user reliability. PSVs strengthen assurances that exporters, consignees, end users, and other transaction parties comply with the terms of export licenses and the EAR. This end-use monitoring program supports the export licensing process by confirming the end uses and end users of items subject to the EAR through on-site verification and generates information about potential export violations. This division, working with regional Export Control Officers (ECOs) stationed abroad, supports Export Enforcement's role in bilateral discussions on export control cooperation and coordination to increase capacity to prevent the diversion of U.S.-origin items.

OEA's ECO Program assigns Special Agents under limited-term Foreign Service appointments under the Department of Commerce's Foreign Commercial Service in nine strategic overseas locations. These locations are critical to BIS's mission and are located in Beijing, China; Hong Kong, China; Dubai, United Arab Emirates (UAE); New Delhi, India; Frankfurt, Germany; Helsinki, Finland; Taipei, Taiwan; Istanbul, Turkey; and Singapore. In addition, it deploys an analyst as an Export Control Attaché to Ottawa, Canada. ECO positions have regional responsibilities that extend their reach to more than 75 additional countries. As BIS's representatives overseas, ECOs leverage their law enforcement, commercial, and diplomatic skills to expand the U.S. government's export control activities beyond its borders and into key overseas trade centers. ECOs focus on export control enforcement and compliance by conducting end-use checks, establishing the *bona fides* of foreign parties to transactions subject to the EAR, and coordinating with U.S. and foreign government agencies to ensure effective export controls and secure trade. BIS end-use checks are also conducted by domestically based OEE Special Agents under the Sentinel Program, and occasionally by U.S. Embassy personnel. In FY2023, BIS completed 1,509 end-use checks in 62 countries.

Finally, OEA's Investigative Analysis Division is responsible for producing investigative leads relating to potential export violations for outreach and investigation by OEE Special Agents. Investigative leads are developed from multiple sources of information, including industry, government partners, and extensive reviews of export and license data, and classified and open sources of information. In addition, OEA's Investigative Analysis Division provides research and analytical case support to OEE investigations.

Office of Antiboycott Compliance

The Office of Antiboycott Compliance (OAC) administers and enforces the antiboycott provisions of the EAR. The OAC carries out its mandate through a threefold approach: monitoring boycott requests received by U.S. businesses; bringing enforcement actions when necessary; and guiding U.S. businesses on the application of the EAR to transactions. In addition to these traditional compliance tools, OAC liaises with foreign governments to eliminate boycott requests at their points of origin. By working with U.S. Government partners in the Office of the U.S. Trade Representative and at the Department of State, OAC has met with officials of boycotting countries issuing boycott-related requests. By pointing out the barrier to trade that boycott requests impose, OAC can ensure the removal of prohibited language, thereby enabling U.S. businesses to compete on an equal footing in various markets.

Authorities and Remedies

Criminal and Civil Penalties

In cases involving a willful violation of the EAR, violators may be subject to both criminal fines and administrative penalties. Administrative penalties may also be imposed when there is no willful intent, meaning that administrative cases can be brought in a much wider variety of circumstances than criminal cases. BIS has a unique range and combination of administrative enforcement authorities. These include the imposition of civil penalties, denial of export privileges, and placement of individuals and entities on lists that restrict or prohibit their involvement in export and reexport transactions. Under ECRA, criminal penalties can reach 20 years imprisonment and $1 million per violation. Administrative monetary penalties can reach $364,992 per violation (subject to adjustment in accordance with U.S. law, e.g., the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (Pub. L. 114 - 74, sec. 701)) or twice the value of the transaction, whichever is greater.

The EAR provide that in appropriate cases the payment of a civil penalty may be suspended or deferred in whole or in part during a probationary period. If the probationary conditions are not fulfilled, the suspended or deferred penalty is subject to activation and collection. Penalty suspensions may occur, for example, when the respondent has demonstrated, typically through the submission of financial

statements and tax returns, that it is unable to pay some or all of the penalty that would be appropriate for the violations at issue. Penalties may also be suspended in whole or in part as a result of exceptional cooperation with the investigation where the agency nonetheless decides that a suspended penalty should be imposed for its deterrent effect.

One of the most significant enforcement tools in the BIS arsenal is our administrative enforcement authorities. The Guidelines, set forth in Supplement No. 1 to Part 766, capture OEE's administrative enforcement policies and procedures in several ways. First, the Guidelines outline the following four categories of Factors affecting administrative sanctions: 1) Aggravating Factors; 2) General Factors that could be considered either aggravating or mitigating depending upon the circumstances; 3) Mitigating Factors; and 4) other Relevant Factors on a case- by-case basis, such as related violations or other enforcement action.

Additionally, the Guidelines formally account for the substantial increase in the maximum penalties for violations of the EAR and distinguish between egregious and non-egregious civil monetary penalty cases. Finally, reference in the Guidelines to "transaction value" provides sufficient flexibility to allow for the determination of an appropriate transaction value in a wide variety of circumstances. Amounts set forth in a schedule provide for a graduated series of penalties based on the underlying transaction values, reflecting appropriate starting points for penalty calculations in non-egregious cases not voluntarily disclosed to OEE. The base penalty amount for a non-egregious case involving a VSD equals one-half of the transaction value, capped at the statutory maximum per violation of the EAR. The base penalty amount for cases deemed to be egregious brought to OEE's attention by means other than a VSD, shall be an amount up to the statutory maximum. For those egregious cases involving a VSD, the base penalty amount shall be an amount up to half the statutory maximum.

INCREASING TRANSPARENCY THROUGH PENALTY GUIDANCE

BIS provides guidance (found in Supplement No. 1 to Part 766 of the EAR) to provide the public with a comprehensive description of how BIS determines appropriate penalties in the settlement of administrative export control enforcement cases. It explains that BIS carefully considers each settlement in light of the facts and circumstances of the case, relevant precedent, and BIS's objective to achieve an appropriate level of penalty and deterrent effect.

The penalty guidance can be found online at *https://www.bis.doc.gov/index.php/documents/pdfs/1567-adminstrative-enforcement-guidelines/file*

Several factors are taken into account when determining the appropriate administrative penalty. The penalty guidance encourages parties to provide information to BIS that would be helpful in the application of the guidance to their cases. At the same time, when a party informs us about another party's conduct and that information allows us to take enforcement action, we will consider it "extraordinary cooperation" and treat it as a mitigating factor if the notifying party engages in prohibited conduct in the future.

Some factors are given up to a specific percentage of mitigation and are treated as considerably more significant than factors that are not so designated. The Factors set forth in the Guidelines are reconstituted into the following:

Aggravating Factors

A. Willful or Reckless Violation of Law
B. Awareness of Conduct at Issue
C. Harm to Regulatory Program Objectives

General Factors

D. Individual Characteristics
E. Compliance Program

Mitigating Factors

F. Remedial Response
G. Exceptional Cooperation with OEE
H. License Was Likely To Be Approved

Other Relevant Factors Considered on a Case-by-Case Basis

I. Related Violations
J. Multiple Unrelated Violations
K. Other Enforcement Action
L. Future Compliance/Deterrence Effect
M. Other Factors that OEE Deems Relevant

Voluntary Self-Disclosures

Export Enforcement at BIS encourages the submission of voluntary self-disclosures (VSDs) by parties who believe they may have violated the EAR. BIS encourages parties that believe they may have violated export controls or economic sanctions administered by other U.S. government agencies, or failed to file complete and accurate electronic export information (EEI) as required by the Foreign Trade Regulations (FTR) (15 CFR part 30), to file disclosures concurrently with BIS and all other relevant federal agencies. VSDs are a compelling indicator of a party's intent to comply with U.S. export control requirements. Parties can submit an initial disclosure when the violations are first uncovered and follow-up with a complete narrative within 180 days.[4] OEE carefully reviews VSDs received from disclosing parties to determine if violations of the EAR have occurred and to determine the appropriate corrective action when violations have taken place.

Since June 30, 2022, a 'fast track' resolution policy for VSDs involving minor or technical infractions has been in effect. Under that policy, qualifying VSDs receive a warning letter or no-action letter within 60 days of the final submission of the VSD. A January 2024 announcement further enhanced the VSD process by adopting an 'abbreviated narrative account' option for VSD submissions involving violations where no aggravating factors are present.

In January 2024, BIS published a policy memorandum announcing further enhancements to the VSD program that addressed:

- Manner of Submission
- Abbreviated Narrative Account of Certain Disclosures
- What Makes a Violation Significant
- Treatment of Unlawfully Exported Items

VSDs are a compelling indicator of a party's intent to comply with U.S. export control requirements in the present and the future. Export Enforcement may afford significant mitigation to parties that submit VSDs while at the same time may aggravate penalties when parties make a deliberate decision not to disclose a significant possible violation.

Additional VSD policy guidance can be found at
https://www.bis.doc.gov/index.php/enforcement/oee/voluntary-self-disclosure

[4] See Section 764.5 of the EAR for details on how to submit a VSD.

Denial of Export Privileges

BIS has the authority and discretion to deny all export privileges under the EAR of a domestic or foreign individual or company. Consider the potentially catastrophic impact upon a person or organization of not being able to export, reexport, transfer (in-country), or receive any item – including an EAR99 item – that is subject to the EAR. BIS may impose a denial of export privileges as a sanction in an administrative case, or as a result of a person's criminal conviction under certain statutes. A denial of export privileges prohibits a person from participating in any transactions subject to the EAR. Furthermore, it is unlawful for other businesses and individuals to participate in an export, reexport, or transfer (in-country) subject to the EAR with a denied person.

Denial of export privileges may be imposed as part of an administrative penalty. Under 50 U.S.C. 4819(e), a denial of export privileges may be imposed for up to ten years from the date of a person's conviction under ECRA (or any regulation, license, or order issued thereunder), IEEPA, or Section 38 of the Arms Export Control Act, or one of the several espionage, conspiracy, smuggling, and false statement-related statutes. In cases where no administrative charges are brought, there is no limit to the period of export denial. The standard terms of a BIS denial order are described in Supplement No. 1 to Part 764 of the EAR. (Note: 50 U.S.C. 4819(e) does not apply to convictions that arise out of antiboycott violations.)

In addition, the Assistant Secretary for Export Enforcement may issue a Temporary Denial Order (TDO) denying any, or (typically) all, of the export privileges of a company or individual to prevent an imminent or ongoing export control violation. These orders are issued ex parte for a renewable 180-day period or for a period of no more than one year if a party has engaged in a pattern of repeated, ongoing, and/or continuous apparent violations of the EAR, and deny not only the right to export from the United States, but also the right to receive or participate in exports from the United States. TDOs are also described in Section 766.24 of the EAR.

BIS-Administered Lists

The Department of Commerce maintains four screening lists, which advise the exporting public that listed persons are subject to specific restrictions. In the event an entity, company, or individual on one of the following lists appears to match a potential party in a transaction subject to the EAR, additional due diligence is required before proceeding to ensure the transaction does not violate the EAR. These lists are available on the BIS website *at* *https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern*. They are also included in the U.S. Government Consolidated Screening List, a comprehensive screening system containing export-related lists managed by the Departments of State, Treasury and Commerce, available at *https://www.export.gov/article?id=Consolidated-Screening-List*. In addition, Section 744.22 identifies a non-exhaustive list of 'military intelligence end users.'

Denied Persons List

The Denied Persons List contains the names and addresses of individuals and entities located in the United States and overseas subject to a denial of export privileges. Any dealings with a person or entity on this list that would violate the terms of the denial order are prohibited. See Section 764.3(a)(2) of the EAR.

Entity List

The BIS Entity List has evolved into a formidable administrative enforcement tool that imposes a license requirement for exports, reexports, or transfers of some or all items subject to the EAR to listed foreign entities. Those on the BIS Entity List were placed there because there is reasonable cause to believe they have been involved, are involved, or pose a significant risk of being or becoming involved, in activities contrary to U.S. national security or foreign policy, such as WMD programs, destabilizing accumulations of conventional weapons, terrorism, or enabling human rights abuses. These license requirements are in

addition to any license requirements imposed on the transaction by other provisions of the EAR. As a general rule, BIS generally applies a presumption of denial for license applications involving listed entities. The Entity List thereby serves as an incentive for listed foreign parties to implement effective export management compliance programs to stop the diversion of U.S.-origin items to unauthorized destinations, uses, or users, thereby providing a basis for removal. General Orders also may restrict exports to named individuals or entities. For General Orders, see Supplement No. 1 of Part 736 of the EAR.

For guidance concerning the license application review policy applicable to a particular entity, please review that individual or organization's entry on the list. Listed entities may request removal from the Entity List by submitting a petition pursuant to Section 744.16 and Supplement 5 to Part 744 of the EAR.

Unverified List

The Unverified List (UVL) contains the names and addresses of foreign persons that have been parties or intended parties to transactions subject to the EAR whose *bona fides* could not be confirmed as a result of an end-use check, including the U.S. Government's inability to conduct such an end-use check. The presence of a person listed on the Unverified List in a proposed export transaction creates three consequences: all export transactions must be reported in the Automated Export System (AES) (see Section 758.1(b)(8) of the EAR); license exception-eligibility is suspended (see Section 740.2(a)(17) of the EAR); and for all other EAR transactions not subject to a license requirement, the exporter must obtain a statement from the UVL party agreeing to abide by the EAR, including to permit an end-use check prior to export (see Section 744.15 of the EAR). Once BIS confirms the *bona fides* of the foreign party, including through completion of an end-use check, a party may be removed from the UVL. Similar to the Entity List, the UVL provides an incentive for foreign parties to comply with the EAR, including its end-use check requirements.

Military End-User List

Established on December 23, 2020,[5] the Military End-User (MEU) List identifies foreign parties that are prohibited from receiving items described in Supplement No. 2 to part 744 of the EAR, unless the exporter secures a license. These parties have been determined by the U.S. Government to be 'military end users,' as defined in Section 744.21(g) of the EAR, and represent an unacceptable risk of use in or diversion to a 'military end use' or 'military end user' in Belarus, Burma, Cambodia, China, Russia, or Venezuela. The MEU List is not exhaustive and exporters must conduct their own due diligence to identify any license requirements described in Section 744.21 of the EAR that may apply to entities not listed on the MEU List. The list supplemented existing BIS authorities that imposed licensing requirements on certain exports, reexports, or transfers (in-country) for 'military end-uses' and 'military end users,' including BIS's authority to inform the public of a license requirement for any item subject to the Regulations due to an unacceptable risk of use in or diversion to a 'military end use' or 'military end user' in Belarus, Burma, Cambodia, China, Russia, or Venezuela.

General Prohibition 10 List

Effective February 24, 2022, BIS imposed expansive and stringent controls on aviation-related items destined for Russia, including a new license requirement for specified aircraft or aircraft parts. Effective March 2, 2022, BIS imposed similar controls on Belarus. As a result, any aircraft manufactured in the United States, or that is manufactured in a foreign country and includes more than 25% U.S.-origin controlled content, is subject to a license requirement if such aircraft is destined for Russia.

Based on publicly available information, BIS has identified aircraft flying from third countries to Russia since March 2, all of which are owned or controlled by, or under charter or lease to, Russia or Russian nationals, and has listed those aircraft on its website (i.e., GP 10 list). BIS alerted the public that any subsequent actions taken with regard to any of the listed aircraft, including, but not limited to, refueling, maintenance, repair, or the provision of spare parts or services, are subject to the prohibitions outlined in General Prohibition Ten of the EAR (Section 736.2(b)(10)).

Asset Forfeiture

Asset forfeitures target the financial motivation underlying many illicit export activities. The forfeiture of assets obtained in the conduct of unlawful activity may be imposed in connection with a criminal conviction for export violations or in a civil forfeiture action. Asset forfeitures prevent export violators from benefiting from the fruits of their crimes and the value of forfeited assets can greatly exceed criminal fines or administrative penalties. As described in Section 758.7(b)(7) of the EAR, OEE is authorized to initiate administrative forfeiture (nonjudicial civil forfeiture or summary forfeiture) proceedings and forfeit property.

False Statements

A party to an export transaction may be subject to criminal and/or administrative sanctions for making false statements to the U.S. Government in connection with an activity subject to the EAR. Most frequently, the false statements are made on an export document or to a federal law enforcement officer. Common types of false statements seen by OEE are: 1) statements on Electronic Export Information or EEI (information now filed through the Automated Export System (AES), but formerly filed as a paper Shipper's Export Declarations (SED)) that an export is destined for one country when it is really destined for a sanctioned destination; 2) SED or AES filing statements that the export does not require a license (i.e., it is "NLR") when in fact a license is required for the shipment; 3) false item valuations; and 4) statements that an export was shipped under a particular license number when in fact that license was for a different item. False statements that are made to the U.S. Government, whether directly or indirectly through another person, such as a freight forwarder, may constitute violations of the EAR and may serve as the basis for the issuance of a denial order.

The Scott Communications, Inc. investigation is a good example of the potential outcome of making false statements. In March 2023, Scott Communications, Inc., Mission Communications LLC, and Kenneth Peter Scott, all of St. Ignatius, Montana, agreed to a 20-year denial order to settle charges that they attempted to export two portable Motorola radios, controlled for anti-terrorism reasons, to Jordan with knowledge that they would be reexported to Iran, and engaged in false statements in subsequent interviews with OEE.

Export Compliance

Responsible Parties

All parties that participate in transactions subject to the EAR must comply with the EAR. These persons may include exporters, freight forwarders, carriers, consignees, and other participants in an export transaction. The EAR apply not only to parties in the United States, but also to persons in foreign countries who are involved in transactions subject to the EAR.

Due Diligence: Eight Principles for an Effective Compliance Program

Many exports of controlled items, including software and technology, require a license from BIS. It is the responsibility of the exporter to obtain a license when one is required under the EAR. License requirements for a particular transaction, as described in the EAR, are based on a number of factors, including technical characteristics of the item to be exported and the item's destination, end user, and end use. When determining whether a license is required for your transaction, you should be able to answer the following questions:

- ☐ **What is being exported?**
- ☐ **Where is the item being exported?**
- ☐ **Who will receive the item?**
- ☐ **How will the item be used?**

PREVENTIVE MEASURES YOU CAN TAKE

- Check exporters and customers
- Check end users and end uses
- Review Electronic Export Information
- Educate relevant personnel

BIS weighs a variety of aggravating and mitigating factors in deciding the level of penalties to assess in administrative cases. As set forth in Supplement Nos. 1 and 2 to Part 766 of the EAR, the presence of an effective compliance program may entitle a party to significant mitigation. BIS's Export Compliance Program (ECP) guidelines can be accessed through BIS's website at *www.bis.doc.gov* under the Compliance and Training tab. Additionally, BIS has published numerous advisory notes, guidance documents, and alerts in coordination with other government agencies like the Departments of Justice, Treasury, Homeland Security, and State. Those can be found through BIS's website under "Enforcement" at *https://www.bis.gov/enforcement-policy-memos*. BIS employs the following eight guiding principles when assessing the effectiveness of a company's export compliance program:

1. Have strong and continuous management commitment. In order to build and maintain an effective program senior management must:

   - Publicly support compliance policies and procedures
   - Provide sufficient resources
   - Support export compliance training and training sessions

2. Identify and mitigate your organization's potential vulnerabilities by conducting frequent risk assessments.

3. Write and implement export authorization procedures on jurisdiction, classification, licensing and screening. This is vital for preventing your organization from exporting unauthorized items and possibly facing export penalties.

4. Assign individuals roles in recordkeeping and ensure procedures meet the requirements in § 762.4 of the EAR.

5. Require training for all employees, including support staff, whose responsibilities relate to exports in order to keep up with changing regulations and to network with other export compliance practitioners.

6. Perform regular audits to gauge how well procedures are implemented and how elements need to be augmented.

7. Implement a program to handle compliance issues, including how to prevent export violations and how to complete corrective actions when a violation is found.

8. Whether writing an ECP for the first time or maintaining an ECP, make sure to keep the manual current and relevant to the members of your organization.

Developing an effective company compliance program is essential not only for preventing export violations, but also for enabling BIS to differentiate violations by individual employees from larger patterns of corporate noncompliance. Export Enforcement may afford significant mitigation to companies or universities with effective compliance programs while at the same time may aggravate penalties when companies or universities make a deliberate decision not to disclose a significant possible violation.

If you need assistance to determine whether the item you want to export requires a license you should:

1. Check the BIS website at *https://www.bis.doc.gov*

2. Call one of our export counselors at 202-482-4811 (Washington, DC), 949-660-0144 (Western Regional Office) or 408-998-8806 (Northern California Branch) for counseling assistance.

Please note that, whether you are the exporter, freight forwarder, consignee, or other party to the transaction, you must address any red flags that arise. Taking part in an export transaction where a license is required but not obtained may subject you to criminal and/or administrative liability. The EAR discuss red flags in Supplement No. 3 to Part 732, which is available on the BIS website.

A key in determining whether an export license is required from the Department of Commerce involves knowing whether the item for export has a specific ECCN, an alpha-numeric code that describes a particular item or type of item, and shows the controls placed on that item. All ECCNs are listed on the CCL. Once an item has been classified, the next step is to determine whether an export license is required based on the "reasons for control" of the item and the country of ultimate destination. Reasons for control include national security, chemical and biological weapons controls, nuclear nonproliferation, missile technology, regional stability, anti-terrorism, and crime control. Please visit *https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl* for more information on how to classify items.

Transshipments & Reexports

Parties to an export transaction cannot bypass the EAR by shipping items through a third country. The transshipment or reexport of items in international commerce may be a violation of U.S. law. For example, an exporter cannot bypass the U.S. embargo against Iran by shipping an item to a distributor in the United Kingdom and asking the distributor to transship the item to a customer in Iran. Under U.S. law, this would be considered an export to Iran, even though it does not go directly to that country, and both the U.S. exporter and the United Kingdom distributor could be liable for violating U.S. law.

Parties to exports or reexports of items subject to the EAR should be alert to the red flag indicators of possible unlawful diversion found in Supplement No. 3 to Part 732 of the EAR, and should consult BIS's guidance on reexports at *https://www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions* as well as "Best Practices" to Guard Against Unlawful Diversion through Transshipment Trade at *https://www.bis.doc.gov/index.php/documents/pdfs/625-best-practices/file.*

In addition, exporters should be knowledgeable about the export control requirements of their customers and are strongly encouraged to obtain copies of any relevant import licenses (permits) prior to export. For example, Hong Kong requires all importers to receive a license prior to receipt of multilaterally-controlled items from abroad. The EAR requires exporters or reexporters to Hong Kong of any item subject to the EAR and controlled on the CCL for NS, MT, NP Column 1, or CB reasons to obtain a copy of the Hong Kong import license or a written statement that no such license is necessary. (See Section 740.2(a)(19), (20) of the EAR.) Similarly, exporters are required to notify their customers of export license conditions (e.g., requirement for BIS authorization for subsequent transfer (in-country) or reexport) and should make their customers aware that a license (permit) may be required for subsequent reexport from their own government in addition to BIS. BIS published guidance on its website to assist exporters in this regard: *https://www.bis.doc.gov/index.php/licensing/9-bis/carousel/689-foreign-import-export-license-requirements-hong-kong-singapore-united-arab-emirates*.

Catch-All Controls

BIS controls exports of items not only based on their technical specifications, but also based on their intended end use and end user. The EAR impose license requirements on exports of items subject to the EAR if the exporter knows or has reason to know that any of the items will be used in an end use of particular concern to the U.S. Government, such as a missile or nuclear weapons program, for a military-intelligence end use or end user, or in certain circumstances a military end use or by a military end user. These controls are often referred to as "catch-all" controls because they apply to a broad set of items, or in the case of WMD and military-intelligence activities, to any support to such activities, even if not involving an item not subject to the EAR.

Export restrictions based on the end use and end user are specified in Part 744 of the EAR and include restrictions on certain nuclear, missile, chemical and biological, and military/military-intelligence end uses, as well as restrictions on certain end users. BIS maintains restrictions on end users listed on the Denied Persons List, the

Entity List, the UVL, and the MEU List, as well as the illustrative list of military-intelligence end users in Section 744.22. BIS uses these lists to notify the public of end users of concern, including entities engaged in illicit export activity or other activities contrary to U.S. national security or foreign policy, entities that could not be confirmed as reliable recipients of U.S.-origin commodities, software, or technology, and certain entities subject to military end-user controls.

The EAR also incorporate by reference certain entities sanctioned by the Department of the Treasury, including certain Specially Designated Terrorists, Specially Designated Global Terrorists, Foreign Terrorist Organizations, and Weapons of Mass Destruction Proliferators and their Supporters.

These lists are not comprehensive and do not relieve parties to an export transaction of their responsibility to determine the nature and activities of potential customers who may not be listed (see BIS's "Know Your Customer" Guidance in Supplement No. 3 to Part 732 of the EAR, available on the BIS website).

Sanctions Programs

The United States maintains broad export controls on certain countries for foreign policy reasons. It has imposed such controls unilaterally or multilaterally pursuant to United Nations Security Council Resolutions. Countries may be subject to partial or comprehensive embargoes, in some cases as a consequence of their designation by the Secretary of State as state sponsors of terrorism. As of the date of publication of this document, Syria, Iran, Cuba, and North Korea remain designated as state sponsors of terrorism. BIS implements stringent export controls on these four countries under the EAR.[5]

As a practical matter, many exports of ordinary commercial items not typically controlled to other destinations may require authorization from BIS and other federal agencies, including the Department of the Treasury's Office of Foreign Assets Control (OFAC). For these four countries, BIS or OFAC – and in some cases both agencies together – administer the licensing requirements and enforce the controls.

What is OFAC and what does it do?

OFAC administers and enforces economic sanctions programs against countries, entities, and individuals, including terrorists and narcotics traffickers. The sanctions may be either partial or comprehensive, requiring the blocking of assets of designated persons in some situations or the imposition of broad trade restrictions on regions and sectors to accomplish foreign policy and national security goals.

BIS and OFAC work together to administer and enforce the sanctions against Iran and both maintain license requirements for Iran. To reduce duplication with respect to these licensing requirements, exporters or reexporters are not required to seek separate authorization from BIS for an export or reexport subject both to

[5] *https://www.bis.doc.gov/index.php/documents/regulation-docs/420-part-746-embargoes-and-other-special-controls/file*

the EAR and to the Iranian Transactions and Sanctions Regulations (ITSR). If OFAC authorizes an export or reexport, such authorization is considered authorization for purposes of the EAR as well. It is important to note that transactions that are not subject to OFAC regulatory authority may require BIS authorization. No person may export or reexport any item that is subject to the EAR if such transaction is prohibited by the ITSR and not authorized by OFAC. This prohibition applies whether or not the EAR independently require a license for export or reexport. Please see section 746.7 of the EAR or visit *https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations/iran* for more information.

