

China-Related Export Control Risks

Eric Carlson, Partner, Covington & Burling LLP (Shanghai), ecarlson@cov.com

Peter Lichtenbaum, Partner, Covington & Burling LLP (Washington), plichtenbaum@cov.com

Companies and other parties engaged in dealings with China ignore U.S. trade controls laws and regulations at their peril. U.S. government export control laws and regulations are designed to ensure that transfers of products, software, technology, and services to non-U.S. persons are consistent with U.S. national security and foreign policy goals. Failure to strictly adhere to these laws and regulations can result in severe consequences ranging from fines to suspension of a company's U.S. export privileges to jail time for individuals who willfully violate the law. In recent years, enforcement agencies have increasingly targeted trade controls violations involving China. According to the U.S. Department of Commerce's Assistant Secretary for Export Enforcement, David Mills, the export of goods and technology for unauthorized use in China is a top priority, and China-related criminal investigations are second only to those involving Iran.¹

This article provides background on U.S. trade controls laws and regulations and identifies key risks and protective actions for companies that do business with China.

KEY RISKS

- Classifying items—is a license required?
- Prohibition on exporting defense services to China
- Exporting items for military use
- Avoiding transactions with restricted parties
- Exporting technology: emails, online databases, and shared drives
- Dealing with Chinese nationals inside and outside the company
- Providing customer support
- Complying with export license conditions
- Joint ventures
- M&A
- China's export control regulations

I. Overview of U.S. Export Controls

U.S. trade control laws and regulations control exports, reexports, and in-country transfers of goods, technology, software, and services based on the destination, end-use, and end-user. “Exports” and “reexports” are defined broadly to include physical shipments, cross-border electronic transmissions (such as by email or downloading from a remote computer server), and the disclosure of controlled technology to a non-U.S. citizen or permanent resident even if such transfers occur entirely outside of the United States. Certain restrictions are country-specific due to national security, foreign policy, nonproliferation, or other concerns. Other restrictions apply only to identified parties or where an item would be used for certain end-uses that raise policy or security concerns. Where restrictions apply, items may not be supplied unless the parties involved obtain export licenses from relevant U.S. government agencies. Key U.S. trade controls laws and regulations include:

- The Arms Export Control Act (“AECA”) (22 U.S.C. § 2778) and the International Traffic in Arms Regulations (“ITAR”) (22 C.F.R. Parts 120-130) administered by the Department of State’s Directorate of Defense Trade Controls (“DDTC”);
- The Export Administration Regulations (“EAR,” 15 C.F.R. Parts 730-774) administered by the Department of Commerce’s Bureau of Industry and Security (“BIS”); and
- The trade and economic sanctions programs and regulations (31 C.F.R. Parts 500-598) administered by the Department of the Treasury’s Office of Foreign Assets Control (“OFAC”).

U.S. export controls permit most civil and dual-use goods and services to be supplied to China without a U.S. governmental license. However, certain U.S.-origin goods and technology, and even certain foreign-origin goods and technology containing more than *de minimis* amounts of U.S. content, require licensing before they can be exported to China, even if they are not being exported directly from the United States. At the same time, certain persons and entities in China are prohibited from receiving any item of U.S. origin or containing more than *de minimis* U.S. content. In addition, as discussed in more detail in Part II.C below, the export of certain items for certain military end-uses in China also is prohibited.

Violations of U.S. export control laws and regulations can result in civil penalties of up to \$500,000 per violation under the ITAR and up to \$250,000 per violation under the EAR and under OFAC sanctions. Criminal penalties are up to \$1 million and 20 years in prison, or both. In addition, violators may face debarment and/or be denied export privileges. These penalties may be imposed on any entity—whether U.S. or non-U.S.—that deals in (i) U.S.-origin goods; (ii) foreign-made products or technology that include more than *de minimis* amounts of controlled U.S.-origin content; or (iii) foreign-made direct products of sensitive U.S.-origin technology. The U.S. regulatory agencies also may hold U.S. parents responsible for the actions of non-U.S. subsidiaries and owned or controlled affiliates and joint ventures.

II. Key China-Related Risks

A. Classifying Items: Is a License Required?

Determining the proper jurisdiction and classification of goods, technology, software, and services is essential to understanding which U.S. government agency regulates their export, transfer, reexport, and retransfer, and which export controls apply. A company that fails to properly classify its products may inadvertently export items to China without the required license.