It is important to familiarize yourself with the restrictions that apply to the ultimate destination of your export. U.S. law in this area frequently changes in accordance with an evolving foreign policy. The following websites are good resources:

OFAC's website:
https://www.treasury.gov/ofac

BIS's website:
https://www.bis.doc.gov

Consolidated Screening List website:
https://www.trade.gov/data-visualization/csl-search

Successor Liability

Businesses can be held liable for violations of the EAR committed by companies that they acquire. Businesses should be aware that the principles of successor liability may apply to them and should perform "due diligence" in scrutinizing the export control practices of any companies that they plan to acquire. A properly structured due diligence review can determine whether an acquired company has violated any export laws. This review should examine the company's export history and compliance practices, including commodity classifications, technology exchanges, export licenses and authorizations, end users, end uses, international contracts, the status of certain foreign employees who have access to controlled technologies, and the company's export policies, procedures, and compliance manuals. Voluntary self-disclosures should be submitted outlining any violations that this review uncovers, if not by the company responsible, then by the company seeking to acquire it. Failure to scrutinize properly an acquired company's export practices can lead to liability being imposed on the acquiring company.

Educational Outreach

To raise awareness of export control requirements and prevent potential violations of the EAR, Export Enforcement conducts educational outreach to U.S. exporters and foreign trade groups. In addition to participating in BIS export control seminars and conferences, Export Enforcement conducts outreach to individual exporters to inform them of their responsibilities under the EAR, review compliance best practices, and alert them if appropriate to offshore illicit procurement activities of which they may be a target. Export Enforcement also engages American business communities overseas and foreign trade and industry associations to promote awareness of U.S. export and reexport controls, including in cooperation with foreign government partners. In 2022, the Assistant Secretary for Export Enforcement Matthew Axelrod announced BIS's 'Academic Outreach Initiative', aimed at assisting 20 prioritized universities with elevated risk profiles in developing and implementing an Export Compliance Program (EMCP) to ensure compliance with the EAR. This initiative was expanded to 29 universities in 2023.

During FY2023, OEE conducted more than 1,700 outreaches. Industry's knowledge and compliance with the EAR establishes a built-in warning system for Export Enforcement to be aware of suspicious actors. Coupled with this general outreach, Export Enforcement has expanded its Guardian outreach program to industry,

alerting companies of suspicious parties that may be seeking to obtain sensitive items. In FY2023, BIS initiated over 35 Project Guardian leads (i.e., alerts to Special Agents about a suspicious transaction). OEE fully appreciates the reputational risk associated with your items being involved in illicit activities, and this advance warning system is meant to help you identify otherwise unforeseen risks in potential transactions.

Cyber-Intrusions and Data Exfiltration

One of the newer areas of focus in our outreach efforts relates to cyber-intrusions and data exfiltration that result in controlled technology being exported. It is becoming almost a daily occurrence to read about a cyber-intrusion or attack. The perpetrators of cyber-crime are varied; they include independent hackers and criminal organizations, as well as state actors. The theft of export-controlled information from your computer systems as a result of foreign cyber actors is a threat to U.S. national security interests and your company's competitive lifeblood: intellectual property.

The U.S. Government is attempting to address this theft through a whole-of-government approach. On February 12, 2014, the National Institute of Standards and Technology, a sister agency at the Department of Commerce, published the first National Cybersecurity Framework, which can be found at *https://www.nist.gov/cyberframework*. An updated version was released in April 2018. Regardless of the type of business sector or an organization's size, an entity can use the framework to determine its current level of cybersecurity, set goals for cybersecurity that are in sync with its business environment, and establish a plan for improving or maintaining its cybersecurity. This Framework also offers a methodology to protect privacy and civil liberties to help organizations incorporate those protections into a comprehensive cybersecurity program. The Framework is part of a larger initiative to combat the ever-evolving cyber threat. Both the FBI and the Department of Homeland Security's Office of Infrastructure Protection are developing programs and initiatives to help the private sector protect, identify, mitigate, and report malicious cyber activity and actors. For our part, BIS has leveraged the Entity List to impose export restrictions on certain foreign entities involved in thefts of intellectual property.

Companies need to evaluate whether to incorporate cybersecurity into your ECP as well as report cyber incidents. Reporting the exfiltration of controlled technology is separate and distinct from submitting a VSD. The latter involves your discovery of a violation of the EAR. By reporting cyber thefts, you are giving us critical information that can allow BIS, working with our interagency partners, to identify these cyber-actors and bring our unique BIS tools to bear against them. Cybersecurity, like effective export controls, can only be achieved with your support and partnership.

Enforcement Priorities

For over 40 years, the Department's Office of Export Enforcement (OEE) has been on the front line of protecting U.S. national security, ensuring that EAR items are not falling into the hands of our adversaries. OEE's efforts, and their results, have been consistent for those 40-plus years, but the nature of the threat and the items, end users, and end uses of concern have evolved during that time span.

Forty years ago, our export control system was narrower, focused singularly on traditional dual-use items related to conventional military applications, and were aimed at a single adversary. The coordinating Committee for Multilateral Export Controls, or CoCom, was established by the U.S. and our allies after World War II as an informal mechanism to coordinate an embargo policy on the export of sensitive technology and goods to the communist bloc. In 1982, when OEE began, its job was to enforce U.S. export controls in a CoCom world.

From these narrow post-World War II beginnings, the global export control system evolved in the mid-1990s with the simultaneous fall of the Soviet Union and rise of the proliferation of weapons of mass destruction. New multiple export control regimes were developed that focused on a broader array of items, not only dual-

use items, tied to conventional weapons, but also items related to missiles, chemical and biological weapons, and nuclear weapons.

Fast-forward to the aftermath of September 11, 2001, and the focus of our country's national security efforts pivoted to face a new and pressing threat of the terrorist attacks on our homeland by non-state actors like al-Qaeda. The changing nature of the threat meant OEE, in addition to investigating proliferation of WMD and destabilizing military activities, also worked more closely with the Department of Defense to prevent U.S. components from getting into the hands of terrorists for use in improvised explosive devices. In parallel, we expanded the use of our Entity List to allow for the designation of parties when supporting any activity contrary to U.S. national security or foreign policy interests.

OEE Special Agents conducting an inspection

Today, more than twenty years since 9/11, the national security landscape has changed again. While non-state actor threats remain, nation-state actors are once again the paramount threat. Each year, the Office of the Director of National Intelligence (DNI) publishes the Intelligence Communality's Annual Threat Assessment, which details the DNI's view of the gravest national security threats faced by the United States. The first four sections of its 2024 assessment each focus on a different nation-state actor – China, Russia, Iran, and North Korea. As the assessment notes, "An ambitious but anxious China, a confrontational Russia, some regional powers, such as Iran, and more capable non-state actors are challenging longstanding rules of the international system as well as U.S. primacy within it." The assessment also points out that "North Korean leader Kim Jong Un will continue to pursue nuclear and conventional military capabilities that threaten the United States and its allies…"

Accordingly, Export Enforcement's highest priority is to prevent nation-state actors that pose the gravest threat to U.S. national security from illicitly acquiring EAR items. "Don't Let This Happen to You" chapters have been organized to reflect this reprioritization of threats by nation-state actors, with the reason or basis for control for items found to be exported in violation of the EAR – i.e., *National Security*, *Military* (including catch-all), *WMD* (including catch-all), and *Other* such as firearms and sanctioned items like oilfield equipment – identified by subsection within each chapter.

End-Use and End-User Controls

In addition to the controls set forth on the CCL based on the technical parameters (ECCN) of the items and the destination country, the EAR control the export of items, which may include items listed in an ECCN on the CCL, as well as items designated EAR99, when destined to certain end uses or end users. These end-use and end-user controls, found in Part 744 of the EAR, and certain special controls found in part 746 of the EAR, are intended to prevent items subject to the EAR from contributing to activities contrary to U.S. national security and foreign policy interests, including certain:

- Nuclear explosive activities and safeguarded and unsafeguarded nuclear activities, as described in Section 744.2 of the EAR.
- Rocket systems and unmanned aerial vehicles, as described in Section 744.3 of the EAR.
- Chemical and biological weapons, as described in Section 744.4 of the EAR.
- Maritime nuclear propulsion end uses, as described in Section 744.5 of the EAR.
- Military end uses and end users, as described in Sections 744.17 and 744.21 of the EAR.
- Military-intelligence end uses and end users, as described in Section 744.22 of the EAR.
- Russian deepwater, Arctic offshore, or shale oil or gas exploration or production activities, as described in Section 746.5 of the EAR.
- Russian and Belarusian industry sector sanctions, as described in Section 746.5 of the EAR.
- "Supercomputer," "advanced-node integrated circuits," and semiconductor manufacturing equipment as described in Section 744.23 of the EAR.

Foreign parties have also been listed on the Entity List based on their involvement in certain of the foregoing activities. Restrictions on parties listed on the Entity List (Sections 744.11 and 744.16 of the EAR and Supplement No. 4 to part 744), the Denied Persons List, the UVL (Section 744.15 of the EAR and Supplement No. 6 to part 744), and the MEU List (Section 744.21 of the EAR and Supplement No. 7 to part 744) are described above. In addition to screening your customers against the Consolidated Screening List, you should also exercise due diligence, in accordance with the "Know Your Customer" Guidance in Supplement No. 3 to part 732 of the EAR, to determine whether any "red flags" indicate your customer may be planning an unlawful diversion to one of the foregoing end uses or end users.

The U.S. Government maintains controls on exports of certain items based on its participation in multilateral export control regimes as well as for unilateral foreign policy reasons. These items are identified on the Commerce Control List and controlled pursuant to Part 742 of the EAR.

EAR controls based on multilateral export control regimes include:

- NP (nuclear nonproliferation) controls implemented pursuant to the Nuclear Suppliers Group. The EAR control items that could be of significance for nuclear explosive purposes.
- CB (chemical-biological weapons) controls implemented pursuant to the Australia Group. The EAR control items, including entire chemical plants, toxic chemicals and precursors, and certain microorganisms, that could be used for chemical or biological weapons programs;
- MT (missile technology) controls implemented pursuant to the Missile Technology Control Regime. The EAR control unmanned delivery systems, including unmanned aerial vehicles, capable of delivering weapons of mass destruction;
- NS (national security) controls implemented pursuant to the Wassenaar Arrangement; and
- FC (Firearms Convention) controls implemented pursuant to the Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other Related Materials (CIFTA). The EAR control certain firearms and ammunition, shotguns, shells, optical sights, and other related CIFTA items that could contribute to such activities as drug trafficking, terrorism, and transnational organized crime within the Organization of American States.

BIS also imposes unilateral controls on items in the following categories: significant items (SI), encryption

(EI), anti-terrorism (AT), communication intercept/surreptitious listening (SL), regional stability (RS) and crime control and other items for human rights (CC) reasons.

Freight Forwarder Responsibilities

Primary responsibility for compliance with the EAR generally falls on the "principal parties in interest" in a transaction, who are usually the U.S. seller and the foreign buyer. However, freight forwarders or other agents acting on behalf of the principal parties are also responsible for their actions, including the representations they make filing EEI or other export control documents.

To help avoid liability in an export transaction, agents and exporters must decide whether any aspect of the transaction raises red flags, inquire about those red flags, and ensure that suspicious circumstances are not ignored. Both the agent and the principal party are responsible for the accuracy of each entry made on an export document. Good faith reliance on information provided by the exporter may excuse an agent's actions in some cases, but the careless use of pre-printed "No License Required" forms or unsupported entries can get an agent into trouble. Guidance describing the newest freight forwarder roles and responsibilities can be found on the BIS website: *https://www.bis.doc.gov/index.php/all-articles/24-compliance-a-training/export-management-a-compliance/48-freight-forwarder-guidance*.

Assistant Secretary for Export Enforcement Matthew S. Axelrod (far right) and Assistant Attorney General for National Security Matthew G. Olsen Assistant (second from right) tour the Kyiv Scientific Research Institute of Forensic Expertise, which houses drones, electronic components, and other devices used by Russia and found on the battlefields in Ukraine

Chapter 1 – China

Criminal and Administrative Case Examples

National Security Controls

Seagate Technology LLC / Seagate Singapore International Headquarters PTE. LTD.

The Violation: Between 2020 and 2021, Seagate Technology LLC of Fremont, California (Seagate US) and Seagate Singapore International Headquarters PTE. LTD (Seagate Singapore) ordered or caused the reexport, from abroad, or transfer (in-country) of more than 7.4 million hard disk drives (HDDs) valued at over $1.1 billion to Huawei Technologies Co., Ltd. (Huawei) or other Huawei entities listed on the BIS Entity List without a license or other authorization from BIS. Huawei, whose headquarters is located in Shenzhen China, was added to the BIS Entity List in 2019, based on a determination made by multiple U.S. government agencies "that there is a reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States." In August 2020, BIS issued a Foreign Direct Product Rule (the Huawei FDPR), imposing controls over the export, reexport, or transfer (in-country) of certain foreign-produced items to Huawei. Despite this, Seagate continued to do business with Huawei. Seagate did so despite the fact that its only two competitors had stopped selling HDDs to Huawei, resulting in Seagate becoming Huawei's sole source provider of HDDs. Subsequently, Seagate entered into a three-year Strategic Cooperation Agreement with Huawei, naming Seagate as "Huawei's strategic supplier" and granting the company "priority basis over other Huawei suppliers." The HDDs are designated EAR99, but were manufactured using ECCN 3B992 tools that were the "direct product" of U.S.-origin ECCN 3E991 technology, thus subjecting them to the Huawei FDPR, meaning a license was required for the export, reexport, or transfer (in-country) of the HDDs to Huawei. Seagate did not obtain a license for its HDD sales.

The Penalty: On April 19, 2023, BIS imposed a $300 million civil penalty as part of a settlement agreement with Seagate Technology LLC and Seagate Singapore to resolve the alleged violations. This represents the largest standalone administrative penalty in BIS history. The settlement also includes a multi-year audit requirement and a five-year suspended Denial Order.

Yi-Chi Shih / Kiet Ma

The Violation: Yi-Chi Shih schemed to illegally obtain integrated circuits with military applications that were exported to China without the required filing of Electronic Export information (EEI). Shih is a former Honeywell employee, and the former owner of U.S.-based company MMCOMM, that provided millimeter wave technology and services. Shih established a non-functioning U.S. "entertainment" business named Pullman Lane Productions that received $1 million dollars from Qing'an International Trading Group in China. The money was used to pay Shih and his brother to assist in developing a foundry in China, Chengdu Gastone Technology Company (CGTC), where Shih was the president. In 2014, CGTC was placed on the BIS Entity List. Shih and his associate Kiet Mai conspired to illegally provide Shih with unauthorized access to a protected computer of a U.S. manufacturer of wide-band, high-power semiconductor chips known as monolithic microwave integrated circuits (MMICs). MMICs, classified under ECCN 3A001, are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures and radar applications. As part of the scheme, Shih accessed the company's computer systems via its web portal after Mai obtained access. Mai posed as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih used Ma to conceal his true intent to export the company's MMICs to China. This case resulted from a joint investigation conducted by OEE's Los Angeles Office, the FBI, and IRS-CID.

The Penalty: On November 16, 2023, Yi-Chi Shih was re-sentenced in the U.S. District Court for the Central District of California to 85 months in prison, 12 months of home confinement, three years of supervised release, a $300,000 criminal fine, $362,698 in restitution, and a $1,800 special assessment. On September 19, 2019, Kiet Mai was sentenced to 18 months of probation and a $5,000 fine.

3D Systems Corporation

The Violation: 3D Systems Corporation of Rock Hill, South Carolina committed 19 violations of the EAR when it exported technology classified under ECCNs 9E515 and 3E611 to China and Germany, without the required

authorizations; exported and transferred metal alloy powder classified under ECCN 1C002 and controlled for national security and nuclear nonproliferation reason to China; and failed to comply with recordkeeping requirements. Additionally the investigation identified ITAR-controlled technology that was accessed by foreign individuals, as well as exported to Germany and China without the proper export licenses. This case resulted from an investigation conducted by OEE's Dallas Field Office.

The Penalty: On February 27, 2023, 3D Systems Corporation agreed to a $2,777,570 civil penalty, to complete two audits of its export controls compliance program with the hiring of an unaffiliated third-party consultant, and to be subject to a three-year denial of its export privileges, to be waived provided no further violations are committed during the probationary period. Additionally, the company agreed to pay in fines and remedial compliance measures $20 million as part of a consent agreement with the U.S. Department of State's Directorate of Defense Trade Controls. Finally, the company agreed to pay $4.4 million to settle the FCA allegations brought by the U.S. Department of Justice for improperly transmitting export-controlled technical data to China in violation of export control laws in connection with certain NASA and DOD contracts.

Alex Yun Cheong

The Violation: Between 2014 and 2018, Alex Yun Cheong Yue of South El Monte, California utilized a fictitious company called Ecycle Tech International LTD to acquire and attempt to acquire cesium atomic clocks classified under ECCN 3A002 and controlled for National Security reasons from a Massachusetts-based manufacturer. OEE Special Agents were alerted to this behavior by the manufacturer following an earlier outreach visit. Compliance officers at the company noted that Yue told the manufacturer that these items were to be used by another company in City of Industry, California for calibration of mobile phone equipment. This company was an unwitting participant in the scheme, receiving the deliveries for Yue. In fact, Yue was acquiring these on behalf of Premium Tech Systems of Hong Kong, and its principal, Victor Zee. Yue falsified air waybills by mislabeling and undervaluing the atomic clocks and shipped them to Hong Kong without obtaining the proper BIS export license authorization. Their ultimate end use remains unknown. After his arrest at his California home in June 2019, Yue pled guilty to three counts of violating the IEEPA, and one count of smuggling. Zee remains at large. This case resulted from a joint investigation conducted by OEE's Boston Field Office and HSI.

The Penalty: On March 3, 2021, Yue was sentenced to time served plus one year of home confinement, two years of probation, and a $5,960 criminal fine. BIS issued Yue a post-conviction denial order for a period of 10 years.

Avnet Asia Pte. Ltd / Cheng Bo

The Violation: Avnet Asia Pte. Ltd is a Singapore company and global distributor of electronic components and related software. Former Avnet Asia Sales Account Manager Cheng Bo, aka Joe Cheng, participated in a criminal conspiracy from 2012-2015 to violate U.S. export laws by shipping power amplifiers classified under ECCN 3A001 and controlled for National Security and Anti-Terrorism reasons to China. Cheng, having established Globe Communication Limited as a false front company and end user in Hong Kong, submitted paperwork on behalf of the customer to purchase export-controlled items, including the power amplifiers. Cheng caused false statements to be made to the U.S. manufacturer of the power amplifiers stating that his customer would use them in Hong Kong when, in fact, Cheng knew the goods would be illegally shipped to China to a party linked to the Chinese military. Another former Avnet Asia employee caused U.S. goods to be shipped to China and Iran without a license in violation of the IEEPA, to include ECCN 3A001 electronic components. Avnet Asia cooperated with the U.S. government in this investigation and terminated Cheng and the other former employee because of their participation in the illegal schemes. An indictment charging Cheng with conspiracy to violate the IEEPA and money laundering was unsealed in January 2021. Cheng remains at-large. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, HSI, and the Federal Bureau of Investigation (FBI).

The Penalty: Avnet Asia Pte. Ltd agreed in January 2021 to a global settlement with BIS and the U.S. Department of Justice (DOJ). Avnet Asia agreed to a Non-Prosecution Agreement with DOJ that included a $1.5 million fine to settle criminal liability for both the Cheng transshipments described above and the illegal export of electronic components to Iran and China through Singapore by other employees. Avnet Asia also agreed to a BIS administrative settlement of $3.2 million (with $1.5 million suspended) for the aforementioned and additional violations, including unauthorized shipments to a company appearing on the BIS Entity List.

CBM International / Uka Uche / Qui Bo / Samuel Ogoe / Shan Shi

The Violation: On July 29, 2019, Shan Shi was found guilty of conspiracy to steal trade secrets at the end of a three-week jury trial. On October 17, 2018, Samuel Ogoe pled guilty related to charges of conspiracy to commit theft of trade secrets. On April 26, 2018, Shi, Gang Liu, and Chinese companies CBM International Inc. (CBMI) and CBM Future New Material Science and Technology Co. Ltd (CBMF) were charged, in a superseding indictment, with economic espionage, and Shi was also charged with money laundering. On April 16, 2018, Uka Uche and Qui Bo pled guilty to charges of conspiracy to commit theft of trade secrets. On May 23, 2017, Shi, Uche, Ogoe, Johnny Wayne Randall, Bo, and Liu were arrested and charged with conspiracy to commit theft of trade secrets. Additionally, charges were filed against one Chinese national living in China, Hui Huang. The trade secrets were stolen in order to benefit CBM Future New Material Science and Technology Co. Ltd. (CBMF) in China. Shi was contracted in March 2014 by CBMF to bring in experts, set up a design team, and market marine buoyancy technology. CBMF intended to sell syntactic foam, a strong, light material that can be tailored for commercial and military uses, such as oil exploration; aerospace; underwater vehicles, such as submarines; and stealth technology to both military and civilian, state-owned enterprises in China. Shi incorporated CBMI, International Inc. (CBMI), which was owned by CBMF, in Houston, Texas as part of a systematic campaign to steal the trade secrets of a global engineering firm (the Firm) that was a leader in marine technology. Shi and CBMI employee Qui Bo systematically targeted U.S. employees with experience in the production of syntactic foam. Between late 2014 and early 2015, CBMI hired Samuel Ogoe and Gang Liu who were former employees of the Firm. Johnny Wayne Randall and Uka Uche, who were at the time employees of the Firm, provided trade secrets to Ogoe. Ogoe and Liu provided these trade secrets to CBMI shortly after being hired. Some of these trade secrets were sent by Shi and Bo to defendant Hui Huang, a Chinese national living in China and an employee of the CBMF. The technology for the syntactic foam was classified under ECCN 8E001 and was controlled for reasons of national security. This case resulted from a joint investigation conducted by OEE's Houston Resident Office, the FBI, and the Internal Revenue Service-Criminal Investigation (IRS CI).

The Penalty: On February 10, 2020, Shi was sentenced in the U.S. District Court for the District of Columbia to 16 months in prison and a forfeiture of over $330,000.

Shaohua "Eric" Wang and Ye Sang "Ivy" Wang

The Violation: On September 26, 2019 and July 20, 2021, U.S. naturalized citizens Shaohua "Eric" Wang and Ye Sang "Ivy" Wang, respectively, pled guilty to charges related to the unlawful export of sensitive military items to China. From approximately January 2018 to May 2019, Ivy Wang, a Logistics Specialist with the U.S. Navy and her husband, Eric Wang, purchased military helmet components classified under ECCNs 1A613 and 3A611, a military face respirator classified under ECCN 1A004, and various other military items (including body armor and U.S. military uniforms) from U.S. companies and sold them without the required authorizations in online marketplaces, including EBay, to consignees in China without the appropriate authorization from the Directorate of Defense Trade Controls or BIS. Ivy intentionally utilized her government employment to purchase the export-controlled items, falsely advising vendors she was procuring them in her official capacity on behalf of the United States Navy, knowing they would be exported unlawfully to China. This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office, HSI, and Naval Criminal Investigative Service (NCIS).

The Penalty: On February 3, 2020, Eric Wang was sentenced in U.S. District Court for the Southern District of California to 36 months in prison, three years of probation, and a $25,000 criminal fine. On December 21, 2021, Ivy Wang was sentenced in U.S. District Court for the Southern District of California to 30 months in prison and a $20,000 criminal fine. BIS issued Eric Wang and Ivy Wang post-conviction denial orders for a period of 10 years.

Glen Viau / Oceanworks International Corporation

The Violation: Glen Viau, Canadian citizen and President of Oceanworks International Corporation of Houston, Texas, exported submarine rescue system technology classified under ECCN 8E620 and controlled for reasons of National Security and Regional Stability to China without the required export license. Additionally, Oceanworks International Corporation submitted a voluntary self-disclosure letter which contained multiple false statements concerning the number and nature of export violations committed by the company. Viau was arrested in January 2019 at the George Bush Intercontinental Airport in Houston, Texas. Viau pled guilty to these charges in December 2019. This case resulted from a joint investigation conducted by OEE's Houston Resident Office and the FBI.

The Penalty: On December 2, 2019, Viau was sentenced in the U.S. District Court for the District of Columbia to a $25,000 criminal fine.

Odusseus Technologies

The Violation: On two occasions, Odusseus Technologies, aka "United Force Corporation" of Northville, Michigan, exported computer simulation software classified under ECCN 1D002 to China. As part of the export of the computer simulation software, the company filed Electronic Export Information (EEI) knowingly and falsely describing the software as "unrecorded magnetic media, tapes." The company pled guilty to these charges in the U.S. District Court for the Eastern District of Michigan. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, the FBI, and HSI.

The Penalty: On May 22, 2019, Odusseus Technologies was sentenced to a $147,819 criminal fine.

Zhongxing Telecommunications Equipment Corporation (ZTE) and ZTE Kangxun Telecommunications Equipment

The Violation: On March 22, 2017, Chinese companies Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd., known collectively as ZTE, pled guilty in the U.S. District Court in the Northern District of Texas in connection with the illegal shipment of telecommunications equipment to Iran and North Korea in violation of the EAR and the ITSR. ZTE conspired to evade the U.S. embargo against Iran in order to obtain contracts with and related sales from Iranian entities, including entities affiliated with the Iranian Government, to supply, build, operate, and/or service large-scale telecommunications networks in Iran, the backbone of which would be U.S.-origin equipment and software. As a result of the conspiracy, ZTE was able to obtain hundreds of millions of dollars in contracts with and sales from such Iranian entities. ZTE also undertook other actions involving 283 shipments of controlled items to North Korea with knowledge that such shipments violated the EAR. Shipped items included routers, microprocessors, and servers controlled under the EAR for national security, encryption, regional security, and/or anti-terrorism reasons. In addition, ZTE engaged in evasive conduct designed to prevent the U.S. Government from detecting its violations. OEE learned that in November 2013, following a meeting of senior managers chaired by its then-CEO, ZTE made plans to resume transshipments to Iran that would continue during the course of the investigation. On March 7, 2016, BIS sanctioned ZTE by adding it to the BIS Entity List, which created a license requirement to export, reexport, or transfer (in-country) to ZTE any items subject to the EAR. During the course of the investigation, ZTE made knowingly false and misleading representations and statements to OEE or other U.S. law enforcement agencies, including that the company had previously stopped shipments to Iran as of March 2012, and was no longer violating U.S. export control laws. ZTE also engaged in an elaborate scheme to prevent disclosure to and affirmatively mislead the U.S. Government, by deleting and concealing documents and information from the outside counsel and forensic accounting firm that ZTE had retained with regard to the investigation. Following the 2017 settlement, ZTE admitted that it had falsely informed the U.S. Government that the company would or had discipline numerous employees responsible for the violations that led to the March 2017 settlement agreement. ZTE instead rewarded that illegal activity with bonuses. This case resulted from a joint investigation conducted by OEE's Dallas Field Office, HSI, and the FBI.

The Penalty: On March 22, 2017, ZTE agreed to a combined civil and criminal penalty of $1.19 billion, the largest fine and forfeiture ever levied by the U.S. Government in an export control case. ZTE agreed to pay a penalty of $661 million to BIS, with $300 million suspended during a seven-year probationary period. ZTE also agreed to pay OFAC $100,871,266 pursuant to a settlement agreement. In addition, ZTE agreed to active audit and compliance requirements designed to prevent and detect future violations and a seven-year suspended denial of export privileges. On April 15, 2018, BIS activated the suspended denial order against ZTE in response to the company's admission that it had made false statements to the U.S. Government. On June 8, 2018, BIS and ZTE agreed to a superseding settlement agreement including a civil penalty of $1.4 billion, of which ZTE paid $1 billion out-of-pocket and deposited $400 million into an escrow account in a U.S. bank, where it would remain for ten years unless the company violated U.S. export controls. ZTE also agreed to a 10-year suspended denial order and the retention of a Special Compliance Coordinator, selected by BIS and paid by ZTE.

Daofu Zhang / Jian Guangzhou Yan / Xianfeng Zuo

The Violation: Daofu Zhang, Jian Guanghou Yan and Xianfeng Zuo, all Chinese nationals, each operated businesses in China that bought and sold electronic components, including integrated circuits. In 2015, Zuo requested that Yan locate and purchase several advanced integrated circuits classified under ECCN 9A515 which had military applications, including radiation tolerance for uses in space. Yan then asked a U.S. individual to locate the items and sell them to Yan. The U.S. individual explained that the items cannot be shipped outside the United States without an export license, but Yan still wished to make the purchase. When the U.S. individual expressed concern that the desired integrated circuits would have to be stolen from military inventory, Yan proposed to supply the U.S. individual with fake integrated circuits to replace the ones to be stolen from the military. In November 2015, Zhang shipped from China to the U.S. individual, two packages containing counterfeit integrated circuits, each bearing a counterfeit brand label. After further discussions between Yan and the U.S. individual, Yan, Zhang, and Zuo flew together from China to the U.S. in early December 2015 to complete the purchase of the integrated circuits. On December 10, 2015, Yan, Zhang, and Zuo drove to a location in Connecticut, where they planned to meet the U.S. individual, make payment, and take custody of the items. Yan, Zhang, and Zuo were arrested at the meeting location. On April 15, 2016, Zhang pled guilty to charges related to the sale of counterfeit parts intended for the U.S. military in connection with the attempted export of computer chips to China without the required export license. On March 7 and March 16, 2016, respectively, Yan and Zuo pled guilty in connection with the conspiracy. This case resulted from a joint investigation conducted by OEE's Boston Field Office, HSI, DCIS, the FBI, and the U.S. Air Force Office of Special Investigations (AFOSI).

The Penalty: On July 8, 2016, Zhang was sentenced to 15 months in prison. On November 4, 2016, Zuo was sentenced to 15 months in prison. On December 20, 2016, Yan was sentenced to 12 months in prison. In addition, all three defendants' sentences included a $63,000 forfeiture.

Fulfill Your Packages

The Violation: Fulfill Your Packages (FYP) of Gresham, Oregon, allowed its foreign customers in China to use its U.S. domestic address for the purchase and delivery of items from U.S. companies that FYP later repackaged and/or relabeled for export to China. In about June 2014, FYP engaged in a transaction or took other actions with intent to evade the EAR in connection with the intended export of a FLIR thermal imaging camera classified as ECCN 6A003 and controlled for national security and regional stability reasons. Specifically, a FYP customer purchased the camera from a U.S. distributor located in Florida for delivery to FYP's offices in Oregon and for ultimate export to China. The FYP customer provided FYP's address as his own and did not disclose to the U.S. distributor that the thermal imaging camera was to be exported to China. The shipment from the distributor to FYP included an invoice that warned that the product was export-controlled and that was a violation of U.S. law to export the product to certain countries without the required export license. In addition, a label affixed to the item noted that the item was subject to U.S. Department of Commerce export control regulations and must not be exported outside the United States or Canada without a U.S. export license. In preparing to export the thermal imaging camera to China, FYP prepared a U.S. Postal Service shipping label falsely describing the item as "metal parts" valued at $255, even though FYP's order system described the items as an infrared webcam/surveillance camera installation kit, and even though the distributor's invoice described the items as a thermal imaging camera valued at $2,617. This case resulted from a joint investigation conducted by OEE's San Jose Field Office and Portland Resident Office, the FBI and HSI.

The Penalty: On June 17, 2016, FYP agreed to pay a $250,000 civil penalty with $190,000 suspended provided no violations occur during a two-year probationary period.

Military Controls

Tao "Jason" Jiang / Broad Tech System, Inc. / Bohr-Winn Shih

The Violation: This investigation involved the unauthorized export of photoresist chemicals classified under ECCN

3A992 to NTESY, a company in China acting as an alias of NEDI, aka Nanjing Electronic Devices Institute aka China Electronics Technology Group Corporation 55th Research Institute (CETC 55, each of which appear on the BIS Entity List). Tao "Jason" Jiang and Broad Tech System, Inc., (Broad Tech) a California-based electronics distribution company, admitted that they conspired together and with Bohr Winn-Shih, an engineer employed at Broad Tech, to order the photoresist and developer chemicals from a U.S.-based manufacturer, then knowingly submitted false and misleading documentation to the U.S. Government and to shipping companies in an effort to have these products illegally shipped to NTESY. NTESY mainly engages in the manufacturing of electronic components and the research, development and production of core chips and key components in China's military strategic early warning systems, air defense systems, airborne fire control systems, manned space systems, and other national large-scale projects. Photoresist and HPRD are essential to the chip manufacturing process. This case resulted from an investigation conducted by OEE's Boston Field Office and CBP.

The Penalty: On April 27, 2023, Tao "Jason" Jiang was sentenced in the U.S. District Court for the District of Rhode Island to 12 months of probation, a $5,500 criminal fine, 100 hours of community service, and a $300 special assessment. Broad Tech was sentenced to 12 months of probation, a $120,000 criminal fine, and a $1,200 special assessment. On August 3, 2021, Bohr-Winn Shih was sentenced to 12 months of probation, 50 hours of community service and a $300 special assessment.

Zheng Yan / Yang Yang / Ge Song Tao / Shanghai Breeze Technology Co. Ltd.

The Violation: Yang Yang, a dual Chinese-U.S. Citizen and owner of BQ Tree Consulting in Jacksonville, Florida; Ge Song Tao, a Chinese Citizen and President of the Chinese Company Shanghai Breeze; and Zheng Yan, a Chinese Citizen and Manager of the Chinese Company Shanghai Breeze were indicted in the Middle District of Florida for export violations. These individuals and others conspired to illegally export military-grade combat rubber raiding craft (CCRC) classified under ECCN 8A992, used by the U.S. Special Operations community, to China. These CRRCs and accompanying multi-fuel engines are used in austere missions due to their ability to be deployed from submarines and dropped from aircraft. The scheme involved providing a U.S. company with false end-use and end-user information for a front company in Hong Kong, which was used to complete the transaction valued over $266,000 and ultimately destined for China. The intention was to reverse engineer the CRRC and engines to mass produce them for the Chinese People's Liberation Army (PLA) Navy. Items controlled under ECCN 8A992 are currently subject to an EAR license requirement for export to military end users in China, such as the PLA Navy. This is a joint investigation with OEE's Atlanta Resident Office, the FBI, NCIS, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

The Penalty: On March 31, 2021, Zheng Yan was sentenced in the U.S. District Court for the Middle District of Florida to 17 months in prison, one year of supervised release pending deportation, a prohibition on employment with any company that deals with the military, and a $100 special assessment. On December 9, 2020, Yang Yang was sentenced in the U.S. District Court for the Middle District of Florida to 16 months in prison, two years of supervised release, mandatory mental health screening, and a $200 special assessment. On July 14, 2021, Ge Song Tao was sentenced in the Middle District of Florida to 42 months confinement, 3 years supervised probation upon release from confinement, a $50,000 criminal fine, and a $200 special assessment. Tao received an upward enhancement for leading the conspiracy and an additional upward variance for obstruction of justice by falsifying evidence and causing a false proffer in a court proceeding.

Tianjin University / Hao Zhang / Wei Pang / Huisui Zhang / Jinping Chen / Zhou Gang / Chong Zhou

The Violation: Between 2006 and 2015, Hao Zhang, Wei Pang, Huisui Zhang, Jinping Chen, Zhou Gang and Chong Zhou (hereinafter referred to as "the team"), conspired to commit economic espionage and theft of trade secrets by stealing trade secrets owned and controlled by U.S. corporations Avago Technologies and Skyworks Solutions. The team, with the assistance of Tianjin University in Tianjin, China, transferred the secrets to China to benefit the PRC government and its foreign instrumentalities; Tianjin MicroNano Manufacturing Tech (MNMT) and ROFS Microsystems (ROFS).

The stolen trade secrets consisted of Surface Acoustic Wave (SAW), Bulk Acoustic Wave (BAW) and Film Bulk Acoustic Resonators (FBAR) technology designated EAR99. SAW and BAW filters are used in wireless devices to remove interference and improve wireless device performance. These filters are commonly used as radio frequency ("RF") filters for mobile phones and other devices for consumer and military applications. The investigation revealed a pattern of concerted and directed theft of valuable trade secrets/technology guided by two of the team who were, at the time, Avago and Skyworks employees; Hao Zhang and Wei Pang. Evidence showed that TJU was directly involved in assisting the team with a scheme to disguise the origin and sources of the stolen technology and provide funding, equipment and the creation of a shell company to be the legitimate source of the stolen trade secrets. Dating back to 2006, Pang, Zhang and other co-conspirators began soliciting PRC universities and others, seeking opportunities to manufacture FBAR technology in China. Pang, Zhang and the others established relationships with officials from TJU, a PRC Ministry of Education University located in the PRC. For several years, Zhang and Pang shared trade secrets with each other and with co-conspirators in China while they worked for the U.S. companies. In 2009, Zhang and Pang obtained professorships at TJU where TJU guided the defendants in filing patent requests and creating a shell company in the Cayman Islands. Subsequently, the shell company and TJU's MNMT created a new company, ROFS, as a joint venture to manufacture products utilizing the stolen trade secrets. Zhang was arrested in the U.S. in May 2015 and in June 2020, was found guilty of Economic Espionage, Theft of Trade Secrets, Conspiracy to Commit Economic Espionage, and Conspiracy to Commit Theft of Trade Secrets. This case resulted from a joint investigation conducted by OEE's San Jose Field Office and the FBI.

The Penalty: On August 31, 2020, Hao Zhang was sentenced in U.S. the District Court for the Northern District of California to 18 months in prison, three years of supervised release, $476,834.81 in restitution, and forfeiture of property (patents). In December 2020, BIS added Pang, Zhang, Chen, Gang, Zhou, Huisui Zhang, ROFS Microsystems, MNMT and TJU to the BIS Entity List.

Ron Hansen / H-11 Digital Forensics

The Violation: Ron Rockwell Hansen, a retired U.S. Army Warrant Officer and former Defense Intelligence Agency Officer, was arrested in June 2018 on his way to the Seattle-Tacoma International Airport in Seattle, Washington as he was preparing to board a flight to China. At the time of his arrest, Hansen was in possession of classified national defense information that he planned to provide to Chinese intelligence services. In early 2014, agents of a Chinese intelligence service targeted Hansen for recruitment and he began meeting with them regularly in China, ultimately making hundreds of thousands of dollars in compensation for the information he provided them. Hansen subsequently admitted knowing that the information was to be used to the injury of the United States and to the advantage of a foreign nation. The investigation of Hansen resulted in charges of attempt to gather or deliver defense information, acting as an agent of a foreign government, bulk cash smuggling, structuring monetary transactions, and smuggling goods from the United States. At the time of recruitment, Hansen had business interests in and relationships with Utah-based companies Nuvestack Inc. and H-11 Digital Forensics Company LLC. The commodities Hansen smuggled from the United States to China included forensic hardware and software with cryptographic capability classified under ECCN 5D992 and controlled for export for anti-terrorism. This case resulted from a joint investigation with OEE's San Jose Field Office, the FBI, and IRS.

The Penalty: On September 24, 2019, Ron Rockwell Hansen was sentenced to 10 years in federal prison for attempting to communicate, deliver, or transmit information involving the national defense of the United States to China. As part of the plea agreement, Hansen agreed to forfeit property acquired from or traceable to his offense, including property used to facilitate the crime.

WMD Controls

Zaosong Zheng

The Violation: In August 2018, Chinese national Zaosong Zheng entered the United States on a J-1 visa and conducted cancer-cell research at Beth Israel Deaconess Medical Center in Boston. Zheng stole vials of biological research, hid the vials in his luggage, and attempted to take them out of the United States aboard a flight destined for China. Zheng was arrested on December 10, 2019, at Logan International Airport in Boston after an outbound search discovered the vials hidden in a sock inside one of Zheng's bags, and not properly packaged. When asked by federal officers whether he was

traveling with any biological items or research, Zheng lied and answered "no." Zheng later admitted he had stolen the vials from a lab at Beth Israel. Zheng stated that he intended to bring the vials to China to use them to conduct research in his own laboratory and publish the results under his own name. On December 3, 2020, Zheng pled guilty to making false, fictitious or fraudulent statements in connection with his theft of 19 vials of biological research. This case resulted from an investigation conducted by OEE's Boston Field Office, the FBI, and U.S. Customs and Border Protection (CBP).

The Penalty: On January 6, 2021, Zheng was sentenced in the U.S. District Court for the District of Massachusetts to time served in prison, three years of supervised released, a $100 special assessment, and removal from the United States.

Mohawk Global Logistics Corp. / Multiwire Laboratories

The Violation: In 2014 and 2015, Multiwire Laboratories (Multiwire) of Ithaca, New York, and Mohawk Global Logistics Corp. (Mohawk) of North Syracuse, New York, each violated the EAR when Multiwire, aided and abetted by Mohawk, twice exported camera detectors and accessories designated EAR99 and valued at $177,156 to the University of Electronic Science and Technology of China (UESTC) in China without the required BIS license. UESTC appeared on the BIS Entity List, and a BIS license was required to export any items subject to the EAR to that entity. Mohawk acted as Multiwire's freight forwarder and Mohawk used screening software in connection with the 2014 transaction, but assertedly did not enter UESTC's full, unabbreviated name (which was known to Mohawk) into the software, which as a result did not "flag" the transaction. Mohawk proceeded with the 2014 transaction and prepared and filed EEI that incorrectly indicated the export was "NLR." In August 2015, Multiwire (again with the assistance of Mohawk) also exported the same items to UESTC, which had been returned to Multiwire for warranty repair. Mohawk also violated the EAR in August 2012, when it aided and abetted the export of a liquid nitrogen plant designated EAR99 and valued at $33,587 to the All-Russian Scientific Research Institute of Experimental Physics (VNIIEF), aka Russian Federal Nuclear Center-VNIIEF (RFNC-VNIIEF). VNIIEF and its RFNC-VNIIEF alias all relevant times appeared on the BIS Entity List. Mohawk was aware of the BIS Entity List and maintained a screening program to detect and prevent shipments to restricted parties. Mohawk compared the name of the ultimate consignee to entries on the BIS Entity List using their screening software, which correctly identified VNIIEF as being listed on the BIS Entity List, and "flagged" the shipment. However, as Mohawk acknowledged to BIS, an export supervisor erroneously overrode or ignored this red flag and Mohawk proceeded without due diligence to forward the items for export. Mohawk prepared and filed EEI on or about that date indicating that the shipment was "NLR." The exporter in this transaction was Cryomech, Inc., of Syracuse, New York, and previously agreed to a settlement with BIS on June 9, 2017, for its role in the unlicensed export. This case resulted from an investigation conducted by OEE's New York Field Office.

The Penalty: On January 16, 2019, Multiwire was assessed a civil penalty of $80,000. On August 10, 2018, Mohawk was assessed a civil penalty of $155,000, $20,000 of which was suspended during the one-year probationary period and thereafter waived, provided no violations are committed during the probationary period. Cryomech, Inc., was previously assessed a civil penalty of $28,000 and ordered to complete an external audit of its export compliance program.

Fuyi Sun / Zhong Li Bang Ye International Trading Co. Ltd.

The Violation: On April 21, 2017, Fuyi "Frank" Sun, a citizen of China, pled guilty to violating the IEEPA in connection with a scheme to illegally export high -grade carbon fiber to China without a license. The carbon fiber, classified under ECCN 1C210, is used primarily in aerospace and military applications. Since approximately 2011, Sun used fraudulent documents and code words in his attempt to acquire high-grade carbon fiber, including Toray type carbon fiber. On April 11, 2016, Sun traveled from China to New York for the purpose of purchasing carbon fiber from an undercover company. During meetings with undercover agents, Sun repeatedly suggested that the Chinese military was the ultimate end user for the carbon fiber he sought to acquire from the undercover company and claimed to have personally worked in the Chinese missile program. On April 12, 2016, Sun agreed to purchase two cases of carbon fiber from the undercover company. Sun paid the undercover agents $23,000 in cash for the carbon fiber, as well as an additional $2,000 as compensation for the risk he believed the undercover company was taking to illegally export the carbon fiber to China without a license. Sun was arrested the next day. This case resulted from a joint investigation conducted by OEE's New York Field Office, HSI, and DCIS.

The Penalty: On August 31, 2017, Sun was sentenced in the U.S. District Court for the Southern District of New York to three years in prison. On June 13, 2018, BIS issued an order denying Sun's export privileges for ten years (until August 31, 2027).

Xun Wang / PPG Paints Trading Shanghai / Huaxing Construction

The Violation: From 2006 through 2007, Chinese companies PPG Paints Trading Shanghai Co Ltd, Huaxing Construction Co Ltd., and Xun Wang, Managing Director of PPG Paints Trading, agreed upon a scheme to export, reexport and transship high-performance epoxy coatings from the United States to Chashma II Nuclear Power Plant in Pakistan. The epoxy coatings, designated as EAR99, were transshipped via a third party in China without having first obtained the required export license. Chashma II is owned by the Pakistan Atomic Energy Commission, which appears on the BIS Entity List. This case resulted from an investigation conducted by OEE's New York Field Office.

The Penalty: In December 2012, Huaxing Construction pled guilty and as part of its plea agreement, agreed to pay the maximum criminal fine of $2 million, with $1 million suspended if no further violations occur during the five years of probation. Under the terms of a related civil settlement, Huaxing Construction also agreed to pay another $1 million, implement an export compliance program, a five-year denial order suspended if no further violations occurring during that period, and be subject to multiple third -party audits over the following five years. Xun Wang also pled guilty and was sentenced to 12 months in prison, a $100,000 criminal fine, and one year of probation. Under the terms of a related civil settlement, Wang also agreed to pay a civil penalty of $250,000 (with $50,000 suspended), and to be placed on the Denied Persons List for a period of ten years with five years suspended. In December 2010, PPG Paints Trading Shanghai pled guilty, and as part of its plea agreement agreed to pay the maximum criminal fine of $2 million, serve five years of corporate probation, and forfeit $32,319 to the U.S. Government. Under the terms of a related civil settlement, PPG Paints Trading Shanghai also agreed to pay a civil penalty of $1 million and complete third-party audits. Huaxing Construction's guilty plea in this case marks the first time a Chinese corporate entity has entered a plea of guilty in a U.S. criminal export matter.

On September 10, 2014, OEE Special Agents, along with the Assistant U.S. Attorney assigned to the case, were awarded the Executive Office of the U.S. Attorney Director's Award by U.S. Attorney General Eric Holder in recognition of their achievement in the category of Superior Performance by a Litigation Team in connection with this investigation.

Other Controls

Jonathan Yet Wing Soong

The Violation: Between August 2016 and September 2020, Jonathan Yet Wing Soong of Castro Valley, California, was employed as a program administrator by Universities Space Research Association (USRA), a nonprofit research corporation focusing on advancing space science and technology. In April 2016, USRA contracted with the National Aeronautics and Space Administration (NASA) to, among other things, license and distribute aeronautics-related Army flight control software for a fee. Soong's duties included conducting and servicing software license sales, export compliance screening of customers, generating software licenses, and exporting software pursuant to purchased licenses. As part of his duties, Soong was responsible for vetting customers to ensure they did not appear on certain restrictive lists—including the BIS Entity List and other U.S. government lists—that placed limitations on the transfer of products to identified entities. Soong admitted that he willingly exported and facilitated the sale and transfer of restricted software designated EAR99 to Beihang University knowing that the University was on the BIS Entity List. In his plea agreement, Soong acknowledged he used an intermediary to complete the export to avoid detection that the real purchaser was on the BIS Entity List. This case resulted from a joint investigation conducted by OEE's San Jose Field Office, DCIS, and the FBI with assistance from the NASA Office of Inspector General; U.S. Army Criminal Investigation Division (Army CID); the U.S. Army Counterintelligence; and HSI.

The Penalty: On May 3, 2023, Yet Wing Soong was sentenced in the U.S. District Court for the Northern District of California to 20 months in prison, three years of supervised release, $168,885 in restitution, and a $100 special assessment. BIS issued Soong a post-conviction denial order for a period of 10 years.

USGoBuy, LLC

The Violation: During 2015, USGoBuy, LLC of Portland, Oregon twice exported rifle scopes classified under ECCN 0A987 and controlled on crime control grounds, without seeking or obtaining the licenses required for these items, to China and the United Arab Emirates. The export to China occurred following an outreach to the company by OEE Special Agents. USGoBuy, a package forwarding company, offers a "BuyForMe" service in which it purchases U.S.-origin items on behalf of its customers, and then exports the items to a foreign addressee and address provided by the customer. Customers create accounts that allow them to enter a purchase request on the USGoBuy website for specific items on U.S. retailer websites by including a link to the product webpage. This case resulted from an investigation conducted by OEE's Portland Resident Office.

The Penalty: On June 17, 2021, USGoBuy, LLC agreed to pay a $20,000 civil penalty, $15,000 of which was suspended provided no violations occur during a three-year probationary period. In addition, a three-year denial of export privileges was imposed.

OEE Special Agents participating in a tactical training exercise

Yantai Jereh Oilfield Services Group Co, Ltd.

The Violation: Yantai Jereh Oilfield Services Group Co., Ltd (Yantai Jereh) in Yantai Shandong Province, China, violated the EAR by ordering, buying, and/or selling oilfield equipment including coiled tubing and pump sets, items subject to the EAR, with the intention to export the items from the United States to Iran via third countries, including China and the United Arab Emirates, without the required authorization. In order to facilitate its business activities in Iran and avoid detection by U.S. law enforcement, Yantai Jereh structured the transactions to conceal from the U.S. suppliers or exporters that the equipment was ultimately destined for use in Iran. Part of this scheme included the involvement of China-based trading company Jinan Tongbaolai Oilfield Equipment Co. Ltd. (JNTBL), which was done to allow Yantai Jereh to claim it was unaware the items were procured to fulfill contracts with Iranian parties. Based on the false information provided to the U.S. parties by Yantai Jereh, Automated Export System filings were made to the U.S. Government indicating that the items were ultimately destined to China or the UAE. A now-former employee of Yantai Jereh employee identifying herself as Jereh's sales manager for Iran claimed that Yantai Jereh had previously left the Iranian market due to the sanction risk because "all the main components we are using [are] from the US." Nonetheless, this former Yantai Jereh employee indicated that Yantai Jereh would try to circumvent U.S. restrictions, building "a new way to access Iranian market that is using a [Chinese trading] company named JNTBL to deal with Iranian client to control the sanctions risk." OEE's investigation found additional correspondence with this same individual, using a JNTBL email address to conduct business with Iranian customers. Additionally, during an interview with OEE Special Agents, a then-Yantai Jereh sales vice president, who was involved in or aware of the attempted exports to Iran, admitted that he was aware of U.S. policy and laws regarding exporting to countries sanctioned by the United States. The company also made false or misleading statements to BIS in the course of its investigation. This case resulted from a joint investigation conducted by OEE's Houston Resident Office, HSI, and CBP.

The Penalty: On December 10, 2018, Yantai Jereh agreed to pay a $600,000 civil penalty. Additionally, a five-year denial of export privileges was imposed on Yantai Jereh, which was suspended provided that during the suspension period Yantai Jereh commits no future violations and pays the civil penalty, and eight additions were made to the BIS Entity List. A concurrent OFAC penalty in the amount of $2,774,972 was issued against Yantai Jereh and its affiliated companies and subsidiaries worldwide.

OEE Special Agents affecting a detention

Chapter 2 – Russia

Criminal and Administrative Case Examples

National Security Controls

By Trade OU

The Violation: Beginning in 2018, operators of a Latvia-based corporation conspired with the operator of By Trade OU, an Estonia-based company, as well as individuals in Russia and a Russia-based company, to violate U.S. export laws and regulations and smuggle a jig grinder that was manufactured in Connecticut to Russia. A jig grinder is a high-precision grinding machine system that does not require a license to be exported to European Union countries but does require a license for export and reexport to Russia because of its potential application in nuclear proliferation and defense programs. At no time did the defendants apply for, receive or possess a license of authorization from the U.S. Department of Commerce to export or reexport the jig grinder to Russia, as required by the Export Control Reform Act of 2018 and the EAR, which restricts the export of items that could make a significant contribution to the military potential of other nations or that could be detrimental to U.S. foreign policy and national security. The jig grinder is classified under ECCN 2B001 and is subject to export control restrictions if it were to be exported to Russia via Latvia and Estonia. The investigation resulted in a March 29, 2023 forfeiture of $484,696. The forfeiture, coordinated through the Organized Crime Drug Enforcement Task Force (OCDETF), represented funds wired into the U.S. to purchase the jig grinder. That money was transferred to Estonia to be used to finance a drone-based program to assess the damage the Russians have done to Ukraine's electrical infrastructure. This is a joint investigation with OEE's Boston Field Office, Homeland Security Investigations, the Federal Bureau of Investigation, the Internal Revenue Service and the United States Attorney's Office. This case resulted from a joint investigation conducted by OEE's Boston Field Office, HSI, and the FBI.