For example, in a consent agreement published in June 2012, United Technologies Corp. (“UTC”) and its subsidiaries acknowledged that they had failed to properly establish the jurisdiction of defense articles and technical data exported to China to support the design and development of a military attack helicopter. Specifically, a UTC U.S. subsidiary supplied software to operate an engine control system for engines which were ultimately used in the Chinese military helicopters prototypes, but UTC entities failed to recognize that the modification subjected the software to ITAR controls. UTC and its subsidiaries agreed to pay more than \$75 million in penalties and implement remedial compliance measures imposed by the State Department and the Department of Justice, including a requirement that UTC appoint a Special Compliance Officer to monitor, oversee, and promote its export compliance efforts.²

Exporters may self-classify their products—i.e., determine on their own the proper export classification of their products—without consulting U.S. government regulators. In addition, exporters can ask relevant government agencies (the State Department for defense articles, defense services, and related technology controlled under the ITAR, and the Commerce Department for dual-use goods controlled under the EAR) to classify products for them. Companies also can seek government classification where the classification is unclear, or if the exporter requires documentation to support an export classification determination.

B. Prohibition on Exporting Defense Articles to China

The U.S. government maintains a comprehensive arms embargo against China. A company that exports to China articles that the U.S. government has designated as “defense articles” or related technical data or services, violates the ITAR and faces potential civil penalties, criminal fines, and debarment. As discussed above, UTC agreed to pay more than \$75 million in penalties after a subsidiary exported modified software subject to ITAR control to China.

Defense articles are identified on the U.S. Munitions List (“USML”) and include, notably, many sophisticated electronics-, satellite- and space-related items. For example, Zhao Wei Zhang was sentenced to time served and three years of supervised release after pleading guilty to conspiring to export dynamically tuned gyroscopes, which could be used in tactical missile guidance and unmanned aircraft systems, from the United States to China without a license.³

In addition, the USML includes certain parts and components that are used in defense articles. For example, in September 2013, Zhen Zhou Wu received a sentence of 84 months in prison for conspiring over a 10-year-period to illegally export to China military and sophisticated electronics including Commerce Department-controlled electronics components with military applications such as electronic warfare, military radar, and satellite communications systems. Several Chinese military entities received the equipment, which was used in military phased array radar, electronic warfare, and missile systems. After serving his sentence, Wu also will be subject to deportation to China.⁴

Because the U.S. government defines “export” broadly, a party may violate the ITAR any time defense articles or related technical data are transferred outside of the United States, even if the party did not actually transfer those articles or technical data to any foreign persons. For example, the Sixth Circuit found that Professor J. Reece Roth violated the ITAR simply by carrying ITAR-controlled data on his laptop during a trip to China.⁵ Whether or not Professor Roth ever opened or accessed the technical data while he was in China was considered irrelevant. Professor Roth was sentenced to 48 months in prison.⁶

The prohibition on providing defense articles to China impacts both shipments of goods and intangible transfers to Chinese nationals in China or in the United States. For example, Chinese R&D facilities may not receive access—even theoretical access—to databases or networks that contain ITAR-controlled technical data or specifications. See Part II.F below.

Under the Obama Administration’s Export Control Reform initiative, many USML items have been transferred to the Commerce Control List under the EAR. However, these formerly USML items are mostly classified in control categories, principally the “600-series” controls, that are not authorized for export to China.

C. Exporting Items for Military Use: China Military Rule

Under the China Military Rule, the U.S. government prohibits the supply of certain civil or dual-use items that are subject to the EAR⁷ to China if the exporter knows or has reason to know that the item is intended for a “military end-use” in China.⁸ Knowledge is defined broadly to include “not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence.”⁹ Awareness can be inferred from evidence of a conscious disregard of facts or from a person’s willful avoidance of facts.¹⁰ As a result, a party that provides a designated item to a customer with ties to the Chinese military runs the risk of being deemed to have had “knowledge” that the item is being acquired for a military end-use.

Because many Chinese entities engage in both military and commercial activities, making judgments about the nature of a transaction can be difficult. Parties should consider precautions, such as conducting extra due diligence on customers to determine military ties, obtaining information regarding the customer’s intended application of a requested item, and confirming that the intended end-use is legitimate.