The Penalty: On April 4, 2023, By Trade OU was sentenced in the U.S. District Court for the District of Connecticut to a forfeiture of €312,192.44 (approximately $342,000 in United States currency) in addition to the March 29, 2023 forfeiture of $484,696, and an $800 special assessment. On January 23, 2023 and February 12, 2024, two additional defendants pled guilty and multiple other individuals and businesses defendants have been indicted.

Vorago Technologies, Inc.

The Violation: Beginning on about May 2014 through March 2019, Vorago Technologies of Austin, Texas (known as Silicon Space Technology Corporation during part of this time) conspired to send radiation-hardened 16mB SRAM silicon wafers classified under ECCN 9A515 to Russia without the required BIS export license authorization, and ultimately did so, knowingly, via a Bulgarian front company. Vorago Technologies, Inc. (Vorago) designed and manufactured radiation-hardened and extreme-temperature hardened integrated circuit components that could be used in satellite, military, medical, automotive, oil & gas, mining, and other industrial applications. The company had contracts with the U.S. Air Force, Missile Defense Agency, NASA, and other government agencies. This case resulted from an investigation conducted by OEE's Houston Resident Office.

The Penalty: On September 28, 2021, Vorago Technologies agreed to a civil penalty of $497,000, $247,00 of which was suspended, along with a two-year suspended denial of export privileges. Previously, the U.S. Department of Justice entered into a three-year Non-Prosecution Agreement with Vorago related to these illegal transactions and previously returned an indictment against three foreign nationals for related conduct. Additionally, three Russian companies and four Russian individuals were added to the BIS Entity List in connection with this investigation.

Tsvetan Kanev / VEKA, Ltd

The Violation: Between 2015 and 2016, Tsvetan Kanev, owner of VEKA, Ltd in Sofia, Bulgaria, willfully attempted to export and caused to be exported radiation-hardened integrated circuits (RHIC) to the Russian military and space program. The RHICs, classified under ECCNs 3A001 and 9A515, are designed for aerospace applications and controlled for national security reasons. Kanev had initially inquired about the parts with a U.S. manufacturer and told the manufacturer that the RHICs were sought by the Bulgarian Academy of Science. Being suspicious of the inquiry,

the U.S. manufacturer referred the matter to federal law enforcement. Acting in an undercover capacity, Special Agents communicated with Kanev and offered to sell the RHICs. In doing so, it was discovered that Kanev intended to transship the items from Bulgaria through Finland to the Russian military and space program. Kanev engaged the Undercover Agents (UCA) in two transactions, and he acknowledged the illegality of each transaction during business negotiations. In two separate transactions, Kanev transferred over $350,000 to purchase RHICs intended for the Russian military and space program. Kanev structured the payments to avoid scrutiny from banking authorities and completed fraudulent end user statements to deceive U.S. authorities. Additionally, Kanev paid the UCAs extra fees totaling over $50,000 as compensation for the risk involved and for violating U.S. laws. All monies transferred to the UCAs were seized and forfeited to the United States. Kanev was arrested in Germany in January 2020 and extradited to Colorado. This case resulted from a joint investigation conducted by OEE's Dallas Field Office, HSI, and DCIS.

The Penalty: On May 21, 2021, Kanev was sentenced to 24 months in prison, forfeiture of monies transferred to UCAs, and a $100 special assessment.

Comtech Xicom Technology, Inc.

The Violation: Between 2015 and 2017, Comtech Xicom Technology, Inc. (Comtech), located in Santa Clara, California, engaged in conduct prohibited by the EAR when it exported traveling wave tubes classified under ECCN 3A001 and controlled for National Security reasons to Russia, Brazil and the UAE, without seeking or obtaining the required BIS authorization. Comtech is a satellite communications manufacturer and seller of amplifiers, traveling wave tubes (TWTs) and related products for both commercial and military broadcast and broadband applications. In 2017, OEE notified Comtech of unfavorable post shipment verification (PSV) check on Comtech shipments of TWTs exported to the United Arab Emirates and Russia. Upon discovering that the company had failed to obtain licenses for both shipments despite a previous license history and knowledge that those items required a license to both destinations, OEE directed Comtech to conduct an internal review of their exports. The internal review found additional transactions involving exports of TWT's without the requisite licenses to Brazil and Russia. This case resulted from an investigation conducted by OEE's San Jose Field Office.

The Penalty: On March 11, 2021, Comtech agreed to pay a civil penalty of $122,000.

Julian Demurjian / CIS Project LLC

The Violation: Between December 2014 and August 2015 Julian Demurjian and CIS Project LLC, a company that Demurjian owned and operated, caused, aided, or abetted seven violations of the EAR. The seven violations were in connection with the submission of false or misleading information of the values of telecommunications networking equipment controlled for national security, encryption, or anti-terrorism reasons and destined for Russia. Demurjian and CIS Project prepared invoices on CIS Project letterhead that significantly undervalued the items and provided these invoices to a freight forwarder. The freight forwarder subsequently filed EEI containing the false value information in the Automated Export System for each of the shipments. Additionally, in February 2015, Demurjian and CIS Project generated and provided to the freight forwarder an invoice on CIS Project letterhead that falsely undervalued the items so that the stated value did not exceed $2,500, and thus did not appear to trigger an EEI filing requirement. This case resulted from a joint investigation conducted by OEE's San Jose Field Office, the FBI, and HSI.

The Penalty: On January 27, 2021, Demurjian agreed to settle the charges and to resolve the matter, Demurjian was assessed a civil penalty of $540,000, with an out-of-pocket payment of $60,000. He was also subjected to a two-year suspended denial of his export privileges.

Peter Zuccarelli / Syed Razvi / American Coating Technologies

The Violation: Between approximately June 2015 and March 2016, Peter Zuccarelli and Pakistani naturalized U.S. citizen Syed Razvi agreed to illegally export space-grade radiation hardened integrated circuits (RHICs) to Russia and

China. The microchips, classified under ECCN 9A515, are used in satellites and space probes but also have military uses, such as guiding ballistic missiles. In furtherance of the conspiracy, Razvi received purchase orders from customers seeking to purchase RHICs for use in China's and Russia's space programs. Zuccarelli, owner/CEO of American Coating Technologies, in Carrollton, Texas, received these orders from Razvi, as well as payment of approximately $1.5 million to purchase the RHICs for the Chinese and Russian customers. Zuccarelli placed orders with U.S. suppliers, and used the money received from Razvi 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. In an attempt to hide the conspiracy from the U.S. government, he created false paperwork and made false statements. This case resulted from a joint investigation conducted by OEE's Dallas Field Office, the FBI, HSI, DCIS, and the U.S. Postal Inspection Service (USPIS).

The Penalty: On April 22, 2019, Syed Razvi was sentenced to 46 months in prison, three years of supervised release, a $20,000 criminal fine, and a $100 special assessment. On January 24, 2018, Peter Zuccarelli was sentenced to 46 months in prison, three years of supervised release, a $50,000 criminal fine, and a $100 special assessment.

Arc Electronics / Alexander Fishenko / Alexander Posobilov / Shavkat Abdullaev / Anastasia Diatlova

The Violation: Between 2008 and 2012, Alexander Fishenko, owner of Houston, Texas-based Arc Electronics, and several of its employees obtained advanced microelectronics valued at over $30 million from manufacturers and suppliers located within the United States and exported those goods to Russia, while carefully evading the government export licensing system. They provided false end-user information in connection with the purchase of the goods, concealed the fact that they were resellers, and falsely classified the goods they exported on export records submitted to the Department of Commerce. The microelectronics shipped to Russia included analog-to-digital converters, static random access memory chips, microcontrollers and microprocessors. These commodities are classified under ECCN 3A001 and are subject to export controls due to their potential use in a wide range of military systems, including radar and surveillance systems, weapons guidance systems, and detonation triggers. This case resulted from a joint investigation conducted by OEE's Houston Resident Office, the FBI, NCIS, and the IRS.

The Penalty: On October 26, 2015, after a month-long trial, Alexander Posobilov, Shavkat Abdullaev and Anastasia Diatlova were convicted in the U.S. District Court for the Eastern District of New York. On February 28, 2017, Posobilov was sentenced to 135 months in prison. In September 2015, Alexander Fishenko pled guilty in connection with the illegal exports. On October 9, 2012, BIS added 165 foreign persons and companies to its Entity List for allegedly engaging in this illegal export scheme.

Military Controls

Microsoft Corporation

The Violation: On seven occasions between December 2016, and December 2017, employees of Microsoft Russia caused another Microsoft subsidiary to enter into or sell software licensing agreements that would allow the transfer or access to software subject to the EAR by FAU 'Glavgosekspertiza Rossii' and United Shipbuilding Corporation Joint Stock Company ("United Shipbuilding Corporation"), both of which were on the BIS Entity List. FAU 'Glavgosekspertiza Rossii' is a Russian federal institution involved with construction projects, including the Kerch Bridge, which was built to connect Crimea to Russia after its 2014 invasion. United Shipbuilding Corporation is responsible for developing and building the Russian Navy's warships. In the case of FAU 'Glavgosekspertiza Rossii', certain Russia-based employees of Microsoft Russia ordered software licenses through one of Microsoft's Open sales programs in the names of parties not on the BIS Entity List; in the case of United Shipbuilding, an increased number of software licenses were added under non-listed affiliates' enterprise agreements. This case resulted from a joint investigation conducted by OEE's Portland Resident Office and OFAC.

The Penalty: On April 26, 2023, as part of a coordinated enforcement effort, BIS and the Department of the Treasury's Office of Foreign Assets Control imposed a combined $3.3 million in civil penalties against Microsoft Corporation.

Voluntary Self-Disclosure: Microsoft Corporation of Redmond, Washington, voluntarily disclosed the violations to both BIS and OFAC and cooperated fully with the investigation.

Arif Ugur

The Violation: Arif Ugur founded and was the sole manager of Anatolia Group Limited Partnership (Anatolia), a domestic limited partnership registered in Massachusetts. Beginning in approximately July 2015, Ugur bid on and acquired numerous contracts to supply the U.S. Department of Defense (DOD) with various parts and components intended for use by the U.S. military. Many of these contracts required that the parts be manufactured in the United States. Both in bids submitted to DOD and in subsequent email communications with DOD representatives, Ugur falsely claimed that Anatolia was manufacturing the parts in the United States. In fact, Anatolia was a front company with no manufacturing facilities whatsoever. Unbeknownst to DOD, Ugur contracted with a company in Turkey to make the parts and then passed them off to DOD as if they had been manufactured by Anatolia in the United States. Because they had not been manufactured in the United States in accordance with the contacts, Ugur failed to allow DOD to inspect the parts prior to delivery to the U.S. military. Many of the parts were substandard and some could not be used at all. To enable the Turkish company to manufacture the parts, Ugur shared technical specifications and drawings of the parts with his co-conspirators overseas, some of whom were employees of the Turkish company. Ugur also provided his overseas co-conspirators with access to DOD's online library of technical specifications and drawings. Ugur knew of the export license requirements, but nonetheless exported controlled technical data to employees of the Turkish manufacturer without the required authorization. This case resulted from a joint investigation conducted by OEE's Boston Field Office, HSI, and DCIS.

The Penalty: On December 14, 2022, Ugur was sentenced in the U.S. District Court for the District of Massachusetts to 33 months in prison, two years of supervised release, and a $500 special assessment.

Patriot 3, Inc.

The Violation: On or about October 16, 2014, Patriot 3, Inc. of Fredericksburg, Virginia, sold and/or transferred maritime jet boots with underwater propulsion systems (JetBoots) for export to military end users in Russia with knowledge that a violation of the Regulations had occurred or was about to occur. The items are classified under ECCN 8A992 and valued at approximately $329,760. This case resulted from an investigation conducted by OEE's Washington Field Office.

The Penalty: On June 28, 2021, Patriot 3, Inc. agreed to pay a $200,000 civil penalty.

Alexander Brazhnikov / ABN Universal

The Violation: Alexander Brazhnikov, owner of ABN Universal in Carteret, New Jersey, and his companies were part of a sophisticated procurement network that obtained and smuggled more than $65 million worth of regulated, sensitive electronic components from American manufacturers and vendors and exported those items to the Federal States Unitary Enterprise Russian Nuclear Center - Academician E.I. Zababkhin All-Russian Scientific Research Institute of Technical Physics, and MIG Electronics, located in Russia. Both companies appear on the BIS Entity List. Brazhnikov was responsible for nearly 2,000 illegal shipments of EAR99 electronics components, many of which wound up in the hands of Russian military and security forces. Brazhnikov also took extensive measure to conceal the true destination of the parts and to conceal the true sources of funds in Russia, as well as the identities of the various Russian defense contracting firms receiving U.S.-origin electronics components. This case resulted from a joint investigation conducted by OEE's New York Field Office, the FBI, and HSI.

The Penalty: On June 30, 2016, Alexander Brazhnikov was sentenced in the U.S. District Court for the District of New Jersey to 70 months in prison, a $75,000 criminal fine, a $65 million forfeiture, forfeiture of his two houses valued at approximately $500,000 each, and a $300 special assessment. In the related administrative case, the BIS Acting Under Secretary affirmed a recommended decision from an administrative law judge imposing a 15-year denial order against Brazhnikov.

Other Controls

Intertech Trading Corporation

The Penalty: In July 2022, Intertech Trading Corporation (Intertech) of Atkinson, New Hampshire, pled guilty in connection with the failure to file Electronic Export Information (EEI) related to exports of scientific equipment designated EAR99 to Russia and Ukraine. According to court documents and statements made in court, between 2015 and 2019, Intertech exported laboratory equipment to Russia, Ukraine and elsewhere, falsely describing the nature and value of the exported items on commercial invoices and shipping forms. In its plea agreement, Intertech admitted that it used false, innocuous descriptions such as "lamp for aquarium" or "spares for welding system," rather than accurately identifying the sophisticated scientific equipment actually contained in the shipments. Intertech admitted that it drastically undervalued the shipments, thereby evading the requirement to file EEI. This case resulted from a joint investigation conducted by OEE's Boston Field Office and the FBI.

The Violation: On October 17, 2022, Intertech was sentenced in the U.S. District Court for the District of New Hampshire to two years of probation, a $140,000 fine, and a $5,600 special assessment.

Azamat Bobomurodov / Anton Perovznikov / Shoruh Saidov / Akmal Asadov / Zokir Iskanderov

The Violation: This investigation involved the smuggling of stolen cellular telephones and other electronic devices to Russia. Between June 2021 and January 2022, Azamat Bobomurodov, Anton Perovznikov, Shoruh Saidov, Akmal Asadov, Zokir Iskanderov and several other defendants each pled guilty in the U.S District Court for the Eastern District of New York in connection with these charges. This case resulted from a joint investigation conducted by OEE's New York Field Office and the FBI, with assistance from HSI and CBP.

The Penalty: On September 21, 2022, Bobomurodov was sentenced to one year of probation, a $4,000 criminal fine, and a $100 special assessment. Also on September 21, 2022, Perevoznikov was sentenced to 24 months in prison, two years of supervised release, and a $100 special assessment. On September 20, 2022, Saidov was sentenced to 15 months in prison, two years of supervised release, a $100,000 forfeiture, and a $200 special assessment. Also on September 20, 2022, Asadov was sentenced to 15 months in prison, two years of supervised release, $300,000 in restitution, and a $200 special assessment. On February 11, 2022, Iskanderov was sentenced to one year of probation and a $100 special assessment.

World Mining Supply LLC / Dali Bagrou / Oleg Nikitin / Gabriele Villone / GVA International Oil and Gas Services / KS Engineering

The Violation: This investigation involved a conspiracy to attempt to purchase from OEE Undercover Agents a power turbine and a generator designated EAR99 on behalf of Gazprom-Neft/Gazprom-Neft Shelf in Russia, which appears on the BIS Entity List. Gazprom-Neft attempted to pay approximately $23 million to acquire the items illegally from the United States for its sanctioned Prirazlomnaya Arctic Marine Ice Resistant Stationary Platform. Approximately $2.8 million was transferred into an OEE Undercover bank account as the down payment for the purchase of the turbine and generator. On October 1, 2019, Dali Bagrou, Oleg Nitikin, Gabriele Villone, World Mining Supply LLC, KS Engineering, and GVA International Oil and Gas Services (GVA) were indicted in the U.S. District Court for the Southern District of Georgia. All six defendants pled guilty. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, the FBI, and DCIS.

The Penalty: On November 10, 2021, Bagrou was sentenced to 51 months in prison, three years of probation, a $400 special assessment, and forfeiture of his home, which was purchased with illicit proceeds. World Mining and Oil Supply was sentenced to five years of probation and a $400 special assessment. On September 27, 2021, GVA was sentenced to five years of probation. On September 22, 2021, Oleg Nikitin was sentenced to 28 months in prison and a $5,00 criminal fine, and on the same date KS Engineering was sentenced to five years of probation. On June 11, 2020, Gabriele Villone was sentenced to 28 months in prison. In June 2022, Gazprom-Neft Shelf, LLC was also added to the BIS Entity List. Several indicted individuals remain fugitives overseas.

Gene Shilman

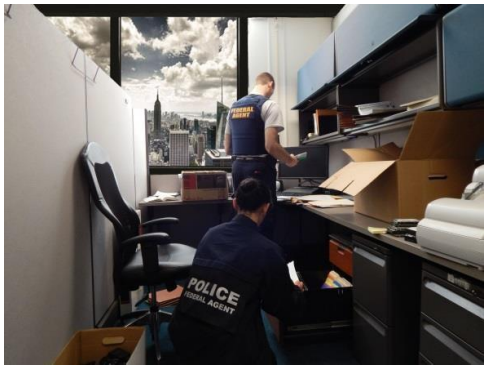
The Violation: The investigation of Gene Shilman was initiated after Ukrainian law enforcement authorities seized gun parts that were imported into Ukraine from the United States. These gun parts were exported from the United States by Gene Shilman, who was operating a weapons company from his home located in Elizabeth, New Jersey. After the seizure, the Ukrainian authorities contacted the FBI, who then contacted OEE's New York Field Office to assist with the investigation. Special Agents used numerous administrative subpoenas to gather shipping, purchasing, and payment information for the export of these weapons parts to Ukraine. Most of the gun parts (to include body armor and night vision goggles) were purchased from manufacturers and gun parts retailers in the United States. The investigation uncovered several packages that were sent though a mail forwarding location in Newark, New Jersey that would consolidate items for export without being inspected. As the investigation continued, the mail forwarding facility began to cooperate with Special Agents from OEE and the FBI and would inform them of pending export shipments. These shipments would then be inspected and subsequently seized as part of the illegal exports to Ukraine being conducted by Shilman. OEE and the FBI set up a mail cover operation and began to monitor items being exported through the U.S. Post Office. As a result, USPIS joined the investigation. A search warrant was executed at Shilman's home business, which led to his arrest. In late 2018, Shilman pled guilty in 2019 to exporting rifle scopes classified under ECCN 0A987 to Ukraine and Russia without the required export license authorization. This case resulted from a joint investigation conducted by OEE's New York Field Office, the FBI, and USPIS.

The Penalty: On May 25, 2019, Shilman was sentenced to 24 months in prison.

Gennadiy Boyko / SHOPOZZ, Inc.

The Violation: On December 6, 2017, Gennadiy Boyko pled guilty in the U.S. District Court for the Northern District of Georgia in connection with conspiring to violate the IEEPA and the Arms Export Control Act. Boyko is the owner of SHOPOZZ, Inc., a mail consolidation and forwarding business located in Alpharetta, Georgia that provides a virtual U.S. address for individuals located in Russia and Ukraine. Boyko and his co-conspirators utilized his business to illegally export EAR-controlled rifle optics classified under ECCN 0A987 as well as ITAR-controlled weapons parts to Russia and Ukraine. The items were ordered from U.S. online vendors and then shipped to SHOPOZZ or Boyko's home, repacked with other innocuous items and then shipped out of the country. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, the FBI, DCIS, and CBP.

The Penalty: On November 28, 2018, Gennadiy Boyko was sentenced to 18 months in prison, one year of supervised release, 100 hours of community service, and a $100 special assessment.



Chapter 3 - Iran

Criminal and Administrative Case Examples

National Security Controls

Johnny Tourino / Spectra Equipment, Inc.

The Violation: Johnny Tourino of Dana Point, California owned and operated Spectra Equipment Inc., a Laguna-Niguel based computer support and services company. Between September 2015 and March 2017, Tourino negotiated the sale of five business-class computer servers valued at $2.1 million, and attempted to have them sent to Iran for use by two Iranian financial institutions. When the manufacturer of the servers asked Tourino to identify the end user, he falsely stated that the servers were being sold to a bank in Africa and "NOT going to Iran." Later that month, Tourino, through is lawyer, falsely represented to the manufacturer that the servers were going to Slovenia. Roughly one week later, Tourino sent three checks to the manufacturer as partial payment for the servers. After learning that the Department of Treasury had blocked funds from Iran that were to be used to pay for the servers, Tourino deleted his emails and contacted the U.S. Department of the Treasury and again falsely stated that the servers were not going to Iran and were destined for Slovenia. This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office, the FBI, and the IRS.

The Penalty: On December 8, 2023, Tourino was sentenced in the U.S. District Court for the Central District of California to 18 months in prison, three years of supervised release, a $20,000 criminal fine, forfeiture of $2,124,859, and a $100 mandatory special assessment.

DES International Co., Ltd.

The Violation: DES International Co. Ltd., (DES) located in Taiwan, conspired with others to procure goods for the benefit of Iranian government entities and business organizations, including goods that originated in the United States. DES procured goods from the United States for the benefit of Iranian government entities and business organizations. In particular, a sales agent helped an Iranian research center obtain U.S. goods without a license from the U.S. Department of the Treasury. These goods included a power amplifier designated for use in electromechanical devices as well as cybersecurity software. The sales agent took steps to conceal the U.S.-origin of the goods, including by removing serial numbers stickers with the phrase "Made in USA" from packages, and by causing the cybersecurity software to be downloaded onto a computer outside of Iran. This case resulted from a joint investigation conducted by OEE's Dallas Field Office, HSI, DCIS and the FBI.

The Penalty: On April 26, 2023, DES International Co., Ltd. was sentenced in the U.S. District Court for the District of Columbia to a $83,769 criminal fine, five years of probation, and a $400 special assessment.

Stefan Gillier

The Violation: In September 2022, Stefan Gillier was found guilty following a criminal trial in the U.S. District Court for the Southern District of New York in connection with a scheme to fraudulently obtain aircraft parts from Honeywell International, Inc. (Honeywell), some of which were exported to Iran via Turkey. Gillier was the president and ran the day-to-day business activities of RTF International (RFT), a broker of aircraft parts. RTF obtained aircraft parts from Honeywell, paying for them by checks written in foreign currency and for amounts well above the cost of the parts, which created an apparent credit balance in RTF's favor in Honeywell's accounting system. In total, Gillier was able to obtain over $6 million worth of aircraft parts from Honeywell without paying for the parts. Gillier was arrested and extradited from Italy in 2019. This case resulted from a joint investigation conducted by OEE's New York Field Office, DCIS, HSI and the FBI.

The Penalty: On March 9, 2023, Gillier was sentenced in the U.S. District Court for the Southern District of New York to 84 months in prison, three years of probation, $3,509,916 in restitution and an $800 special assessment.

Nordic Maritime Pte. Ltd. and Morten Innhaug

The Violation: On March 11, 2020**,** Nordic Maritime Pte. Ltd. (Nordic), and its Chairman, Morten Innhaug, were found to have committed four violations of the EAR for their respective roles in the illegal reexport of controlled undersea surveying equipment to Iran for use in surveying an Iranian oil field. Specifically, between May 2012 and April 2013, Nordic knowingly used seismic surveying equipment classified under ECCN 6A001, and controlled for National Security and Anti-Terrorism purposes, to conduct a survey of the Forouz B natural gas field in Iranian territorial waters under a contract for the ultimate benefit of the state-owned National Iranian Offshore Oil Company. Nordic and Innhaug were informed by the owner of the items that their use in Iranian waters would violate the EAR and was provided with a copy of the BIS re-export license issued to the owner listing all of the license conditions, but they nevertheless proceeded to re-export the items to Iran without authorization from either BIS or OFAC. Upon discovery of the violations by BIS, Nordic then made a written submission falsely stating that the owner of the items had never advised Nordic that the equipment was subject to a BIS re-export license, never provided Nordic with a copy of the re-export license, and never advised Nordic of the license conditions.

After a hearing, an administrative law judge determined that Nordic committed three violations including acting with knowledge when it illegally re-exported the items and making false and misleading statements to BIS during the investigation. Nordic's Chairman, Morten Innhaug, was also found to have aided and abetted Nordic in violating the Regulations. This case resulted from an investigation conducted by OEE's Houston Resident Office.

The Penalty: On March 11, 2020, the BIS Acting Under Secretary issued an order denying the export privileges of both Nordic and Innhaug for 15 years and remanded the case to the ALJ for further consideration of a civil monetary penalty. On August 19, 2020, the BIS Acting Under Secretary then issued a second order imposing a $31,425,760 civil monetary penalty jointly and severally against Nordic and Innhaug in addition to the 15-year denial orders.

Alireza Jalali / Negar Ghodskani / Green Wave Telecommunication

The Violation: As part of a conspiracy to export digital communication devices classified under ECCN 3A001 to Iran, Negar Ghodskani assisted in establishing and operating Green Wave Telecommunication Sdn Bhn, a Malaysian company. Green Wave operated as a front company for Fanavar Moj Khavar (Fana Moj), an Iran-based company that specializes in broadcast communications, microwave communications as well as the production of digital video broadcasting equipment. Fana Moj supplies microwave radio systems and wireless broadband access in Iran. Fana Moj's principal customer was the Islamic Republic of Iran Broadcasting, which is controlled by the Government of Iran. In 2017, Fana Moj was designated by OFAC as a Specially Designated National (SDN) for providing financial, material, technological or other support for, or goods or services in support of, the Iranian Revolutionary Guard Corps (IRGC). Ghodskani, who was based in Tehran, falsely represented herself as an employee of Green Wave to U.S. companies in order to obtain controlled technology from the United States on behalf of Fana Moj. Ghodskani and her co-conspirators concealed the ultimate destination and end users of the exported technology through false statements and unlawful financial transactions. When received by Green Wave in Malaysia, the goods were repackaged and unlawfully exported from Malaysia to Fana Moj in Iran. On August 9, 2019, and November 29, 2017, Ghodskani and Jalali pled guilty, respectively, to conspiracy to defraud the government in the U.S. District Court for the District of Minnesota. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, the FBI, and HSI.

The Penalty: On September 24, 2019, Negar Ghodskani was sentenced to 27 months in prison. On March 20, 2018, co-defendant, Alireza Jalali was sentenced to 15 months of prison.

Military Controls

Saber Fakih

The Violation: Saber Fakih of the United Kingdom conspired with others to export and attempt to export an industrial microwave system and a counter-drone system from the United States to Iran without first obtaining the requisite license from OFAC. Fakih's co-conspirators held themselves out as procurement agents of Rayan Roshd, which has been sanctioned by the U.S. Government for its procurement activities related to the IRGC. Potential military

uses of the industrial microwave systems (with some modification) include high-power microwave-based Directed-Energy Weapon systems. The counter-drone system, which has both commercial and military uses, can be used to stop, identify, redirect, land or take control of a target unmanned aerial vehicle. Fakih admitted in his statement of offense that he was the primary liaison between the Iranian purchaser and the U.S.-based seller of the industrial microwave system. He placed a bid with the Massachusetts vendor, coordinated an inspection of the machine, and generally corresponded with the vendor, knowing the item was ultimately destined for Iran. This case resulted from a joint investigation conducted by OEE's Washington Field Office, the FBI and HSI.

The Penalty: On February 1, 2024, Fakih was sentenced in the U.S. District Court for the District of Columbia to 18 months in prison, three years of supervised release, and a $100 special assessment.

Edsun Industries / Joyce Eliabachus / Edsun Industries / Peyman Amiri Larijani

The Violation: On June 11, 2019, Joyce Eliabachus pled guilty to conspiracy to violate the IEEPA in connection with her role in an international procurement network that smuggled over $2 million worth of aircraft components to Iran through the United Arab Emirates and Turkey. Eliabachus was the principal officer and operator of Edsun Equipments LLC, a New Jersey-based aviation parts trading company run out of her residence. Peyman Amiri Larijani was the owner of an Iran-based procurement firm and served as operations and sales manager of a network of supply and engineering companies in Tehran, Iran, and Istanbul, Turkey. From May 2015 through October 2017, Eliabachus, Larijani, and their co-conspirators facilitated at least 49 shipments containing 23,554 controlled aircraft parts from the United States to Iran, all of which were exported without the required licenses. Eliabachus conspired with Larijani, whose international network helped initiate the purchase of U.S.-origin aircraft components on behalf of Larijani's clients in Iran. The network's client list included Iranian airline companies, several of which have been officially designated by the United States as a threat to national security, foreign policy, or economic interests. One company, Mahan Air Co., has been subject to sanctions by the United States for providing financial, material and technological support to the Islamic Revolutionary Guard Corps-Qods Force, and allegedly ferrying arms and reinforcements to designated terrorist groups such as Hezbollah and Hamas. Eliabachus used her company to finalize the purchase and acquisition of the requested components from the various U.S.-based distributors. She repackaged and shipped the components to shipping companies in the UAE and Turkey, where Larijani and other Iranian conspirators directed 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 avoid 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 Iranian purchasers, funneled through Turkish bank accounts held in the names of shell companies controlled by the Iranian conspirators. The money was ultimately transferred into one of Edsun Equipments' accounts in the United States. This case resulted from a joint investigation conducted by OEE's New York Field Office and HSI.

The Penalty: On October 6, 2020, Joyce Eliabachus was sentenced in the U.S. District Court for the District of New Jersey to 18 months in prison, one year of supervised release, and a $100 special assessment.

Aiden Davidson aka Hamed Aliabadi Davidson

The Violation: Aiden Davidson, also known as Hamed Aliabadi Davidson, is a citizen of Iran and a naturalized citizen and resident of the United States. Davidson was the manager/member and registered agent of a New Hampshire limited liability company, Golden Gate International, LLC. Babazadeh Trading Co., aka Babazadeh Hydraulic Trading Group was an Iranian company that operated an online resale business based in Tehran, Iran. Stare Lojistik Enerji Sanayi Ticaret was a Turkish freight forwarding company with a location in Igdir, Turkey. Between December 2016 and February 2017, Davidson and Golden Gate smuggled goods from Savannah, Georgia, to Babazadeh in Iran. The goods included motors, pumps, valves, and other items designated EAR99 and valued at more than $100,000. Documents related to the shipments falsely identified the ultimate consignee of the shipments as Stare in Turkey. In causing the unlicensed exportation of these goods, Davidson and Golden Gate willfully evaded national security controls related to transactions with Iran. All told, between 2014 and 2017, Davidson caused a total of at least ten exports of containers of industrial goods and equipment including items demilitarized by the Defense Department, from the U.S. to Iran. During

that period he received approximately $1 million in international wire transfers to Golden Gate's bank account in New Hampshire. Davidson was arrested in September 2018 prior to boarding a flight from Atlanta to Turkey. This case resulted from an investigation conducted by OEE's Boston Field Office and HSI.

The Penalty: On July 16, 2020, Davidson was sentenced to 46 months in prison, 12 months of supervised release, and a $200 special assessment.

On March 30, 2021, several OEE Special Agents received the Excellence in the Pursuit of Justice Award from the U.S. Attorney's Office for the District of New Hampshire for their work on this investigation.

Resit Tavan / Ramor Construction

The Violation: In June 2017, Turkish company Ramor Construction and Turkish Nationals Resit Tavan and Fulya Oguzturk were indicted for conspiring to defraud the United States by exporting marine equipment from the state of Wisconsin in violation of the IEEPA and the ITSR. The violations involved a scheme to transship U.S.-origin marine parts and components designated EAR99 and classified under ECCN 8A992 to Iran through Turkey. Some of the items, including surface drives and generators, were for use by the Islamic Revolutionary Guard Corps-Navy on a prototype attack boat. Tavan pled guilty in April 2019. Oguzturk remains at large with an outstanding arrest warrant issued in June 2017. In December 2019, a Red Notice seeking Oguzturk's arrest was issued by INTERPOL. This case resulted from a joint investigation conducted by OEE's Chicago Field Office and the FBI.

The Penalty: On August 29, 2019, Tavan was sentenced in the U.S. District Court for the Eastern District of Wisconsin to 28 months in prison. Prior to these charges, Resit Tavan and Ramor Construction were added to the BIS Entity List. On December 31, 2019, a 10-year denial order was issued for Tavan and Ramor Construction.

David Levick / ICM Components

The Violation: On February 1, 2019, Australian national David Levick pled guilty to charges related to his involvement in the procurement and shipment of U.S.-origin items, including aircraft parts classified under ECCN 9A991 and controlled under the U.S. Munitions List, to Iran. Levick, the General Manager of ICM Components, Inc. in Thornleigh, Australia, solicited purchase orders and business for aircraft parts from a representative of a trading company in Iran. This individual in Iran also operated and controlled companies in Malaysia that acted as intermediaries for the Iranian trading company. Levick then placed orders with U.S. companies on behalf of the Iranian individual for the goods, which included aircraft parts, precision pressure transducers that have a wide variety of applications in the avionics industry, emergency flotation systems kits designed for use on Bell 206 helicopters to assist when landing in water or soft desert terrain, and shock mounted light assemblies designated for high vibration use that can be used on helicopters and other fixed wing aircraft. When necessary, Levick used a broker in Tarpon Springs, Florida, through whom orders could be placed for the parts to further conceal that they were intended for transshipment to Iran. Levick intentionally concealed the ultimate end use and end users of the parts from manufacturers, distributors, shippers, and freight forwarders located in the United States and elsewhere. In addition, Levick and others structured their payments between each other for the parts to avoid trade restrictions imposed on Iranian financial institutions by other countries. Levick and ICM Components wired money to companies in the United States as payment for the parts. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, HSI, and DCIS.

The Penalty: On March 21, 2019, Levick was sentenced in the U.S. District Court for the District of Columbia to 24 months in prison, 12 months of supervised release, a $199,227 forfeiture, a $400 special assessment, and deportation upon completion of his sentence.

Arash Sepehri / Tajhiz Sanat Shayan

The Violation: Between 2008 and 2014, Iranian citizen Arash Sepehri, an employee and member of the board of directors of Tehran-based Tajhiz Sanat Shayan (TSS), conspired with individuals and companies operating in Hong Kong, the United Arab Emirates (UAE), and Iran to send hundreds of thousands of dollars' worth of U.S.-origin goods and technology, most with military applications, to Iran. 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. Sepehri and his conspirators relied on well-known techniques to evade export controls and sanctions including the use of aliases, front companies, and circuitous shipping and payment methods. These techniques allowed Sepehri to conceal both the true end users and intended use of the procured goods. Through TSS and associated companies, Sepehri and others conspired to obtain high-resolution sonar equipment, data input boards, laptops, and acoustic transducers classified under ECCN 6A991 and designated EAR99, as well as a lens for a missile tracking device controlled under the ITAR, to Iran via Hong Kong and the UAE. In June 2018, Sepehri was returned to the United States based on an Interpol Diffusion Notice. On November 7, 2018, Sepehri, pled guilty in the U.S. District Court for the District of Columbia for his role in the scheme. This case resulted from a joint investigation conducted by OEE's Washington Field Office, HSI, and the FBI.

The Penalty: On February 26, 2019, Arash Sepehri was sentenced to 25 months in prison with credit for time served, a $100 special assessment and a $125,661 forfeiture. In addition, on September 30, 2019, a seven-year denial order was imposed against Sepehri.

Arzu Sagsoz / Kral Havacilik

The Violation: On October 4, 2018, Arzu Sagsoz pled guilty in the U.S. District Court for the District of Columbia to conspiracy to violate the IEEPA. Sagsoz was arrested on September 27, 2017, by law enforcement authorities at the Batumi International Airport in the country of Georgia pursuant to an Interpol Red Notice submitted by BIS. After a period of detention in Georgia, Sagsoz was extradited to the United States and was arrested and processed upon her arrival at Washington Dulles International Airport. Sagsoz operated as a corporate employee of Turkish Aviation Supply Company, Kral Havacilik, which was responsible for illegally supplying the Iranian airline Mahan Air with U.S.-origin aircraft parts. Mahan Air has been subject to a BIS Temporary Denial Order since 2008. In 2011, Mahan Air was also added to OFAC's SDN List for Mahan Air's support of global terrorism. This case resulted from an investigation conducted by OEE's Atlanta Resident Office and Washington Field Office.

The Penalty: On January 10, 2019, Arzu Sagsoz was sentenced to 20 months in prison, with credit for time served in the country of Georgia, one year of probation, and a $100 special assessment.

WMD Controls

Murat Bukey

The Violation: Turkish citizen Murat Bukey and Iranian citizen Amanallah Paidar conspired to procure and export U.S.-origin technology for Iran through their companies Farazan Industrial Engineering in Iran and Ozon Spor Ve Hobbi Urunleri in Turkey. Specifically, Bukey and Paidar exported and transshipped to Iran via Turkey a device that can test the efficacy and power of fuel cells classified under ECCN 1A004 and a bio-detection system that has application in weapons of mass destruction research and use. Bukey was extradited to the United States from Spain in July 2022 and pled guilty in December 2022. Paidar is a fugitive and remains at large. This case resulted from a joint investigation conducted by OEE's Boston Field Office and the FBI.

The Penalty: On March 20, 2023, Bukey was sentenced in the U.S. District Court for the District of Columbia to 28 months in prison and a $100 special assessment.

Mehdi Hashemi

The Violation: From at least 2015 to 2018, Mehdi Hashemi, a dual citizen of Iran and the United States, and Feroz Khan, a citizen of India and resident in the United Arab Emirates, conspired to unlawfully export used Computer Numerical Control (CNC) machines classified under ECCN 2B201, 2B991, and EAR99, some of which are controlled for nuclear non-proliferation, to Iran via the United Arab Emirates. Hashemi purchased the CNC machines and related equipment from suppliers in the U.S. and Canada, made arrangements to ship the machines to the UAE under false and forged invoices and packing lists, and then arranged with Khan to forward the machines from the UAE to Iran. Hashemi purchased the machines on behalf of a Tehran-based company that claimed to manufacture textiles, medical and automotive components, and spare parts. In December 2019, Hashemi pled guilty in the U.S. District Court for the

Central District of California in connection with the illegal exports. Khan remains a fugitive. This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office, HSI, and CBP.

The Penalty: On July 1, 2020, Mehdi Hashemi was to 12 months and one day in prison, and three years of supervised release. On September 30, 2022, BIS issued Hashemi a post-conviction denial order for a period of 10 years.

Matteo Taerri

The Violation: In January 2016, OEE's Atlanta Resident Office began a joint investigation with the FBI involving the illegal export of biological vectors and medical filters classified under ECCN 2B352 to Iran. Taerri was providing the biological material and filters to his nephew, who was a PhD student at Tehran University Research Center and claimed to need the commodities for research on HPV and herpes vaccines. The commodities were hand-carried to Iran by Taerri. Taerri was arrested in November 2018 and pled guilty in December 2019. This case resulted from an investigation conducted by OEE's Atlanta Resident Office and the FBI.

The Penalty: On June 4, 2020, Taerri was sentenced to time served (16 months), three years supervised release, a $200 special assessment, and a $227,334 forfeiture. On August 10, 2021, a 10-year Denial Order was issued against Taerri.

Beng Sun Koh / Anh Minh Cuong Co Ltd.

The Violation: On November 1, 2019, Beng Sun Koh, also known as Michael Koh, pled guilty in the U.S. District Court for the District of Columbia in connection with the illegal transshipment of U.S.-origin commodities to Iran via Singapore. Koh, Owner and Director of Anh Minh Cuong Co. Ltd. in Singapore, was directed to use his company to acquire U.S.-origin as chromatograph mass spectrometers and electron capture detectors classified under ECCN 3A999 on behalf of an Iranian national and his Tehran, Iran based company. Koh purchased the requested items from a U.S. company through a distributor located in Singapore. Koh then conspired with the Iranian to transship the goods from Singapore, through a freight forwarder in the United Arab Emirates to Iran without valid OFAC or BIS export license authorization. On January 2, 2019, Koh arrived in the United States for vacation and was taken into custody at the JFK International Airport in Queens, New York, by OEE, HSI, and DCIS Special Agents the same day. Koh was transferred from New York to Washington DC for prosecution. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, HSI, and DCIS.

The Penalty: On January 24, 2020, Koh was sentenced to 18 months in prison, supervised release for 12 months, a $23,025 forfeiture, a $34,000 fine, and a $100 special assessment, followed by deportation.

Erdal Akova / Esa Kimya

The Violation: On March 8, 2017, Turkish national Erdal Akova pled guilty in U.S. District Court for the Northern District of Georgia in connection with a conspiracy to export military grade epoxy to Iran for final use by the Iran Aircraft Manufacturing Industrial Company (HESA). The U.S. Department of the Treasury designated HESA as an entity with roles in Iran's nuclear and ballistic missile programs and because it has provided support to the Iranian Revolutionary Guard Corps. Akova knowingly allowed his name and his company's name to be used to purchase epoxy destined for Iran. He also allowed his company in Turkey, Esa Kimya, to be used as the transshipment location for the epoxy ultimately destined for delivery to Iran. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, HSI, and the FBI.

The Penalty: On March 8, 2017, Akova was sentenced to 36 months in prison and a $200 special assessment.

Sihai Cheng

The Violation: In 2013, Chinese national Sihai Cheng was charged in an indictment along with Seyed Abolfazl Shahab Jamili, an Iranian national, and two Iranian companies, Nicaro Eng. Co., Ltd. and Eyvaz Technic Manufacturing Company, with conspiring to export, and exporting, highly sensitive U.S.-manufactured goods with nuclear applications to Iran from at least 2009 to 2012. In December 2014, Cheng was extradited from the United Kingdom to the United States and has remained in custody since then. On December 18, 2015, Cheng pled guilty to conspiracy to commit export violations and smuggle goods from the United States to Iran and to illegally exporting

U.S.-manufactured pressure transducers to Iran. From February 2009 through at least 2012, Cheng, Jamili, and a third individual conspired with each other and others in China and Iran to illegally obtain hundreds of U.S.-manufactured pressure transducers and export them to Iran. Initially, the parts were exported to China using fraudulently obtained BIS export licenses. When they arrived in the China, Cheng inspected them in the Shanghai Free Trade Zone and removed their U.S. manufacturer serial numbers to conceal the fact that he was violating U.S. law. Cheng then caused the pressure transducers to be exported to Iran knowing that the parts were being supplied to the Government of Iran. Jamili advised Cheng that the Iranian end- user was Kalaye Electronic Company, which the U.S. Government designated as a proliferator of weapons of mass destruction in 2007 for its work with Iran's nuclear centrifuge program. Pressure transducers can be used in gas centrifuges to enrich uranium and produce weapons -grade uranium. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, and HSI.

The Penalty: On January 27, 2016, Cheng was sentenced in the U.S. District Court for the District of Massachusetts to nine years in prison and a $600 special assessment in connection with the export of the pressure transducers to Iran.

Qiang (Johnson) Hu / MKS Shanghai

The Violation: This investigation was initiated after photographs surfaced of the former President of Iran, Mahmoud Ahmadinejad, touring the Natanz Uranium Enrichment facility in Iran which revealed the presence of what appeared to be pressure transducers manufactured by MKS Instruments in Andover, MA. From 2008 through his arrest in 2012, Qiang (Johnson) Hu, a sales manager at MKS Shanghai, conspired with co-workers and others to illegally supply thousands of export-controlled pressure transducers, worth more than $6.5 million, to unauthorized end users in China, Iran and elsewhere using export licenses fraudulently obtained from the Department of Commerce. The pressure transducers are classified under ECCN 2B230 and are controlled for nuclear nonproliferation reasons. Hu was arrested in May 2012 and in October 2013 he pled guilty to conspiracy to violate the IEEPA. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, and HSI.

The Penalty: On July 21, 2014, Hu was sentenced in the U.S. District Court for the District of Massachusetts to 34 months in prison and $100 special assessment. On February 3, 2016, BIS issued an order denying Hu's export privileges for ten years (until July 24, 2024).

Other Controls

Rik Wimp

The Violation: This case involved efforts by a Turkish Company to obtain surface drives, also known as specialized propulsion systems holdings, classified under ECCN 8A992, that were believed to be destined for Iran. In August 2021, Rik Wimp pled guilty to knowingly and willfully making materially false, fictitious, and fraudulent representations to Special Agents related to the transaction. Wimp represented that he had not received money from a foreign company under investigation for violations of U.S. export control laws, when Wimp had received over $156,000 from the company.

The Penalty: On August 18, 2022, Wimp was sentenced in the U.S. District Court for the Central District of California to one year of probation and a $156,600 criminal fine, and a $100 special assessment. This case resulted from a joint investigation conducted by OEE's Chicago Field Office and the FBI.

Arash Yousefi Jam / Amin Yousefi Jam

The Violation: Brothers Arash Yousefi Jam and Amin Yousefi Jam both pled guilty in the U.S. District Court for the Eastern District of Michigan in connection with a conspiracy to unlawfully export U.S.-origin goods to Iran in violation of the ITSR. According to the indictment, beginning in or around January 2015, and continuing through February 2017, Arash and Amin received instructions from a co-conspirator located in Iran to acquire U.S- origin goods. Arash and

Amin placed orders for electrical discharge boards, CPU boards, servo motors, and railroad crankshafts, which are all designated EAR99, from U.S. companies and caused them to be shipped through the UAE to Iran. To conceal the true location and nature of the end users, Arash and Amin utilized fictitious companies located in Canada and the UAE when purchasing and shipping the goods from the United States. This case resulted from a joint investigation conducted by OEE's Chicago Field Office and HSI.

The Penalty: On October 14, 2021, Arash Yousefi Jam was sentenced to 10 months in prison. On November 17, 2021, Amin Yousefi Jam was also sentenced to 10 months in prison. Additionally, both were denied export privileges for a period of seven years.

Sadr Emad-Vaez / Pouran Aazad / Hassan Ali Moshir-Fatemi

The Violation: In April 2013, a shipment containing a drill press designated EAR99 was intercepted prior to its attempted export from the United States, facilitated by Ghareh Sabz Co. (GHS) in Iran via concealment through a third party in the United Arab Emirates. Subsequent investigation determined that GHS was operated by three naturalized U.S. citizens, Sadr Emad-Vaez, Pouran Aazad, and Hassan Ali Moshir-Fatemi, who divided their time between Iran and the United States. The individuals were found to be engaged in an unlawful procurement scheme for GHS that involved, in addition to the attempted acquisition of the drill press, the unauthorized export of sensors designated EAR99 and the unauthorized (due to the individuals' U.S. citizenship) procurement of numerous industrial commodities from international suppliers. The scheme also involved financial misconduct, such as the use of financial institutions sanctioned by the U.S. Department of the Treasury. In May 2019, all three defendants pled guilty in the U.S. District Court for the Northern District of California. This case resulted from a joint investigation conducted by OEE's San Jose Field Office, HSI, IRS-CID, and the FBI.

The Penalty: The case resolved via global settlement. On January 28, 2021, Sadr Emad-Vaez, was sentenced to 14 months in prison, a $500,000 criminal fine, and a $100 special assessment. Pouran Aazad was sentenced to three years of probation, a $200,000 criminal fine, and a $100 special assessment. Hassan Ali Moshir-Fatemi was sentenced to one year plus one day of prison, a $50,000 criminal fine, and a $100 special assessment. On July 8, 2019, BIS issued a joint $300,000 administrative penalty and ten-year denial order against Emad-Vaez, Aazad, and GHS. On July 8, 2022, BIS issued a ten-year denial order against Moshir-Fatemi.

SAP SE

The Violation: SAP SE is a German multinational software corporation based in Waldorf, Baden-Wurttenburg, Germany. It develops enterprise software to manage business operations and customer relations among other things. In 2018, SAP filed a voluntary self-disclosure with the Department of Justice, Department of Commerce and OFAC regarding violations of US sanctions. The multi-year investigation that followed revealed that, during a period including December 2009 through September 2019, SAP engaged in conduct prohibited by the EAR when it exported SAP products. including software, upgrades and patches. From the United States to various end users located in sanctioned countries, including Iran, without the required export licenses. This case resulted from an investigation conducted by OEE's Boston Field Office and OFAC.

The Penalty: In April 2021, SAP entered into a non-prosecution agreement with DOJ, and agreed to a global settlement with DOJ, DOC and OFAC. As part of the agreement, SAP agreed to pay combined penalties of more than $8 million as part of a global resolution with the U.S. Departments of Justice (DOJ), Commerce and Treasury. Included in the settlement was a payment of $3.29 million to the Department of Commerce and an agreement to conduct three audits of its export compliance program over a three-year period. In voluntary disclosures the company made to the three agencies, SAP acknowledged violations of the EAR and the ITSR. As a result of its voluntary disclosure, in addition to the penalties, SAP spent more than $27 million to bring its company's exporting into compliance.

ETCO / Mahin Mojtahedzadeh / Mojtaba Biria / Olaf Tepper

The Violation: Mahin Mojtahedzadeh was the President and Managing Director of ETCO-FZC, an export company with an office in the UAE. ETCO is a supplier of spare and replacement turbine parts for power generation companies in the Middle East, including Iran. Between 2013 and 2017, Mojtahedzadeh worked with Olaf Tepper, the founder and

Managing Director of Energy Republic GmbH based in Germany, and Mojtaba Biria, Technical Managing Director at Energy Republic, also based in Germany, to violate and evade U.S. sanctions against Iran. Mojtahedzadeh instructed a company in Canada and Energy Republic to acquire more than $3 million turbine parts designated EAR99 from U.S. distributors. When the U.S. parts arrived in Canada and Germany, respectively, these companies and Mojtahedzadeh arranged for the parts to be re-exported to ETCO's customers in Iran. Mojtahedzadeh, Biria, and Tepper all pled guilty in the U.S. District Court for the Northern District of New York in connection with these violations. This case resulted from a joint investigation conducted by OEE's New York Field Office, the FBI, and HSI.

The Penalty: On January 30, 2020**,** Mahin Mojtahedzadeh was sentenced to time served and a $5,000 criminal fine. On August 14, 2018, Mojtaba Biria was sentenced to time served and a $5,000 criminal fine. On August 3, 2018, Olaf Tepper was sentenced to 24 months in prison and a $5,000 criminal fine. On June 8, 2019, BIS issued a ten-year denial order against Tepper. On November 7, 2019, BIS issued a ten-year denial order against Biria. On July 1, 2020, BIS issued a ten-year denial order against Mojtahedzadeh.

Behrooz "Bruce" Behroozian

The Violation: U.S./Iranian citizen Behrooz "Bruce" Behroozian and his co-conspirators illegally diverted millions of dollars' worth of industrial parts designated EAR99 and classified under 2B999 to Iran's oil and petrochemical industry, all in violation of the ITSR and the IEEPA. Behroozian was the owner and operator of a computer parts supplier in Dublin, Ohio called Comtech International. Comtech had no storefront and made no domestic sales and it primarily exported industrial equipment to co-conspirators in the United Arab Emirates for diversion to Iran. Behroozian and his co-conspirators used a Hawala money remittance system in order to try and avoid sanctions placed on the Iranian financial sector and to obfuscate law enforcement. In 2016, Behroozian pled guilty to an IEEPA violation. This case resulted from a join investigation conducted by OEE's Washington Field Office and the FBI.

The Penalty: On October 24, 2019, Behroozian was sentenced in U.S. District Court for the Southern District of Ohio to 20 months in prison, 24 months of supervised release, a $100 special assessment, $79,000 monetary forfeiture, and forfeiture of gas turbine parts valued at $101,300.