D. Avoiding Transactions with Restricted Parties

The U.S. government maintains several denied/restricted party lists of U.S. and foreign persons and entities that have been identified as threats to U.S. national security, as supporting terrorist activities, as associated with criminal organizations, or who the U.S. government otherwise wants to restrict from trading with U.S. persons and/or from trading in U.S.-origin items. These lists include the [Debarred Parties List](#), the [Denied Persons List](#), the [Entity List](#), the [Nonproliferation Sanctions List](#), the [List of Specially Designated Nationals and Blocked Persons](#), and the [Unverified List](#). A number of China-based parties, including significant commercial entities and their affiliates, are on these lists.¹¹ Further, if a Specially Designated National owns, directly or indirectly, at least a 50 percent interest in an entity, then the entity is treated as if it were listed. (This policy does not apply to companies listed on the Entity List, however, according to a recent clarification by the Commerce Department.) Note that these lists are not available in Chinese-language versions, which can make accurate screening a challenge.

In December 2012, Xun Wang, the former Managing Director of PPG Paints Trading (Shanghai) Co., Ltd., a wholly-owned Chinese subsidiary of U.S.-based PPG Industries, Inc., was sentenced to one year in prison for conspiring to export, reexport, and transship high-performance epoxy coatings from the United States, through China, to a Pakistani party identified on the Entity List. Ms. Wang also was ordered to pay \$300,000 in administrative and civil penalties and to perform 500 hours of community service.¹² PPG Paints Trading and a major Chinese company, China Nuclear Industry Huaxing Construction Co., Ltd., also pled guilty in the same matter and each company paid substantial civil and criminal fines.

U.S. companies should conduct due diligence on all parties to a transaction whose information they obtain for business purposes. Where U.S. companies work with distributors, they should ensure that the distributors are aware of and agree to abide by U.S. limitations on doing business with restricted parties. U.S. companies should follow up on any red flags that distributors are not abiding by these restrictions.

E. Exporting Via Technology: Emails, Online Databases, Shared Drives, and the Cloud

U.S. export control regulations govern transfers of technology, including (i) the physical shipments or transfer of technology; (ii) cross-border electronic transmissions, including phone conversations, email, or downloads from a remote computer server; (iii) transfers of technical data subject to U.S. jurisdiction from one non-U.S. business unit to another non-U.S. business unit; and (iv) transfers of technical data subject to U.S. jurisdiction to a third party, including subcontractors. U.S. export controls may apply even to transfers that occur between two parties both located within China.

Providing a Chinese business partner or subsidiary with access to U.S.-origin technology (including build-to-print specifications or technical diagrams) may require a license, even if a U.S. entity owns the facility, or the product being manufactured in China will be shipped exclusively back to the United States. For example, in October 2013, Precision Image Corporation was fined \$300,000 and its owner, Chih-Kwang Hwa, was sentenced to four months in prison and six months of home detention, with two years of supervised release, for exporting to Taiwan ITAR-controlled technology. Hwa obtained contracts from the U.S.

Navy worth approximately \$180,000 to supply circuit boards by falsely claiming the boards would be manufactured in the United States when they were actually being manufactured in Taiwan.¹³

Emailing controlled technology to foreign persons, including foreign person employees, or allowing them to access (even theoretically access) controlled technology through online databases or shared drives also would be considered an export. This means that parties that employ Chinese nationals and other personnel located in China may risk violating U.S. law by providing such parties with access to global R&D resources.

While no license is needed to transfer technology that is “publicly available” or in the “public domain,” an export license often is required to transfer technology, including technical data, to China. Parties that export technology, provide technical support to China, provide parties in China with access to technological specifications through the intranet or networks (including the cloud), and/or travel to China to assist customers, run the risk of violating U.S. law if they do not first obtain the necessary licensing. For example, ArvinMeritor, Inc. was assessed a \$100,000 civil penalty for engaging in the unlicensed export to China and other countries of technical drawings controlled for national security reasons.¹⁴ In an unrelated incident, Zhaoxin Zhu of Shenzhen, China was sentenced to two years in prison and three years’ supervised release for conspiring to purchase controlled satellite and radar technology for export to China.¹⁵

F. Dealing with Chinese Nationals Inside and Outside the Company: Deemed Exports and Reexports

An export to a Chinese national—wherever that person is located—is considered an export to China. An export license may be required to disclose technology or software source code to Chinese nationals, including those working at U.S. companies. For example, for failing to comply with U.S. export control laws, including failing to obtain export licenses that were required to transfer controlled technology to Chinese nationals who worked at Suntek Microwave, Inc. in the United States, Suntek was assessed a \$275,000 civil penalty, and Suntek’s president was individually assessed a \$187,000 civil penalty. Each party also was assessed a 20-year denial of export privileges. In related criminal proceedings, Suntek agreed to pay a \$339,000 criminal fine and Suntek’s president was sentenced to 12 months in prison.¹⁶