IC Link Industries Ltd / Mohammad Khazrai Shaneivar / Arezoo Hashemnejad Alamdari

The Violation: Mohammad Khazrai Shaneivar, an Iranian national and owner of the Iranian Company, Sensor Co., immigrated to Canada and founded the company IC Link Industries Ltd. The name IC Link is an abbreviation of Iran – Canada Link, and the company's sole objective was to procure U.S. and North American manufactured industrial goods designated as EAR99 which were used in the oil, gas, petrochemical and steel industries. Shaneivar created IC Link to avoid scrutiny from U.S. suppliers, and to aid in the conspiracy to illegally export U.S.-origin items to Iran. The scheme to evade the sanctions generally worked as such: Arezoo Hashemnejad Alamdari, an Iranian national and Sensor employee located in Iran, would receive requests to obtain parts on behalf of Iranian end-users such as the National Iranian Oil Company (NIOC) and other entities controlled by the government of Iran. Sensor would forward these requests to Shaneivar and IC Link. The request for quote (RFQ) was then sent to Michael Sheehan, operating as Real-Time Industrial Solutions located in Lakewood, Ohio. Sheehan would contact U.S. companies, negotiate pricing, and then procure the goods on behalf of IC Link. In order to obscure the end users being located in Iran, IC link engaged in business relationship with Parisa Mohamadi,(AKA Parisa Javidi), a dual U.S. and Iranian citizen, residing in Dubai, United Arab Emirates (UAE). Mohamadi, using her UAE-registered company Intelligent Solutions, arranged for the items to be exported to her and/or freight forwarding companies in Dubai. Mohamadi then arranged with Alamdari of Sensor to move the goods to Iran. In an attempt to obfuscate export enforcement, IC Link and Mohamadi would direct Sheehan to de-value the items and remove labels and markings that identified the manufacturer of that the items were of U.S.-origin. From 2009 to 2016, this network was responsible for procuring and illegally exporting millions of dollars' worth of goods from the U.S. to Iran. In 2017, IC Link, Shaneivar, Mohamadi, and Alamdari were indicted in the Northern District of Ohio for multiple counts of violating the IEEPA and conspiracy to do the same. In 2018, Sheehan was charged with submission of false or misleading information to the Automated Export System (AES) and providing false information to an OEE Special Agent. This case resulted from a joint investigation conducted by OEE's Washington Field and HSI.

The Penalty: In November 2018, Sheehan was sentenced to 24 months of probation, a $500 criminal fine, and a $200 special assessment. In September 2019, Mohamadi was sentenced to 24 months in prison, 24 months of supervised release, and a $200 special assessment. In October 2020, Shaneivar was sentenced to a $100,000 criminal fine and the forfeiture of three commercial properties appraised at over $2,000,000. IC Link was sentenced to a $200,000 criminal fine, and Alamdari was sentenced to a $5,000 criminal fine. On March 6, 2023, BIS issued Mohamadi and Shaneivar post-conviction denial orders for a period of 10 years.

OEE Special Agents training at an outdoor firing range

Schlumberger Oilfield Holdings Ltd.

The Violation: Starting in about 2004 and continuing through June 2010, Drilling & Measurements (D&M), a United States-based Schlumberger business segment, provided oilfield services to Schlumberger customers in Iran and Sudan through their non-U.S. subsidiary Schlumberger Oilfield Holdings Ltd. (SOHL), incorporated in the British Virgin Islands. Although SOHL and the parent company Schlumberger Limited had policies and procedures designed to ensure that D&M did not violate U.S. sanctions, both companies failed to train their employees adequately to ensure that all U.S. persons, including non-U.S. citizens who resided in the United States while employed at D&M, complied with Schlumberger Ltd.'s sanctions policies and compliance procedures. As a result of D&M's lack of adherence to U.S. sanctions combined with SOHL's failure to properly train U.S. persons and to enforce fully its policies and procedures, D&M, through the acts of employees residing in the United States, violated U.S. sanctions against Iran and Sudan by: (1) approving and disguising the company's capital expenditure requests from Iran and Sudan for the manufacture of new oilfield drilling tools and for the spending of money for certain company purchases; (2) making and implementing business decisions specifically concerning Iran and Sudan; and (3) providing certain technical services and expertise in order to troubleshoot mechanical failures and to sustain expensive drilling tools and related equipment in Iran and Sudan. This case resulted from an investigation conducted by OEE's Dallas Field Office.

The Penalty: In May 2015, Schlumberger Oilfield Holdings Ltd. entered a plea of guilty in the U.S. District Court for the District of Columbia and agreed to pay over $232.7 million, the largest criminal fine ever imposed for violations of sanctions programs administered under the IEEPA. Parent company Schlumberger Ltd. also agreed to the following additional terms during the three-year term of probation maintaining its cessation of all operations in Iran and Sudan, (2) reporting on the parent company's compliance with sanctions regulations, (3) responding to requests to disclose information and materials related to the parent company's compliance with U.S. sanctions laws when requested by U.S. authorities, and (4) hiring an independent consultant to review the parent company's internal sanctions policies and procedures and the parent company's internal audits focused on sanctions compliance.

On June 21, 2016, the OEE Special Agent responsible for this investigation was recognized at the United States Attorney's Office, District of Columbia's Thirty-Fourth Law Enforcement Awards Ceremony for his outstanding work on the Schlumberger Oilfield Holdings Ltd. case.

Chapter 4 – Rest of the World

Criminal and Administrative Case Examples

National Security Controls

Robert Alcantara

The Violation: From approximately 2017 until 2022, Robert Alcantara operated a "ghost gun" factory out of his home in Rhode Island. Alcantara purchased ghost gun kits and machined them into working firearms that he exported to the Dominican Republic. Alcantara and others then laundered the proceeds of his gun sales. On November 20, 2021, Alcantara was stopped in his vehicle in possession of kits to build approximately 45 ghost guns. Ghost gun kits include all of the necessary component parts to turn the unfinished frame or receiver into a fully functioning gun, which once assembled looks, feels, and functions like a traditional gun, whether a handgun or assault weapon, and is just as deadly and dangerous in the wrong hands. Alcantara was interviewed by law enforcement agents and stated that he was planning to turn the 45 kits into working firearms and that he had 50 additional similar ghost guns at his home. This case resulted from a joint investigation conducted by OEE's New York Field Office and ATF.

The Penalty: On December 21, 2023, Alcantara was sentenced in the U.S. District Court for the Southern District of New York to 68 months in prison, 36 months of supervised release, a $127,622 forfeiture, and a $200 special assessment.

Rafael Richiez

The Violation: On November 29, 2022, three firearms classified under ECCN 0A501 were seized at the Port of Haina in the Dominican Republic (DR). The firearms had been purchased by Rafael Richiez of Lawrenceville, Georgia and were addressed to Richiez's mother, a resident of DR. DR law enforcement conducted a controlled delivery and arrested Richiez's mother, who ultimately spent 35 days in jail. The shipping container manifest listed 'household goods'. The inspection conducted by Special Agents discovered firearms concealed inside of cylindrical containers of powdered iced tea. The firearms were not declared, nor had export license authorization been obtained. OEE, HSI and ATF Special Agents conducted a search warrant of Richiez's residence in December 2022 and seized multiple firearms. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, ATF and HSI.

The Penalty: On September 14, 2023, Richiez was sentenced in the U.S. District Court for the Northern District of Georgia to 20 months in prison, two years of supervised release, 200 hours of community service, and a $100 special assessment.

Eric Ampong-Coker

The Violation: Eric Ampong-Coker pled guilty in June 2023 in connection with the illegal export of firearms and magazines from the Port of Baltimore to Ghana. Ampong-Coker purchased at least 81 firearms from separate Maryland Federal Firearms Licensees (FFLs) and in 2018 received Regulated Firearms Collector status through the Maryland State Police, which waived the restriction on the number of firearms Ampong-Coker could purchase during a 30-day period. Special Agents surveilled the defendant retrieving firearms purchased and was observed at a business that packed and shipped items from the Port of Baltimore. A shipping vehicle was seen departing the business location. Ampong-Coker was searched before he was scheduled to depart the United States from Detroit, Michigan bound for Ghana. Special Agents seized foam cutouts used for packing and securing firearms in gun cases from his luggage. The container, scheduled to depart the Port of Baltimore for Tema, Ghana, was identified along with the vehicle used to store the firearms. Upon searching the vehicle, the firearms were found in the trunk inside of a suitcase. Ampong-Coker admitted that he had not obtained the required license or written approval to export the firearms or magazines to Ghana. This case resulted from a joint investigation conducted by OEE's Washington Field Office, ATF, HSI, and DCIS.

The Penalty: On September 11, 2023, Ampong-Coker was sentenced in the U.S. District Court for the District of Maryland to 30 months in prison, two years of supervised release, and a $100 special assessment.

Suhaib Allababidi / 2M Solutions, Inc.

The Violation: Suhaib Allababidi and his company 2M Solutions, Inc. (2M) of Grand Prairie, Texas pled guilty in November 2022 to defrauding the U.S. Government of approximately $3 million by selling Chinese cameras for use in sensitive U.S. structures. According to court documents, Allababidi, the owner and president of 2M, admitted that the company – which provided security cameras, solar-powered light towers, digital video recorders, and other electronics to various U.S. government agencies – claimed that its products were manufactured in the United States, when in actuality they were manufactured in China by Chinese companies. In order to secure contracts with U.S. government agencies, including the Departments of Defense, Justice, and Homeland Security, Allababidi represented that 2M was "a USA Manufacturing Company." 2M also pled guilty to submitting false information in relation to products exported to foreign customers. In contravention of export laws, the company falsified the description of items exported, misrepresented the ultimate recipient of the items, and falsely stated that no export license was needed for shipments that required a license. This case resulted from a joint investigation conducted by OEE's Dallas Field Office, DCIS, HSI, the FBI, General Services Administration's Office of the Inspector General, and the U.S. Department of Justice's Office of the Inspector General.

The Penalty: On May 5, 2023, Suhaib Allababidi was sentenced to 48 months in prison, three years of supervised release, joint restitution with 2M Solutions, Inc. in the amount of $1,154,634, and a $100 special assessment. 2M Solutions, Inc. was sentenced to five years of probation, a $1,000,000 criminal fine, the joint restitution, and a $800 special assessment.

Jorge Chica-Giler / Rolando Alexei Pupo-Abrahantes / Nicolas Ayala

The Violation: This investigation involved the smuggling of firearms from the United States to Ecuador. Jorge Chica-Giler directed co-conspirators to purchase firearms classified under ECCN 0A501, hide the firearms inside compressed air tanks, and send them to a co-conspirator in Ecuador. Chica-Giler admitted to making eight shipments totaling at least 35 firearms, including several assault rifles. He further admitted to dealing firearms without a license, smuggling firearms from the United States, delivery of a firearm to a common carrier without written notification, and possession of a firearm by an unlawful alien. Rolando Alexei Pupo-Abrahantes and Nicolas Ayala assisted Chica-Giler in the conspiracy. This case resulted from an investigation conducted by OEE's Atlanta Resident Office, ATF, and HSI.

The Penalty: On November 18, 2022, Chica-Giler was sentenced to 262 months in prison, one year of supervised release, and a $500 special assessment. On November 17, 2022, Pupo-Abrahantes was sentenced to 30 months in prison, two years of supervised release, and a $300 special assessment. On November 17, 2023, Ayala was sentenced to 36 months in prison, three years of supervised release, and a $400 special assessment.

Virgil Griffith

The Violation: On September 27, 2021, Virgil Griffith pled guilty to conspiring to provide services to the Democratic People's Republic of North Korea (DPRK), including technical advice on using cryptocurrency and block chain technology to evade sanctions. Griffith exported a gaming system classified under ECCN 4A994 to the DPRK to help with the cryptocurrency scheme. Griffith began formulating plans as early as 2018 to provide services to individuals in the DPRK by developing and funding cryptocurrency infrastructure there, including to mine cryptocurrency. Griffith knew that the DPRK could use these services to evade and avoid U.S. sanctions, and to fund its nuclear weapons program and other illicit activities. This case resulted from a joint investigation conducted by OEE's New York Field Office, DSS, and the FBI.

The Penalty: On April 12, 2022, Griffith was sentenced in the U.S. District Court for the Southern District of New York to 63 months in prison, three years of supervised release, a $100,000 criminal fine and a $100 special assessment. On May 8, 2023, BIS issued Griffith a post-conviction denial order for a period of 10 years.

Jorge Orencel

The Violation: On December 17, 2021, Jorge Orencel pled guilty to attempting to smuggle goods out of the United States without the required export license. Orencel owned and operated Sumtech, which advertised itself as specializing in the distribution of American merchandise, including "high technology laboratory devices," to South America, Asia, and the

Middle East. Orencel procured five ionization chambers and one fission chamber from a U.S. company for sale to a company in Hong Kong. Orencel provided the U.S. company with an end user statement falsely indicating that the end user and ultimate destination were Argentina. Orencel shipped the ionization chambers to Hong Kong and obtained the fission chamber from the U.S. company. In order to obtain the fission chamber, Orencel falsified the value and destination of the item so as avoid filing a Shipper's Export Declaration with the U.S. government. The fission chamber was detained in New York prior to leaving the country. When questioned, Orencel admitted that he intended to ship the fission chamber to Hong Kong. This case resulted from an investigation conducted by OEE's New York Field Office.

The Penalty: On February 22, 2022, Orencel was sentenced in the U.S. District Court for the District of Maryland to six months in prison, a $5,000 criminal fine, one year of supervised release, and a $100 special assessment.

Nihad Al Jaberi / Ashraf Taha / Mahmood Al Tayyar

The Violation: In August 2020, OEE Special Agents and CBP Officers targeted a shipment suspected of containing firearms or firearm-related parts classified being exported by Nihad Al Jaberi, a former Iraqi refugee and current U.S. resident, from the Port of Savannah to Iraq. Upon inspection, the shipment, listed as auto parts, was found to contain three handguns, magazines, and six sniper type rifles. The firearms, now classified under ECCN 0A501, were seized. ATF then joined the investigation, which revealed the firearms were purchased in the Atlanta area by co-defendants Ashraf Taha and Mahmood Al Tayyar. Al Jaberi was arrested in Atlanta, Georgia in February 2021 based on an arrest warrant issued in the U.S. District Court for the Southern District of Georgia. Al Jaberi was found guilty in February 2022 following a criminal trial. Ashraf Taha pled guilty in March 2021. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, HSI, ATF and CBP.

The Penalty: On August 11, 2022, Al Jaberi was sentenced to 94 in months in prison and a $300 special assessment. Taha was sentenced to two years of probation and a $100 special assessment. Al Tayyar received pre-trial diversion.

Charlton Ameyaw

The Violation: In 2010, Charlton Aboagye Ameyaw of Middletown, Delaware purchased two firearms now classified under ECCN 0A501 and exported them to Ghana by concealing them in a vehicle that was shipped to Ghana. In March 2020, Ameyaw exported six more firearms to Ghana by placing them in a plastic barrel, hiding the firearms within clothes, candy, and shoes. That barrel was listed as containing household items and was shipped by a freight forwarder to Ghana. In September 2020, he purchased 20 more firearms with the intent of exporting the firearms to Ghana but was arrested before he was able to export them. Ameyaw did not obtain the appropriate export license authorization for any of the firearms and did not notify the freight forwarder/carrier of the firearms content. On February 1, 2022, Ameyaw pled guilty to the charges in U.S. District Court for the District Delaware. This case resulted from a joint investigation conducted by OEE's Washington Field Office, HSI, and ATF.

The Penalty: On June 3, 2022, Ameyaw was sentenced to 18 months in prison, 24 months of supervised release, $100 special assessment, and forfeiture of the 20 firearms.

Rashad Sargeant / David Johnson / Shunquez Stephens

The Violation: David Johnson, Rashad Sargeant, and Shunquez Stephens were involved in the shipping of firearms classified under ECCN 0A501 to Barbados after obliterating the serial number from the firearms and packing them inside false compartments in boxes. Johnson recruited Stephens and others to unlawfully purchase guns from federally licensed firearms dealers. Stephens and the other "straw purchasers" made false statements to the licensed dealers by swearing that they were purchasing guns for themselves. Sargeant and Johnson would then take possession of the guns and use false identifications to mail them to Barbados through common carriers like UPS, FedEx and DHL. All three defendants pled guilty in the U.S. District Court for the Northern District of Georgia. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, HSI and ATF.

The Penalty: On June 2, 2022, Sargeant was sentenced to 46 months in prison, three years of supervised release, and a $400 special assessment. On March 17, 2022, Johnson was sentenced to 46 months in prison, three years of supervised

release, and a $400 special assessment. On September 30, 2021, Stephens was sentenced to three years of probation and a $100 special assessment.

Jahziah Lewis / Clairvorn Kelly / Deja Bess

The Violation: In or about April 2020, OEE began a joint investigation with ATF and HSI that involved the illegal export of firearms and narcotics from the United States to the United Kingdom and island nations in the Caribbean such as Saint Kitts and Nevis and Saint Maarten. The investigation began as a request for assistance from the UK's National Crime Agency (NCA). UK authorities conducting undercover operations interdicted firearms now classified under ECCN 0A501 that were shipped from Atlanta, Georgia to the UK through the U.S. Postal Service, and learned the firearms were destined for crime groups in the UK. One firearm exported from the United States was used in a murder in the UK. Eight firearms and 350 rounds of ammunition were seized in the UK, and all of the weapons seized were destined to be sold to the criminal market. The investigation further revealed Jahziah Lewis, a Saint Kitts citizen living in the Bronx, New York, coordinated and supplied funds for the purchase and distribution/illegal export of weapons and narcotics from the United States. The weapons and narcotics were concealed in blue tooth speakers and stools. Co-conspirators Clairvorn Kelly and Deja Bess, both Saint Kitts citizens living in the Atlanta, Georgia area, used several aliases to purchase and export weapons and narcotics. All three defendants pled guilty in the U.S. District Court for the Northern District of Georgia. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, HSI and ATF.

The Penalty: On March 15, 2022, Kelly was sentenced to 51 months in prison, three years of probation, and a $500 special assessment. On November 15, 2021, Bess was sentenced to three years of probation and 80 hours of community service after she cooperated with the government. On September 15, 2021, Lewis was sentenced to 57 months in prison and a $400 special assessment.

Add Helium / Peter Sotis / Emily Voissem

The Violation: On October 21, 2021, Peter Sotis and Emily Voissem were found guilty by a jury in the U.S. District Court for the Southern District of Florida. Sotis and Voissem were indicted in October 2019 related to smuggling and conspiracy to violate and attempted violation of the IEEPA and the EAR. Sotis was an 80% owner and principal of Add Helium, a dive shop located in Fort Lauderdale, Florida and Voissem was the office manager. Sotis and Voissem, through Add Helium, transferred four rebreathers classified under ECCN 8A002 and controlled for National Security and Anti-Terrorism reasons to a shipping company for export to Libya. This occurred after they had been informed by an OEE Special Agent that the items could not be exported while a license determination was pending. A rebreather is an apparatus that absorbs the carbon dioxide of a scuba diver's exhaled breath to permit the rebreathing (recycling) of each breath. This technology produces no bubbles, thereby concealing the diver's activities from those on the surface, and also allows a diver to stay underwater longer compared to normal diving equipment. Sotis and Voissem allowed the shipment of rebreathers to occur without an export license. This case resulted from a joint investigation conducted by OEE's Miami Field Office, the FBI, HSI, and CBP.

The Penalty: On January 12, 2022, Sotis was sentenced to 57 months in prison, and Voissem was sentenced to five months in prison. Both defendants were sentenced to three years of supervised release and a $300 special assessment. The rebreathers were also forfeited. BIS issued Sotis a post-conviction denial order for a period of 10 years; Voissem was also subjected to a separate post-conviction denial order for a period of seven years.

Berrick Ciceron

The Violation: In February 2020, using a false identification, Berrick Ciceron of Dacula, Georgia, attempted to export to Haiti an item described as a toaster. An X-ray of the package showed that the package contained three firearms. The ensuing investigation revealed that Ciceron exported approximately 50 firearms classified under ECCN 0A501 to Haiti. Special Agents also seized six pistols over the course of the investigation that were in transit to Haiti. Ciceron was arrested in March 2021 and pled guilty in August 2021. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, HSI, and ATF.

The Penalty: On December 17, 2021, Ciceron was sentenced to 18 months in prison, three years of supervised release, and a $100 special assessment.

VTA Telecom Corporation / Huy Bui

The Violation: In June 2016, Vietnamese citizen Huy Bui and VTA Telecom Corporation (VTA) in Milpitas, California were identified as being involved in a missile procurement network in support of customers in Vietnam attempting to develop a missile similar to the AGM-84 (Harpoon) missile. Bui, CEO of VTA, made payments to Undercover Agents (UCAs to procure a turbo jet engine controlled under the ITAR for use in the missile and asked UCAs to procure Harpoon spare parts. In or around 2015, VTA began procuring and exporting items to its parent company in Vietnam, even though it was aware that some of the exports were intended to support a defense program. The company on several occasions provided false information to BIS and other U.S. Government agencies in connection with export license applications and other export activity related to the export of power amplifiers/transistors classified under ECCN 3A001, actuators classified under ECCN 9A610, and a mass properties instrument and related equipment classified under ECCN 9B604. Bui was arrested in October 2016 and pled guilty in the U.S. District Court for the District of New Mexico in June 2017. This case resulted from a joint investigation conducted by OEE's Phoenix Field Office, the FBI, and HSI.

The Penalty: On October 12, 2021, VTA Telecom Corporation agreed to pay a $1,866,372 civil penalty with $200,000 suspended, provided no violations occur during a two-year probationary period, and to expend an additional $25,000 on compliance efforts. On September 19, 2017, Bui was sentenced to 12 months and one day in prison, and deportation upon completion of his sentence.

Shamoi Whyte / Kymani Cline

The Violation: Shamoi Whyte, Kymani Cline, and others were investigated related to the straw purchase and illegal export of firearms, ammunition, and accessories now classified under ECCNs 0A501 and 0A505 to the U.S. Virgin Islands (USVI). The items were believed to be ultimately destined for various Caribbean Islands. One firearm that Whyte purchased in Atlanta was recovered in the British Virgin Islands by local authorities. Additionally, Whyte was involved in a running street gun battle in the USVI in June 2020, during which over 100 rounds were fired. OEE Special Agents seized nine firearms discovered in Cline's checked baggage while traveling from Atlanta to the USVI and identified approximately 41 guns purchased in this conspiracy. Whyte was arrested in November 2020 at his residence in Atlanta, Georgia, during which Special Agents recovered narcotics and firearms. Cline was also arrested in November 2020 at the Atlanta International Airport as he boarded a flight to the USVI. During Cline's arrest, Special Agents conducted an inspection of his carry-on baggage and discovered approximately four kilos of marijuana. Cline's arrest also led to the identification of three other individuals who were hand-carrying approximately 20 kilos of marijuana, who were also arrested upon arrival in the USVI from Atlanta. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office and ATF.

The Penalty: On August 31, 2021, Whyte was sentenced to 18 months in prison, two years of supervised release, and a $400 special assessment. On the same date, Cline was sentenced to 24 months in prison, two years of supervised release, and a $300 special assessment.

Ali Abdulkareem

The Violation: On March 16, 2021, Phoenix, Arizona resident Ali Abdulkareem pled guilty in the U.S. District Court for the District of Arizona to charges related to his involvement in the purchase and export of gun parts now classified under ECCN 0A501to Iraq. Abdulkareem mixed the gun parts with other items and labeled the export as "headset/beauty supply/argan oil." Special Agents discovered Abdulkareem had previous exports to Iraq and had a cousin that worked at a U.S. shipping company in Iraq. Abdulkareem would address the packages to Jack or John Robert as an employee at the U.S. Embassy. Checks with Embassy officials confirmed that there was no Jack or John Roberts at the Embassy. It is believed that Abdulkareem and his cousin conspired to ship these items to a fictitious Embassy employee, as these items did not receive as much scrutiny as other packages, and it would be easy for Abdulkareem's cousin to intercept any packages as an employee of the U.S. shipping company. A search warrant executed at Abdulkareems's residence uncovered several gun parts and paraphernalia that were going to be exported to Iraq. This case resulted from a joint investigation conducted by OEE's Phoenix Field Office, the FBI and HSI.

The Penalty: On August 26, 2021, Abdulkareem was sentenced to six months in prison and three years of probation.

Luis Alberto Patino Linares / Gregori Jerson Mendez Palacios

The Violation: On April 6, 2021, Venezuelan nationals Luis Alberto Patino Linares and Gregori Jerson Mendez Palacios pled guilty in the U.S. District Court for the Southern District of Florida to charges related to their involvement in the procurement and smuggling of U.S.-origin items, including firearms and shotguns of various makes and calibers now classified under ECCNs 0A501 and 0A502, to Venezuela, and being aliens in possessions of firearms. Both attempted to depart the United States from the Fort Lauderdale-Hollywood International Airport aboard a jet. Mendez Palacios was the pilot of the jet and Patino Linares was the co-pilot. Upon search of the jet, law enforcement located approximately $20,000 of undeclared U.S. currency. The goods were purchased from private internet sales and from retail locations throughout the South Florida area. This case resulted from a joint investigation conducted by OEE's Miami Field Office, CBP, and HSI.

The Penalty: On June 30, 2021, Patino Linares was sentenced to 70 months in prison and Mendez Palacios was sentenced to 87 months in prison. Both defendants were also sentenced to three years of supervised release, a $200 special assessment, and deportation upon completion of their prison sentences.

X-ray photo and photo of firearms concealed within air tanks, intercepted by Special Agents prior to their intended export

Tian Min Wu

The Violation: On June 9, 2021, Chinese national Tian Min Wu pled guilty in the U.S. District Court for the Central District of California to charges related to the procurement and attempted unlawful export of a military encryption decoder used in the control of shortwave radio receivers, recording, demodulation, and decoding of digital signals emissions controlled under the ITAR to China. Wu, the owner of several companies in Beijing, China, engaged with undercover law enforcement officers in an attempt to purchase and export the decoder, as well as additional technology classified under ECCN 5A002, without first obtaining a license from the Directorate of Defense Trade Controls or BIS. Wu knowingly and willfully solicited the export of these items from the United States, intending to deliver them to the Chinese government. This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office and HSI.

The Penalty: On June 9, 2021, Wu was sentenced to 52 months in prison (time served) and a $100 special assessment (suspended). In July 2022, Wu was deported from the United States. On December 1, 2022, BIS issued Wu a post-conviction denial order for a period of 10 years.

OEE Special Agents conducting inspections with U.S. Customs and Border Protection Officers

Lionel Chan / Muhammad Mohd Radzi

The Violation: On January 22, 2021, Lionel Chan of Brighton, Massachusetts and Muhammad Mohd Radzi of Brooklyn, New York pled guilty in the U.S. District Court for the District of Massachusetts to charges of conspiring to illegally export firearms parts from the United States to Hong Kong in violation of the Arms Export Control Act. Beginning in or around March 2018, Chan began purchasing a variety of U.S.-origin firearm parts online, including parts used to assemble AR-15 assault rifles and 9MM semi-automatic handguns, for a buyer located in Hong Kong. Chan shipped the firearm parts, controlled under the ITAR, via Federal Express to the buyer in Hong Kong without first obtaining the necessary export licenses. Chan intentionally concealed the contents of the shipments by providing Federal Express with false information about the shipments, and by concealing the parts inside of each package. Between March and May 2018, Chan shipped at least 12 packages containing firearm parts from Massachusetts to the buyer in Hong Kong. In or around April 2018, Radzi joined the conspiracy and also began illegally exporting firearm parts from the United States to Hong Kong. Between May and October 2018, Radzi shipped 21 packages from New York to the buyer in Hong Kong. In October 2018, two of those packages were intercepted by Hong Kong authorities and found to contain numerous firearms parts, including a firing pin, a gun sight and numerous pistol grips. Like Chan, Radzi failed to obtain an export license for any of these shipments. This case resulted from a joint investigation conducted by OEE's Boston Field Office, HSI, and CBP.

The Penalty: On May 28, 2021, Chan was sentenced to eight months in prison, three years of supervised release, and a $10,000 criminal fine. Radzi was sentenced to five years of probation and a $10,000 criminal fine.

Jacques Mathieu / Kerline Mathieu

The Violation: Jacques Mathieu and others conspired to straw purchase approximately 32 firearms and 225,000 rounds of ammunition now classified under ECCNs 0A501 and 0A505 and conceal them in vehicles to be exported from Atlanta, Georgia to Haiti. In September 2019, OEE Special Agents detained and seized approximately 46,000 rounds of ammunition and 12 firearms found concealed in the vehicles being exported by Mathieu and his wife Kerline. The Mathieus were arrested in February 2020 and pled guilty in the U.S. District Court for the Northern District of Georgia in July 2020. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office and ATF.

The Penalty: On January 8, 2021, Jacques Mathieu was sentenced to 57 months in prison, three years of supervised release, and a $100 special assessment. Kerline Mathieu received pre-trial diversion.

Usama Hamade / Issam Hamade

The Violation: From 2009 to 2013, Usama Hamade and his brother, Issam Hamade, conspired to illegally export controlled parts and technology used in unmanned aerial vehicles (UAVs) from the United States through intermediaries for ultimate delivery to Hezbollah, in violation of the EAR and the International Traffic in Arms Regulations (ITAR). A number of these U.S. manufactured items included inertial measurement units (IMUs), which can be used to track an aircraft's position, and digital compasses, which can be paired with the IMUs for drone guidance systems. These more specially designed IMUs are controlled under the USML. Other items illegally exported included a jet engine holding ECCN 9A101, and various aircraft parts and components classified under ECCN 7A994. The items were procured from multiple U.S. companies. Usama Hamade, a citizen of South Africa, falsely claimed that the items would be used in drones in South Africa to monitor wildlife in order to prevent poaching activities. In fact, the items were diverted to Lebanon through South Africa and the UAE and ultimately delivered to Hezbollah, a U.S. designated foreign terrorist organization for use in their UAV program. To fund the procurement of these items, Issam Hamade, a citizen of Lebanon, made multiple wire transfers from a bank in Beirut, Lebanon, to the bank account of a South African company, which was controlled by Usama Hamade. The wired transfers totaled nearly $174,000. Subsequent coordination and information sharing between the United States and the South African Governments resulted in both Hamade brothers being arrested by South African authorities in February 2018, and held pending extradition back to the U.S. to face charges. On October 18, 2019, Usama Hamade and Issam Hamade were extradited from South Africa and made their initial appearances in the U.S. District Court for the District of Minnesota. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, the FBI, and HSI.

The Penalty: On April 27, 2020, Issam Hamade was sentenced to time served (26 months), a $100 special assessment, and deportation to Lebanon. On July 20, 2020, Usama Hamade was sentenced to 42 months in prison, a $100 special assessment, and deportation to South Africa upon completion of his prison sentence. On January 25, 2021, BIS issued Issam Hamade a post-conviction denial order for a period of 10 years. On July 8, 2022, BIS issued Usama Hamade a post-conviction denial order for a period of 10 years.

Military Controls

Saul Eady / Troy Barbour / Janet Sturmer / Khalid Razaq / Eunice Nkongho / Brandon Ross / Eucharia Njoku / Saulina Eady

The Violation: This investigation involved a conspiracy to commit mail and wire fraud in connection with a scheme to fraudulently obtain goods using what appeared to be a military e-mail address, but was actually a registered Yahoo e-mail address. According to Saul Eady's plea agreement, a co-conspirator established and used what was purported to be a U.S. Navy e-mail address, authentic forms, titles, addresses, and other indicia to pose as a U.S. government contracting agent and fraudulently obtain merchandise, including large-screen televisions, specialized communications equipment, cellular telephones and computers. Much of the fraud scheme was conducted from outside the United States, including from Nigeria. Three victim companies shipped merchandise, without prior payment, to Eady's East Coast co-conspirators. Those individuals then shipped the stolen items to Eady and others on the West Coast. Saul Eady also admitted that he engaged in financial transactions using the proceeds of the fraud scheme, assisting in depositing cash obtained from the sale of the stolen goods into bank accounts of co-conspirators. At times, Eady received cash in excess of $10,000, but made smaller deposits at different bank locations in order to avoid detection by financial institutions and law enforcement. Based on bank records, surveillance footage, financial and business records of the victim companies, and other information, the loss foreseeable to Saul Eady was between $1.5 million and $3.5 million. This case resulted from a joint investigation conducted by OEE's Washington Field Office, the FBI, DCIS, HSI, and the FBI.

The Penalty: On December 20, 2022, Troy Barbour was sentenced to three years of probation, with the first six months to be served as home detention, and $28,600 in restitution, and a $100 special assessment. On June 1, 2022, Janet Sturmer was sentenced to 54 months in prison, three years of supervised release, $4,494,892 in joint restitution with Khalid Razaq, a $23,400 forfeiture, and a $200 special assessment. On May 10, 2022, Khalid Razaq was sentenced to 60 months in prison, three years of supervised release, the joint restitution with Sturmer, a $457,594 forfeiture, and a $200

special assessment. On April 28, 2022, Eunice Nkongho was sentenced to 24 months in prison, three years of supervised release, $3,99,780 in restitution, and a $200 special assessment. On April 22, 2022, Brandon Ross was sentenced to 18 months in prison, three years of supervised release, $1,500,000 in restitution, a $14,300 forfeiture, and a $100 special assessment. On February 10, 2022, Eucharia Njoku was sentenced to 24 months in prison, three years of supervised release, $3,662,607 in restitution, and a $100 special assessment. On October 13, 2020, Saulina Eady was sentenced to 36 months in prison, three years of supervised release, forfeiture of $500 and property, $640,173 in restitution, and a $100 special assessment. On February 24, 2020, Saul Eady was sentenced to 48 months in prison, three years of supervised release, $640,173 in shared restitution, and a $100 special assessment.

BV Aerospace / William Vanmanen

The Violation: William Vanmanen was the owner and operator of BV Aerospace, a home business located in Long Island, New York that supplied aircraft to industry. The company had been active in the aviation field for years before federal authorities were alerted that many of its aircraft parts were fraudulent. As a result of this, the Department of Transportation Office of the Inspector General (DOT-IG) began looking into the activity of BV Aerospace and the parts that were being placed on aircraft. During the course of the investigation, it was uncovered that not only was Vanmanen selling fraudulent aircraft parts, but he was also exporting these parts to Hong Kong without the required BIS export license authorization. In August of 2011, William Vanmanen exported numerous fuel filter connector parts classified under ECCN 9A991 to Hong Kong without the required export licenses. During the export transactions, Vanmanen also falsified the Shipper's Export Declarations to undervalue the shipments and falsified the air worthiness approval tags that are required by the Federal Aviation Administration. A search warrant conducted at BV Aerospace uncovered evidence related to the fraudulent aircraft parts that were being sold to the aviation industry, as well as the numerous unauthorized exports to Hong Kong. In 2019, Vanmanen pled guilty in the U.S. District Court for the Eastern District of New York. This case resulted from a joint investigation conducted by OEE's New York Field Office, HSI, DCIS, and DOT-OIG.

The Penalty: On October 3, 2019, Vanmanen was sentenced to 30 months in prison and 24 months of supervised release.

Federal Express

The Violation: On 53 occasions between 2011 and 2012, Federal Express (FedEx), located in Memphis, Tennessee, facilitated the export of civil aircraft parts and equipment used for electronic microscope manufacturing classified under ECCN 9A991 or 7A994, or designated EAR99, and valued at approximately $58,091 from the United States to Aerotechnic France (Aerotechnic), or to the Pakistan Institute for Nuclear Science and Technology (PINSTECH) in Pakistan, without the required BIS licenses. Aerotechnic was added to the BIS Entity List in June 2011 "based on evidence that [it had] engaged in actions that could enhance the military capability of Iran, a country designated by the U.S. Secretary of State as having repeatedly provided support for acts of international terrorism…[and] because [its] overall conduct pose(d) a risk of ongoing EAR violations." PINSTECH is a subordinate entity of the Pakistan Atomic Energy Commission, and has been on the BIS Entity List since November 1988, when it was added along with a number of other Pakistani government (parastatal and private) entities involved in nuclear or missile activities shortly after Pakistan detonated a nuclear device. This case resulted from an investigation conducted by OEE's Miami Field Office.

The Penalty: On April 24, 2018, FedEx agreed to pay a $500,000 civil penalty.

Ali Caby / Marjan Caby / Arash Caby

The Violation: In February 2017, Iranian nationals Ali Caby, Marjan Caby, and Arash Caby were arrested in connection with a conspiracy to illegally export aviation parts classified under ECCN 9A991 to Syrian Arab Airlines, which appears on OFAC's SDN List for transporting weapons and ammunition to Syria in conjunction with terrorist organization Hezbollah, and the Iranian Revolutionary Guard Corps. Ali Caby ran the Bulgaria office of AW-Tronics, a Miami, Florida-based export company that was managed by Arash Caby, and which shipped and exported various aircraft parts and equipment to Syrian Arab Airlines. Ali Caby and Arash Caby closely supervised and encouraged subordinate employees of AW-Tronics in the willful exportation of the parts and equipment to SDN Syrian Air, whose activities have assisted the Syrian government's violent crackdown on its people. Marjan Caby, as

AW-Tronics' export compliance officer and auditor, facilitated these exports by submitting false and misleading electronic export information to federal agencies. This case resulted from a joint investigation conducted by OEE's Miami Field Office, the FBI, HSI, and DCIS.

The Penalty: On December 19, 2017, Ali Caby, Marjan Caby, and Arash Caby were sentenced in the U.S. District Court for the Southern District of Miami. Ali Caby was sentenced to two years in prison, two years of supervised release and a $100 special assessment. Marjan Caby was sentenced to one year and one day in prison, two years of supervised release and a $100 special assessment. Arash Caby was sentenced to two years in prison, two years of supervised release, a $10,000 criminal fine and a $100 special assessment. All three defendants were also subject to a shared $35,000 forfeiture as part of the plea agreement. In addition, in 2019 a six-year denial of export privileges was imposed on Ali Caby, Arash Caby, AW-Tronics and Arrowtronics.

WMD Controls

Muhammad Mohsin Raja

The Violation: Muhammad Mohsin Raja for several years operated a hawala remittance system based out of New York. Raja transmitted approximately $4.7 million to Pakistan in 2021 alone. As part of the hawala, he made multiple payments for products intended for Pakistan's Advanced Engineering Research Organization (AERO), which had been added to the BIS Entity List for procuring items for use in Pakistan's cruise missile and strategic UAV programs. Raja made payments for a blade antenna manufactured by a New Hampshire defense contractor. Those antennas are typically used in UAVs, tactical missiles, helicopters, and aircraft. He also made payments to a Florida defense contractor for rotary pumps and a solenoid valve. The rotary pumps were designed for use in M110 self-propelled howitzers, and the solenoid valve was designed for use in an AIM-9 Sidewinder missile or an AGM-86B air-launched cruise missile. Raja also made payments to a Florida-based firearms manufacturer on behalf of a Pakistani company called Al-Akbar Arms. The payments were for two shipments of assault weapons. Raja messaged another individual suggesting they disguise the purpose of the payments as "purchasing watches as sports equipment." However, law enforcement successfully intercepted the assault weapons. This case resulted from a joint investigation conducted by OEE's Boston Field Office and the FBI.

The Penalty: On August 30, 2023, Muhammad Mohsin Raja was sentenced in the U.S. District Court for the District of New Hampshire to 24 months in prison and one year of supervised release.

Obaidullah Syed / Business Systems International Pvt. Ltd.

The Violation: On October 26, 2021, Obaidullah Syed of Northbrook, Illinois pled guilty to conspiracy to exporting U.S. goods and services without a license from BIS and to submitting false export information. Syed owned Pakistan-based Business Systems International Pvt. Ltd., and BSI USA, which he operated from his home. The companies provided and serviced high-performance computers, servers, and software. Since 2002, Syed used these businesses and their employees to acquire and export computer equipment classified under ECCNs 4A994 and 5A991, or designated EAR99, to the Pakistan Atomic Energy Commission (PAEC). PAEC is a Pakistani government agency that was added to the BIS Entity List for activities related to nuclear weapons proliferation. To avoid any BIS license requirements for exports going to the PAEC, Syed and other conspirators falsely represented to U.S.-based suppliers that the shipments were intended for use by BSI as marketing tools or provided Pakistan-based universities as false end users. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, DCIS, and HSI.

The Penalty: On May 17, 2022, Syed was sentenced to 366 days in prison and a criminal forfeiture of $247,000. BIS subsequently issued a post-conviction denial order for Syed for a period of 10 years.

Alsima Middle East General Trading LLC

The Violation: On or about October 5, 2015, Alsima Middle East General Trading LLC (Alsima) made false and misleading representations, statements, and certifications in connection with the submission to BIS of a license application for the export to the United Arab Emirates (UAE) of a powder grade nickel classified under ECCN 1C402 and controlled for nonproliferation and antiterrorism reasons. In the submission of the license application, Alsima

falsely and misleadingly represented that the nicked powder was to be used to manufacture self-lubricating seal rings in the UAE for distribution in the UAE. In 2016, BIS conducted a post shipment verification check at Alsima. The director of Alsima stated that the nickel powder was for the manufacturing of specialized compressor rings. However, the director further clarified that Alsima had intended to export the manufactured rings to an Azerbaijani company. He also stated that he had contacted companies in South Africa and India about manufacturing the rings for the Azerbaijani company if Alsima provided the nickel powder. This case resulted from an investigation conducted by OEE's New York Field Office.

The Penalty: On May 28, 2021, Alsima agreed to pay a $25,000 civil penalty, $12,500 of which was suspended provided no violations occur during a two-year probationary period.

MDA Precision LLC

The Violation: During April 2015, MDA Precision LLC of Gilroy, California sold and transferred a five-axis benchtop milling machine classified under ECCN 2B201 and controlled on nuclear nonproliferation and anti-terrorism grounds to the United Arab Emirates without the required BIS license. In the shipper's letter of instructions that it provided the freight forwarder, MDA Precision LLC stated that the item was designated EAR99 and did not require a license for export to the UAE. Moreover, the company failed to act on red flags that were present in the transaction indicating that the items were intended for diversion. This case resulted from an investigation conducted by OEE's San Jose Field Office and the FBI.

The Penalty: On April 30, 2021, MDA Precision LLC agreed to pay a $60,000 civil penalty, $35,000 of which was suspended provided no violations occur during a two-year probationary period. The company was also ordered to complete and export compliance training on the Regulations within 12 months.

Princeton University

The Violation: On 37 occasions between 2013 and 2018, Princeton University engaged in conduct prohibited by the EAR when it exported various strains and recombinants of an animal pathogen classified under ECCN 1C351, 1C352, or 1C353, controlled for Chemical and Biological Weapons reasons, from the United States to various overseas research institutions. These research institutions were located in Belgium, United Kingdom, Singapore, Canada, France, Israel, Japan, Denmark, Switzerland, Australia, Hungary, Portugal, South Korea, India and China. This case resulted from an investigation conducted by OEE's New York Field Office

The Penalty: On February 1, 2021, Princeton University agreed to pay a $54,000 civil penalty. The University was also ordered to complete an internal audit of its export controls compliance program, as well as an external audit to be conducted by an unaffiliated third-party consultant.

Voluntary Self-Disclosure: Princeton University voluntarily disclosed the violations and cooperated fully with the investigation.

Kenneth Chait / Tubeman.com / Advantage Tube Services, Inc.

The Violation: In October 2012, U.S. citizen Kenneth Chait, owner/operator of Tubeman.com/Advantage Tube Services, Inc., located in Lake Worth, Florida, communicated to an undercover OEE Special Agent that he was willing to export to Pakistan two ceramic metal triggered spark gaps (also known as nuclear trigger spark gaps), without the required BIS export license. The spark gaps were listed on the Commerce Control List, controlled for nuclear proliferation reasons, and therefore required a license for export to Pakistan. HSI Special Agents then conducted undercover operations by speaking with Chait regarding obtaining a ceramic metal triggered spark gap classified under ECCN 3A228 for export to Pakistan. Chait was arrested in March 2014 during execution of a search warrant, and in April 2015, he pled guilty in the U.S. District Court for the Middle District of Georgia to violations of the International Emergency Economic Powers Act and the EAR in connection with the attempted export of nuclear trigger spark gaps to Pakistan without a license. This case resulted from a joint investigation conducted by OEE's Miami Field Office and HSI.

The Penalty: On November 13, 2018, Kenneth Chait was sentenced to 12 months and one day in prison, two years of supervised release, and a $100 special assessment. As part of the plea agreement, Chait agreed to forfeit $7,465 to the U.S. Government, which represents the proceeds traceable to the undercover transactions in which he participated. On September 30, 2019, BIS issued Chait a post-conviction denial order for a period of five years.

Imran Khan / Kamran Khan / Muhammad Ismail

The Violation: From at least December 2012 through December 2016, brothers Imran Khan and Kamran Khan and their father Muhammad Ismail engaged in a scheme to purchase U.S.-origin items, including spectrometers classified under ECCN 3A999 and other commodities designated EAR99, for parties in Pakistan that appear on the BIS Entity List. 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 United States, or completed an end-user certificate 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 PAEC, the Pakistan Space & Upper Atmosphere Research Commission (SUPARCO), or the National Institute of Lasers & Optronics (NILOP), all of which appeared on the BIS Entity List. The defendants never obtained a BIS 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. In June 2017, Imran Khan pled guilty to violating the IEEPA when he procured, received, and exported a spectrometer to PAEC without an export license. In March 2018, Muhammad Ismail and Kamran Khan each pled guilty for causing funds to be transferred from Pakistan to the United States in connection with the export control violations. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, HSI, DCIS, and USPIS.

The Penalty: On September 19, 2018, Imran Khan was sentenced to three years of probation (the first six months of which were to be served in home confinement), a $3,000 criminal fine, 100 hours of community service, and a $200 special assessment. On July 18, 2018, Kamran Khan and Muhammed Ismail were each sentenced to 18 months in prison, three years of probation, and a $100 special assessment.

Cryofab, Inc.

The Violation: On two occasions during 2012, Cryofab, Inc. of Kenilworth, New Jersey, engaged in conduct prohibited by the EAR by exporting gas storage containers and related tools and accessories designated EAR99 to the Bhabha Atomic Research Center (BARC), without the required BIS export licenses. At the time of the exports, BARC appeared on the BIS Entity List. Although an experienced exporter, Cryofab Inc. failed to screen against the BIS Entity List in connection with these two transactions, and failed to seek or obtain the required BIS export licenses. It also erroneously listed the items as eligible for shipment without a license on the Shipper's Letter of Instructions for each shipment. This case resulted from an investigation conducted by OEE's New York Field Office.

The Penalty: On August 18, 2017, Cryofab, Inc. agreed to pay a $35,000 civil penalty. The company was also ordered to complete an external audit of its export controls compliance program, to be conducted by an unaffiliated third-party consultant.

Trexim Corporation / Bilal Ahmed

The Violation: On October 2, 2014, Bilal Ahmed pled guilty in connection with the export of carbon fiber and microwave laminates, and the attempted export of a thermal imaging camera, from his company Trexim Corporation of Schaumberg, Illinois, to Pakistan without the required export licenses. Ahmed admitted that in 2009 he shipped carbon fiber to Pakistan's Space and Upper Atmosphere Research Commission (SUPARCO), an entity on the BIS Entity List. Ahmed knew that the carbon fiber and thermal imaging camera were export- restricted and a license was required from the U.S. Government. Ahmed also undervalued the goods he exported to Pakistan to

avoid filing an SED and to avoid detection. The carbon fiber was classified under ECCN 1C210 and was controlled for nuclear non-proliferation and anti-terrorism reasons. The thermal imaging camera was classified under ECCN 6A003 and was controlled for national security and regional stability reasons. Ahmed was arrested in March 2014 as he attempted to ship a FLIR thermal imaging camera to Pakistan. This case resulted from a joint investigation conducted by OEE's Headquarters and the FBI.

The Penalty: On May 14, 2015, Bilal Ahmed was sentenced in the U.S. District Court for the Northern District of Illinois to 24 months in prison, two years of supervised release, a $1,000 criminal fine, and a $100 special assessment.

General Logistics International

The Violation: On four occasions between during November 2009, General Logistics International of New Brunswick, New Jersey, facilitated the unauthorized export of EAR99 steel scrap, valued at $672,022, from the United States to the People's Steel Mills, located in Pakistan. The People's Steel Mill appears on the BIS Entity List. For each export, General Logistics International arranged for the trucking of the scrap steel from the U.S. exporter's location to the port of export, arranged for the shipping of the scrap steel to People's Steel Mills in Pakistan, and prepared and submitted shipping documentation, part of which indicated that no license was required for these exports. This case resulted from an investigation conducted by OEE's New York Field Office.

The Penalty: On January 22, 2015, General Logistics International entered into a settlement agreement with BIS in which it agreed to pay $90,000.

GrafTech International Holdings Inc.

The Violation: Between July 2007 and January 2010, GrafTech International Holdings Inc. (GrafTech), of Parma, Ohio, exported 12 shipments of CGW grade graphite to China and India without the required BIS licenses. The high-grade graphite, valued at approximately $524,000, is classified under ECCN 1C107 and controlled for missile technology reasons. This case resulted from an investigation conducted by OEE's Washington Field Office.

The Penalty: On October 25, 2013, GrafTech agreed to pay a $300,000 civil penalty. The agreement also includes an external audit requirement relating to GrafTech's compliance program and the compliance programs of three foreign GrafTech subsidiaries.

Voluntary Self-Disclosure: GrafTech voluntarily disclosed the violations and cooperated fully with the investigation.

Flowserve Corporation

The Violation: Between 2002 and 2008, Flowserve Corporation, located in Irving, Texas, and ten of its foreign affiliates made unlicensed exports and reexports of pumps, valves and related components classified under ECCN 2B350 to a variety of countries including China, Singapore, Malaysia and Venezuela and caused the transshipment of U.S.-origin EAR99 items to Iran and Syria without the required U.S. Government authorization. The items exported to non-embargoes destinations were controlled by the U.S. Department of Commerce for reasons of chemical and biological weapons proliferation and required licenses for export to China, Singapore, Malaysia, and Venezuela. This case resulted from an investigation conducted by OEE's Dallas Field Office.

The Penalty: On September 29, 2011, Flowserve Corporation and ten of its foreign affiliates agreed to pay civil penalties totaling $2.5 million. The settlement also required external audits of Flowserve's compliance program. Flowserve also agreed to pay OFAC a civil penalty of $502,408 for transactions involving Iran, Sudan and Cuba.

Voluntary Self-Disclosure: Flowserve voluntarily disclosed these violations and cooperated fully with the investigation.

Buehler Limited

The Violation: Between November 2001 and July 2006, Buehler Limited of Lake Bluff, Illinois, a global manufacturer of scientific equipment and supplies for use in materials research and analysis, made 80 exports of a product called "Coolmet," a mixture containing triethanolamine (TEA) that is used as a lubricant with cutting tools, to various destinations including China, Hong Kong, Thailand, India, Brazil and Israel, without the required BIS licenses. Additionally, on one occasion in August 2005, the company's German affiliate re- exported Coolmet from Germany to Iran without the required U.S. Government authorization. TEA is a Schedule 3 chemical precursor classified under ECCN 1C350 and is controlled for chemical/biological, anti-terrorism and chemical weapons reasons. This case resulted from an investigation conducted by OEE's Chicago Field Office.

The Penalty: On December 12, 2008, Buehler Limited agreed to pay a $200,000 civil penalty.

Voluntary Self-Disclosure: Buehler Limited voluntarily disclosed the violations and cooperated fully with the investigation.

Dr. Thomas Butler

The Violation: On January 14, 2003, Dr. Thomas Campbell Butler, M.D., a professor at Texas Tech University in Lubbock, Texas, reported to the FBI that 30 vials of a potentially deadly plague bacteria, *Yersinia pestis* (the causative agent of human plague), were missing and presumed stolen from his research lab. The report sparked a bio-terrorism alert in west Texas, and the President was informed of the incident. An investigation ultimately proved that Dr. Butler had illegally exported *Yersinia pestis* to Tanzania. The bacteria is classified under ECCN 1C351 and cannot be exported to Tanzania without an export license from BIS. On January 15, 2003, Dr. Butler was arrested. Dr. Butler was found guilty of numerous charges at trial, two of which were export control-related: making false, fraudulent and fictitious statements regarding the export to federal agents and making an unauthorized export to Tanzania. This case resulted from a joint investigation by OEE's Dallas Field Office, the FBI, IRS, and DOT.

The Penalty: Dr. Butler was convicted of 47 counts of a 69-count indictment. He was sentenced to two years in prison on March 10, 2004, and he resigned from Texas Tech. On October 24, 2005, the U.S. Court of Appeals for the Fifth Circuit affirmed his conviction. In the administrative case, on September 1, 2006, Dr. Butler agreed to pay a $37,400 civil penalty and accept a denial of his export privileges for a period of 10 years.