These types of exports to foreign nationals located in the United States are referred to as “deemed exports” because the technology or source code is deemed to be exported to the home country of the non-U.S. person. Similarly, a transfer of U.S.-origin technology to a Chinese national working at a Singaporean company in Singapore is considered a deemed reexport to China.¹⁷ This means that if a third-country party employs a Chinese national who will have access to U.S. proprietary technology, that party may be required to obtain a “deemed reexport” license authorizing transfer to the Chinese employee. BIS reports that almost 60% of the deemed export licenses that it processes are for Chinese nationals.¹⁸

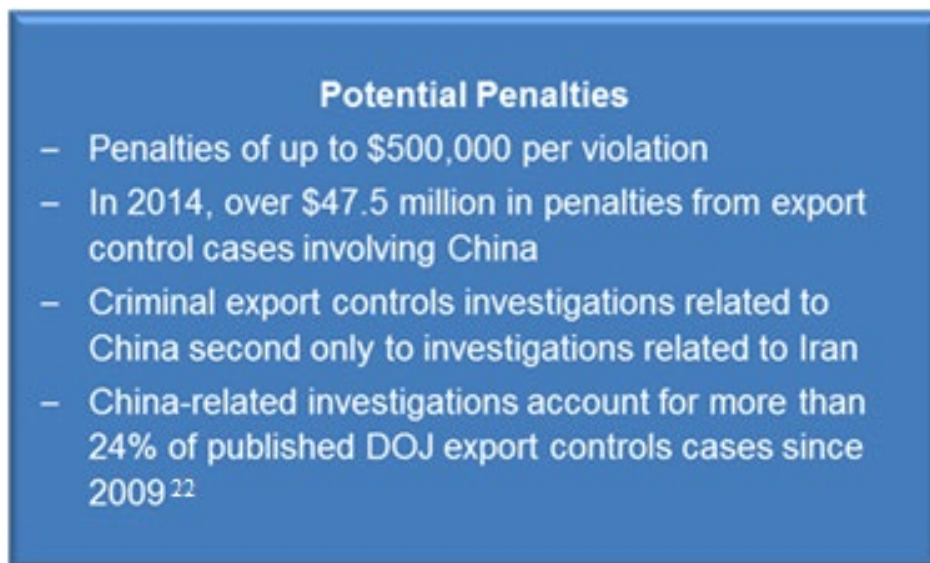
Even once licensing is obtained, companies should carefully monitor employees’ access to controlled technology. Sixing Liu, aka “Steve Liu,” a native of China with a PhD in electrical

engineering who worked as a senior staff engineer for a division of L-3 Communications, was sentenced to 70 months in prison for exporting sensitive U.S. military technology to China, stealing trade secrets, and lying to federal agents. Liu stole thousands of electronic files detailing the performance and design of guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles. Liu had received training on U.S. export control laws and knew that most of his employer's products were covered by those laws. Nonetheless, he allegedly stole the files to better position and prepare himself for future employment in China.¹⁹

G. Providing Customer Support

In addition to controlling the export of hardware and technology, U.S. export controls and economic sanctions also govern the provision of services to non-U.S. parties. As a result, even companies that provide technical support or other customer services should be careful to avoid inadvertently providing technology to customers in China without the necessary authorization.

In addition, the U.S. government's arms embargo against China prohibits the provision of "defense services" to Chinese persons.²⁰ U.S. persons who provide Chinese parties technical support related to defense articles—even foreign defense articles—run the risk of engaging in unauthorized defense services. For example, Hughes Network Systems and DIRECTV Group (collectively, "HNS"), both U. S. companies, were assessed a \$5 million civil penalty for providing services and support to Chinese and other military customers to help resolve technical problems associated with the customers' use of HNS products connected to foreign military equipment.²¹



Potential Penalties

- Penalties of up to \$500,000 per violation
- In 2014, over \$47.5 million in penalties from export control cases involving China
- Criminal export controls investigations related to China second only to investigations related to Iran
- China-related investigations account for more than 24% of published DOJ export controls cases since 2009²²

H. Complying with Export License Conditions

Under certain circumstances, the U.S. government may issue licenses that authorize the otherwise-prohibited supply of goods, technology, software, or services. Licenses impose

various conditions subject to which authorized transactions may occur. While conditions vary by license, common conditions prohibit the resale, transfer, or reexport of items on the license without prior authorization from the U.S. government and require that (i) only licensed parties be involved in the transactions; (ii) the product be used for the stated end-use only; (iii) the applicant verify delivery and installation; (iv) other parties be informed of all license conditions; (v) there be no military end-users or end-uses; and (vi) there be no nuclear, chemical, biological, or missile related end-users or end-uses.