Other Controls

Ya Wen Chen aka Tina Chen / Top One Zone

The Violation: Tina Chen, aka Ya When Chen, owner of Top One Zone, LLC, operated an electronics and computer components exporting company out of her residence in Nevada. From about November 2015 to May 2019, Chen conspired with others to buy and export goods from companies in the United States, including electronic components and drone equipment designated EAR99, and then send those goods to individuals in Iran through companies in Hong Kong. Chen concealed the identities of the end users and did not have the required authorization to export the items. Chen pled guilty to the charges in September 2022. This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office and the FBI.

The Penalty: On February 23, 2023, Chen was sentenced in the U.S. District Court for the District of Nevada to 13 months in prison and three years of supervised release. BIS subsequently issued Chen a post-conviction denial order for a period of 10 years.

NuDay aka NuDay Syria

The Violation: Between 2018 and 2021, NuDay, aka NuDay Syria, a charity located in Windham, New Hampshire, made over 100 shipments to Syria, a country that was subject to sanctions and export restrictions. NuDay claimed that

these shipments were worth over $100 million. NuDay had the items shipped to Mersin, Turkey, where another company would transship them into Syria. DOC regulations require exporters, such as NuDay, to report true and accurate information about the items being exported, including the shipment's description, end user, and monetary value. However, NuDay falsely reported that the end destination of the shipments was Turkey and not Syria, and artificially deflated the value of the goods to be below the $2,500 reporting threshold. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, HSI, and the IRS.

The Penalty: On December 28, 2023, NuDay was sentenced in the U.S. District Court for District of New Hampshire to five years of probation, the maximum penalty for an organizational defendant, a $25,000 fine, and a $1,200 special assessment.

Jacques Yves Duroseau

The Violation: Former U.S. Marine Jacques Yves Sabastien Duroseau impersonated a high-ranking military officer and fraudulently pretended to be on military orders to facilitate the illegal export of eight firearms, ammunition, and body armor controlled under the ITAR, as well as rifle scopes classified under ECCN 0A987, via commercial aircraft to Haiti. In November 2019, Duroseau packed-up the related export-controlled equipment and defense-articles, arrived at the airport, and properly declared the firearms and ammunition to the airline. The airline checked-in Duroseau and processed the firearms and ammunition for the flight to Haiti. Upon landing in Port-au-Prince and engaging Haitian Customs, Duroseau was detained by the Haitian National Police. He spent several weeks in custody in Haiti before he was turned over to NCIS for investigation and ultimate prosecution. On December 10, 2020, following a three-day trial in the U.S. District Court for the Eastern District of North Carolina, Duroseau was found guilty of illegally exporting defense-articles and firearms from the United States to Haiti without the necessary authorization. With the completion of the Defendant's 4th Circuit Appeal, on May 24, 2022, Duroseau was resentenced in the U.S. District Court for the Eastern District of North Carolina. This case resulted from a joint investigation conducted by OEE's Washington Field Office, NCIS, HSI, DSS, ATF, and the U.S. Marine Corps.

The Penalty: On May 24, 2022, Duroseau was re-sentenced to 60 months in prison, three months of probation, and a $400 special assessment. BIS subsequently issued Duroseau a post-conviction denial order for a period of 10 years.

Andrew Hsu

The Violation: On June 26, 2020, Andrew Hsu pled guilty to charges related to the illegal export of gas flowmeters designated as EAR99 to Taiwan in violation of a BIS Denial Order, which was issued in 2015 based on Hsu's previous conviction of unlawfully exporting industrial parts designated EAR99 to Iran. To obscure his activity and evade the Denial Order restrictions, Hsu utilized his wife's business name to procure and illegally export the items to Taiwan. This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office and the FBI.

The Penalty: On December 11, 2020, Andrew Hsu was sentenced in U.S. District Court for the Central District of California to three years of probation, a $10,000 fine, and a $100 special assessment.

Joseph Koyshman

The Violation: Beginning in 2016, Josef Koyshman, owner of LVN Airsoft in Las Vegas, Nevada, conspired with others to export and attempted to export various firearms-related commodities to Hong Kong without the required export authorization. From July through September 2016, Koyshman and his co-conspirator agreed to export high-power advanced laser-aiming systems, handheld radios, and binocular night vision goggles controlled under the ITAR, as well as rifle scopes classified under ECCN 0A987, to Hong Kong. In exchange for compensation, Koyshman received the controlled commodities at his address in the United States to disguise the international nature of the transactions. Koyshman also used his company as the domestic end user on export compliance documents. He then attempted to export or exported the commodities to Hong Kong without a license. The controlled commodities would sometimes be co-mingled with items not requiring an export license. Koyshman's co-conspirator was arrested in October 2016 and Koyshman was arrested in May 2019. Koyshman pled guilty in the U.S. District Court for the District of Columbia in November 2019. This case resulted from a joint investigation conducted by OEE's Portland Resident Office, HSI, AFOSI, and DCIS.

The Penalty: On February 6, 2020, Koyshman was sentenced to 12 months and one day in prison, 24 months of supervised release, and a $100 special assessment. BIS subsequently issued Koyshman a post-conviction denial order for a period of 10 years.

Steven Anichowski

The Violation: In August 2017, HSI requested the assistance of OEE in an ongoing investigation that involved the export of United States Munitions List (USML) and the CCL items to possible Japanese Organized Crime members. After Special Agents conducted interviews, it was confirmed Steven Anichowski was procuring U.S.-origin gun parts and other accessories controlled under the USML, and rifle scopes and sights classified under ECCN 0A997 (currently ECCN 0A054) for two Japanese citizens. In July 2018, OEE, HSI, FBI and NCIS Special Agents arrested and interviewed Anichowski at Los Angeles International Airport as he arrived from Taiwan. In April 2019, Anichowski pled guilty in the U.S. District Court for the District of New Mexico. This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office, the FBI, HSI, USPIS, and NCIS.

The Penalty: On December 4, 2019, Steven Anichowski was sentenced to 12 months and one day in prison, two years of supervised release, and a $100 special assessment.

Patrick Germain

The Violation: On October 9, 2018, Patrick Germain pled guilty in the U.S. District Court for the Northern District of Illinois in connection with the illegal export of firearms to Haiti. In June 2016, Germain purchased 26 firearms, five shotguns classified under ECCN 0A984 (currently ECCN 0A502), 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 a company to deliver the three vehicles to Miami, where he arranged for a shipping company to transport the vehicles to Haiti. Germain devised a scheme to hide some of the items inside a hollowed-out wooden container constructed of plywood in a van he arranged to export through the Port of Miami 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 back seat. The van was detained and the firearms located. Germain was arrested in December of 2016 when he returned to the United States from Haiti. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, HSI, and ATF.

The Penalty: On May 16, 2019, Patrick Germain was sentenced to time served in prison (23 days), two years of supervised release, and a $100 special assessment. On October 30, 2020, BIS issued Germain a post-conviction denial order for a period of 10 years.

Eric Baird / Access USA Shipping, LLC

The Violation: On December 12, 2018, Eric Baird, the former owner and Chief Executive Officer (CEO) of Access, a Florida-based package consolidation and shipping service, pled guilty in the U.S. District Court for the Middle District of Florida 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 BIS. Baird admitted to violations of the EAR committed from August 1, 2011, through January 7, 2013, during his tenure as CEO of Access USA Shipping, LLC dba 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. For example, laser sights for firearms were described as "tools and hardware," and rifle scopes were described as "sporting goods" or "tools, hand tools." 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 AES filings. In doing so he caused, or permitted, the filing of false or misleading SED and AES filings. Baird also failed to make required SED/AES filings and also caused, aided or abetted the export of items subject to the EAR without the required export licenses. 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" (emphasis in original). 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." 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. This case resulted from a joint investigation conducted by OEE's Miami Field Office and HSI.

The Penalty: On January 30, 2019, Eric Baird was sentenced to 24 months of probation and a $100 special assessment. Baird also agreed to a five-year denial of export privileges and a $17 million fine with $7 million suspended. Access USA also agreed to an administrative fine of $27 million with $17 million suspended.

Rasheed Al Jijakli / Palmyra Corporation

The Violation: From June through July of 2012, Syrian-born naturalized U.S. citizen Rasheed Al Jijakli and a co-conspirator purchased tactical gear, including day vision and night vision rifle scopes classified under ECCN 0A987 (currently classified under ECCN 0A504), laser boresighters, flashlights, radios and other items designated EAR99, for intended end use in Syria. On July 17, 2012, Al 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. Al Jijakli provided some of the tactical gear, specifically the laser boresighters, to a second co-conspirator, who Al Jijakli learned was a member of the militant group Ahrar Al-Sham. Al Jijakli also provided the goods to other armed Syrian insurgent groups in Syria and Turkey. Additionally, in August and September 2012, Al Jijakli directed co-conspirators to withdraw thousands of dollars from Palmyra Corporation, where Al Jijakli was the chief executive officer, to pay for tactical gear that would be provided to Syrian rebels. In his plea agreement, Al Jijakli specifically admitted directing that $17,000 from Palmyra be used to purchase tactical gear intended for Syrian rebels. On August 13, 2018, Al Jijakli pled guilty in connection with a conspiracy to illegally export tactical gear to Syria. During Al Jijakli's sentencing hearing, the Judge agreed with prosecutors that the goods Al Jijakli took to Syria were "instruments of death." This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office, the FBI, HSI, and IRS.

The Penalty: On December 20, 2018, Rasheed Al Jijakli was sentenced to 46 months in prison, two years of supervised release, a $5,000 criminal fine, and a $100 special assessment. In addition, on September 30, 2019, a 10-year denial of export privileges was imposed on Jijakli.

Bryan Singer

The Violation: On June 12, 2018, Bryan Singer was found guilty by a jury in the U.S. District Court for the Southern District of Florida in connection with the unlicensed attempted smuggling of electronic devices to Cuba and the making of false statements to federal law enforcement officials. On May 2, 2017, Singer intended to travel from Stock Island, Florida to Havana, Cuba aboard his vessel "La Mala." Prior to his departure, a CBP Officer conducted an outbound inspection of the boat. During the inspection, Singer asserted that he was only bringing to Cuba items observable on the deck and that their value was less than $2,500. However, the CBP agent discovered a hidden compartment under a bolted down bed in the cabin that contained hundreds of electronic devices valued at over $30,000. The devices included more than 300 Ubiquiti Nanostation Network devices designed to provide highly encrypted connections between computer networks over long distances. Singer had been previously warned by U.S. Government officials on at least four occasions that a license was required to export items to Cuba. This case resulted from a joint investigation conducted by OEE's Miami Field Office, HSI, and CBP.

The Penalty: On September 27, 2018, Bryan Singer was sentenced in the Southern District of Florida to 78 months in prison, to be followed by supervised release.

Chapter 5 – Antiboycott Violations

Introduction

The Office of Antiboycott Compliance (OAC) administers and enforces the antiboycott provisions of the EAR, which are set forth in Part 760 of the EAR. These antiboycott provisions prohibit U.S. persons from complying with certain requirements of unsanctioned foreign boycotts, including requirements that the U.S. person provide information about business relationships with a boycotted country or refuse to do business with certain persons for boycott - related reasons. In addition, the EAR requires that U.S. persons report their receipt of certain boycott requests to BIS. Failure to report the receipt of certain boycott requests may constitute a violation of the EAR. Under the antiboycott provisions of the EAR, certain foreign subsidiaries of domestic U.S. companies are considered to be U.S. persons. To help members of the exporting community better understand the substance and applications of the antiboycott provisions, BIS offers an antiboycott training module through the *BIS Online Training Room*. The information and examples contained in the module illustrate how to identify an antiboycott issue and how to respond in a manner that complies with the requirements of the EAR. The Training Room also houses a number of pre-recorded webinars covering a variety of topics, including the basics of U.S. export control and deemed exports. The training modules are presented in a video streaming format.

In addition, Supplement No. 2 to Part 766 of the EAR provides guidance regarding BIS's penalty determination process in the settlement of administrative antiboycott cases involving violations of Part 760 of the EAR or violations of Part 762 (Recordkeeping), which specifies the recordkeeping requirements that pertain to activity that is subject to Part 760. Similar to guidance regarding administrative export control cases, Supplement No. 2 to Part 766 describes how BIS determines appropriate penalties in settlement of violations in antiboycott cases. The guidance contains a comprehensive description of the factors taken into account in determining civil penalties including significant mitigating and aggravating factors.

As in export control cases, BIS encourages submission of voluntary self-disclosures (VSDs) by parties who believe they may have violated the antiboycott provisions of the EAR. The procedures relating to antiboycott VSDs are set out in Section 764.8 of the EAR, which details timing requirements and the information that must be included in the initial notification and in the narrative account of the disclosure.

OAC monitors the type and origin of boycott-related requests received by U.S. persons. Because boycott-related terms and conditions may pose a barrier to trade, OAC partners with the Office of the U.S. Trade Representative and the U.S. Department of State and U.S. Embassy officials to engage with ministers and other government officials in boycotting countries in an effort to remove boycott language from letters of credit, tenders, and other transaction documents at their source. To raise awareness of the sources of boycott-related requests and facilitate fulfillment of the reporting requirements, as required by Part 760 of the EAR, OAC now posts on its webpage, and updates quarterly, a list of entities who have been reported to BIS, on a boycott request report form, as having made a boycott-related request in connection with a transaction in the interstate or foreign commerce of the United States. U.S. companies are encouraged to remain vigilant when they undertake any export or other business transaction that might implicate an unsanctioned foreign boycott and to review transaction documents from all sources, but especially from or involving the listed entities, to identify possible boycott-related language and to report to BIS the receipt of a request to comply with such boycott, as required by part 760 of the EAR.

On October 7, 2022, BIS published updated Guidance on Penalty Determinations in the Settlement of Administrative Enforcement Cases Involving Antiboycott Matters. This rule coincided with an update to BIS antiboycott enforcement policy to enhance penalties, reprioritize violation categories, impose new requirements on the admission of misconduct, and renew focus on foreign subsidiaries of U.S. companies. These enhancements carry strong symbolic importance to the United States and our allies by acknowledging the illegal nature of the discriminatory and other prohibited actions and harm inflicted on the United States foreign policy interests of

unsanctioned boycotts. Further information related to this update can be found on the BIS website: *https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3155-2022-10-06-bis-press-release-enhancing-antiboycott-enforcement-final-1/file*

For advice concerning boycott-related requests contained in export transaction documents, or any other matter concerning the antiboycott provisions of the EAR, please visit the Office of Antiboycott Compliance portion of the BIS website: *https://www.bis.doc.gov/index.php/enforcement/oac*, or contact the OAC advice line via the website, above, or by telephone at (202) 482-2381.

An Overview of the Antiboycott Authorities

History

During the mid-1970s the United States took steps to counteract the participation of U.S. persons in other nations' economic boycotts of countries friendly to the United States. These actions culminated in, among other developments, the enactment of 1977 amendments to the Export Administration Act of 1960 and the Ribicoff Amendment to the 1976 Tax Reform Act. The 1977 amendments, which establish Commerce's core antiboycott prohibitions, subsequently formed the basis of Section 8 of the Export Administration Act of 1979, as amended (EAA). On August 13, 2018, President Trump signed into law the Export Control Reform Act of 2018 (ECRA), 50 U.S.C. §§ 4801-4852, which includes the Anti-Boycott Act of 2018. The ECRA provides the legal authority for BIS's antiboycott enforcement regime. It carries forward Section 8 of the EAA as to prohibited conduct and jurisdictional requirements. Part 760 of the EAR, in turn, implements ECRA's antiboycott provisions.

Objectives

To encourage, and in specific cases, to require U.S. persons to refuse to participate in foreign boycotts of a country friendly to the United States and that is not itself subject to boycott under United States law.

Primary Focus

Although the ECRA/Part 760 of the EAR apply generally to all boycotts of countries that are friendly to the United States that are imposed by foreign countries, the Arab League boycott of Israel is the principal foreign boycott with which U.S. person must be concerned today.

Who (and What Activities) Are Covered by Part 760 of the EAR?

The antiboycott provisions set forth in Part 760 of the EAR apply to "all U.S. persons," defined to include individuals and companies located in the United States and, in certain circumstances, such companies' foreign affiliates and subsidiaries. These U.S. persons are subject to the Part 760 of the EAR when they undertake certain activities relating to the sale, purchase, or transfer of goods or services (including information) within the U.S. or between the U.S. and a foreign country with the intent to comply with, further, or support an unsanctioned foreign boycott. These activities include exports from the U.S., forwarding and shipping, financing, and certain other transactions by U.S. persons who are not located in the United States.

Administrative Case Examples

Forta, LLC

The Violation: During 2019, Forta, LLC, a manufacturer of synthetic reinforcement fibers located in Grove City, Pennsylvania, participated in a trade show in the United Arab Emirates. In connection with the shipment of products and items for display at the trade show, the company furnished to its freight forwarder a commercial invoice/packing list certifying that the goods were not of Israeli origin and not manufactured by a company on the "Israeli Boycott Blacklist." Furnishing such information is prohibited by Section 760.2(d) of the EAR. In addition, the company failed to report to BIS receipt of the request to engage in a restrictive trade practice or boycott.

The Penalty: On November 3, 2023, Forta, LLC agreed to pay a civil penalty of $44,750.

Voluntary Self-Disclosure: Forta, LLC voluntarily disclosed the violations and cooperated fully with the investigation.

Pratt & Whitney Components Solutions, Inc.

The Violation: Pratt and Whitney Component Solutions, Inc. (PWCS), located in Muskegon, Michigan, on 13 occasions failed to report to BIS the receipt of requests to engage in a restrictive trade practice or foreign boycott against a country friendly to the United States. Specifically, between May 2019 and March 2020, PWCS received a request from a customer in Qatar to refrain from importing Israeli-origin goods into Qatar in fulfillment of purchase orders from that customer. Failure to report the receipt of such requests is prohibited by Section 760.5 of the EAR.

The Penalty: On September 7, 2023, PWCS agreed to pay a civil penalty of $48,750.

Voluntary Self-Disclosure: PWCS voluntarily disclosed the violations to BIS.

Regal Beloit FZE

The Violation: Between February 2017 and September 2021, Regal Beloit FZE (Dubai) (Regal Dubai), a controlled-in-fact foreign subsidiary of Regal Beloit America, Inc., received 84 requests from a Saudi Arabian customer to refrain from importing Israeli-origin goods into Saudi Arabia in fulfillment of purchase orders from that customer. Regal Dubai failed to report to BIS the receipt of these requests to engage in a restrictive trade practice or foreign boycott against a country friendly to the United States. Failure to report the receipt of such requests is prohibited by Section 760.5 of the EAR.

The Penalty: On May 18, 2023, Regal Dubai agreed to pay a civil penalty of $283,500.

Voluntary Self-Disclosure: Regal Dubai voluntarily self-disclosed the conduct to BIS, cooperated with the investigation, and took remedial measures after discovering the conduct at issue, which resulted in a significant reduction in penalty.

Kuwait Airways Corporation

The Violation: During the years 2014 through 2015, Kuwait Airways Corporation (KAC), a permanent domestic establishment (registered in New Jersey) of a foreign corporation, on 14 occasions, refused to accept individuals who were holders of Israeli passports for boarding as passengers on Kuwait Airways flight KU 102 from John F Kennedy International Airport (New York) to London Heathrow Airport (United Kingdom). Kuwait Law prohibits entering agreements with entities or persons residing in Israel, or who have Israeli citizenship, regardless of their domicile. In so doing, KAC committed 14 violations of Section 760.2(a) of the EAR, which prohibits refusals to do business with a national or resident of a boycotted country, or with another person, pursuant to an agreement with, a requirement of, or a request from or on behalf of a boycotting country.

The Penalty: On December 26, 2019, Kuwait Airways Corporation agreed to a civil penalty of $700,000, with $600,000 to be paid out-of-pocket and $100,000 to be suspended during a three-year probationary period.

RHDC International (Houston)

The Violation: During the years 2011 through 2013, in connection with the preparation and processing of documents in letter of credit transactions on behalf of its clients involved in the sale and/or transfer of goods to customers in Kuwait, Lebanon, Qatar and the United Arab Emirates, RHDC International LLC (RHDC), located in Houston, Texas, on one occasion received a request to furnish information about the national origin of a United States person and on four occasions received a request to furnish a vessel eligibility certificate signed by other than the owner, master or charterer of the vessel. RHDC failed to report its receipt of these requests to take an action which would have the effect of furthering or supporting a restrictive trade practice or unsanctioned foreign boycott.

The Penalty: On August 11, 2016, RHDC International LLC agreed to pay a civil penalty of $9,000.

Vinmar International, Ltd. / Vinmar Overseas, Ltd.

The Violation: On seven occasions between 2011 and 2012, two related foreign companies with Houston, Texas-based U.S. operations, Vinmar International, Ltd. (VIL) and Vinmar Overseas, Ltd. (VOL), furnished prohibited information in bills of lading or vessel certificates regarding the blacklist status or eligibility status of the vessel to enter Arab ports. On ten occasions between 2009 and 2012, the companies failed to report their receipt of requests from Lebanon, Libya, Oman, Qatar, Syria, and Yemen to furnish a vessel eligibility certificate signed by other than the owner, master or charterer of the vessel. In addition, on three occasions during 2009, VOL failed to report its receipt of a directive from the United Arab Emirates requiring the exclusion of parties of Israeli origin.

The Penalty: On September 25, 2015, VOL agreed to pay a civil penalty of $41,400, and VIL agreed to pay a civil penalty of $19,800.

Baker Eastern, SA (Libya)

The Violation: On 22 occasions during the years 2004 through 2008, Baker Eastern, SA (Libya) (Baker Eastern), a controlled-in-fact foreign subsidiary of Baker Hughes, Inc., furnished to Libyan Customs a certificate of origin that contained two items of prohibited information: first, a negative certification of origin which set out information concerning Baker Eastern's or another person's business relationships with or in a boycotted country; and second, a blacklist certification which set out information concerning Baker Eastern's or another person's business relationships with other persons known or believed to be restricted from having any business relationship with or in a boycotting country. In addition to the 44 violations related to the furnishing of such prohibited information, Baker Eastern committed 22 violations by agreeing to refuse to do business with another person pursuant to a requirement or request from a boycotting country. Specifically, the company included a statement in the certificate of origin regarding compliance with the principles and regulations of the Arab Boycott of Israel. In total, Baker Eastern committed 66 violations of the antiboycott provisions of the EAR.

The Penalty: On June 12, 2013, Baker Eastern, SA (Libya) agreed to pay a civil penalty of $182,325.

Voluntary Self Disclosure: Baker Eastern voluntarily disclosed these transactions to BIS.

TMX Shipping Company, Inc.

The Violation: During the years 2007 through 2010, in connection with transactions involving the sale and/or transfer of U.S.-origin goods to Bahrain, Kuwait, Lebanon and United Arab Emirates, TMX Shipping Company, Inc. (TMX), located in Virginia, on four occasions furnished a statement, signed by other than the owner, master or charterer, certifying that the carrying vessel was eligible to enter, or allowed to enter, the port of destination. In so doing, TMX furnished prohibited information concerning its or another person's business relationships with another person known or believed to be restricted from having any business relationship with or in a boycotting country. In addition, on 11 occasions, TMX received a request to furnish a certification by other than

the owner, master or charterer of the vessel stating that the vessel was allowed to enter certain ports. TMX failed to report its receipt of these requests to take an action which would have the effect of furthering or supporting a restrictive trade practice or unsanctioned foreign boycott.

The Penalty: On October 31, 2013, TMX Shipping Company, Inc. agreed to pay a civil penalty of $36,800.

Laptop Plaza, Inc. (aka IWEBMASTER.NET, Inc.)

The Violation: In 2006, in connection with transactions involving the sale and/or transfer of U.S.-origin goods to Pakistan and Lebanon, Laptop Plaza, Inc. (Laptop), located in California, on four occasions, furnished to its customer an invoice which set out a statement that the goods were not of Israeli origin and did not contain Israeli materials. Furnishing this information is prohibited because the information concerns Laptop's or another person's business relationships with or in a boycotted country. In addition, on three occasions, Laptop failed to maintain records of transactions relating to a restrictive trade practice or boycott for a five-year period, as required by the Regulations.

The Penalty: On September 7, 2013, Laptop Plaza, Inc. agreed to pay a civil penalty of $48,800.

Leprino Foods Company

The Violation: During the years 2009 through 2011, in connection with transactions involving the sale and/or transfer of U.S.-origin goods to consignees in Bahrain, Oman, Qatar and the United Arab Emirates, Leprino Foods Company (Leprino), located in Colorado, on one occasion, furnished a transport certificate, signed by other than the owner, master or charterer, declaring that the ship was permitted to enter the port in Oman, in accordance with the laws of the Sultanate of Oman. By so doing, Leprino furnished prohibited information concerning its or another person's business relationships with another person known or believed to be restricted from having any business relationship with or in a boycotting country. In addition, on 15 occasions, Leprino received a request to take an action which would have the effect of furthering or supporting a restrictive trade practice or unsanctioned foreign boycott. Among these requests were 12 goods directives indicating that products manufactured or produced in Israel were banned. Leprino failed to report its receipt of these requests to engage in a restrictive trade practice or boycott.

The Penalty: On September 16, 2013, Leprino Foods Company agreed to pay a civil penalty of $32,000.

AIX Global LLC

The Violation: In 2008, in connection with a transaction involving the sale and/or transfer of U.S.-origin goods to Iraq, AIX Global LLC (AIX), located in Tennessee, on one occasion agreed to a prohibited condition that the manufacturer must not be a subsidiary of a company included on a list of "Israeli Boycott Companies." By so doing, AIX agreed to refuse to do business with another person, pursuant to an agreement with, a requirement of, or a request from or on behalf of a boycotting country. In the same transaction, AIX furnished prohibited information concerning its or another person's business relationships with another person known or believed to be restricted from having any business relationship with or in a boycotting country. Lastly, AIX, on one occasion, failed to report timely its receipt of requests to take an action which would have the effect of furthering or supporting a restrictive trade practice or unsanctioned foreign boycott.

The Penalty: On September 27, 2013, AIX Global LLC agreed to pay a civil penalty of $15,000 (suspended for six months and thereafter waived, provided AIX committed no violations during the suspension period).

U.S. DEPARTMENT OF COMMERCE
Bureau of Industry and Security
Export Enforcement