Violating a license condition is considered an export violation. For example, Western Geophysical Company of America and WesternGeco LLC agreed to pay \$925,000 and \$1,965,600, respectively, for violating conditions on export licenses for underwater geophysical mapping equipment exported to China.²³

Companies should implement policies and procedures, including technology control plans, to ensure that items sent to China comply with all applicable export conditions.

I. Joint Ventures: Even Chinese JVs May Be Subject to U.S. Export Controls

U.S. parent companies and the U.S. Government generally expect a joint venture (“JV”) that is more than 50 percent owned or controlled by a U.S. person or entity to follow the same export control compliance practices and procedures that U.S. businesses follow. This may be the case even if the JV is incorporated in China. Applicable compliance procedures may include: (i) designating one or more persons to be responsible for oversight of export controls compliance; (ii) establishing an export controls compliance program, including written procedures for ensuring compliance with U.S. export controls laws and regulations; (iii) following appropriate screening procedures; (iv) implementing a technology control plan to ensure that goods, technical data, software, and services are not transferred without authorization; (v) following adequate recordkeeping and reporting procedures; and (vi) instituting training programs. U.S. JV partners also may require periodic audits of the JV’s compliance with U.S. export control and economic sanctions laws.

J. M&A: Buying a Company Means Buying Its Export Control Problems

Under legal theories of successor liability, the Departments of State, Commerce, and Treasury all take the position that companies may be held liable for trade controls violations committed by companies from which they acquire stock or assets. The U.S. Department of Commerce’s Office of Export Enforcement first asserted a theory of successor liability in a matter involving Sigma-Aldrich Corp. in November 2002. In that settlement, Sigma-Aldrich and two of its subsidiaries agreed to pay a \$1.76 million fine to settle charges arising from the unauthorized export of biological toxins made by a company in which Sigma-Aldrich later acquired a partnership interest and assets.²⁴ Similarly, in 2003 Boeing Corporation and Hughes Space and Communications jointly paid a \$32 million fine for violations committed by Hughes before it was acquired by Boeing.²⁵

As a result, U.S. companies would do well to conduct appropriate due diligence prior to an acquisition, divestment, or entering into a joint venture relationship to identify the scope of

any prior violations and penalties, as well as foreseeable future expenditures that may be necessary to bring a newly acquired entity's import/export program into line with U.S. export control laws and regulations.²⁶ Chinese companies entering into such transactions with U.S. companies may not be prepared for this due diligence.

Conversely, many Chinese companies are acquiring U.S. firms, and export control issues can arise there as well. Depending on the information that is reviewed as part of an acquisition or divestment, a Chinese national conducting diligence on a U.S. company that deals in controlled goods, technology, or software may be required to obtain a license to review certain technical materials. In addition, if a Chinese company invests in a U.S. company, items requiring a license for export to China still would require a license, even if the Chinese company has full or partial legal ownership of the goods, software, or technology.

K. China Export Controls

In addition to U.S. export controls, China regulates certain exports and some imports based on economic quotas, policy decisions, international agreements, and national security considerations. China also implements U.N. Security Council resolutions that apply sanctions against countries, entities, and individuals. Finally, Chinese regulations related to state secrets and commercial encryption products restrict the import and export of certain products and technology.

III. Protective Actions

Companies that supply goods, software, or technology to China or whose employees travel to China should take precautions to adhere to trade controls laws and regulations. In addition to the standard procedures of classification, customer screening, and developing technology control plans, our clients are emphasizing the following:

- Conducting a China-focused risk assessment. Prioritizing compliance efforts and resources based on a risk assessment that takes into account, at a minimum: (i) the nature of any compliance matters or other deficiencies that have been identified; (ii) the jurisdiction and classification of the company's products; and (iii) the volume of the company's exports. Benefits from a risk assessment including: (1) identifying issues or gaps before they result in a new or additional violation; (2) make adjustments to account for changes in product lines, business models, and employees; (3) show good faith to U.S. regulators if an issue does occur; and (4) emphasize internally the importance of these issues by committing resources to them.
- Implementing policies and procedures to address the China Military Rule. Companies that do business with Chinese parties should determine whether any of their products, software, or technology are subject to the China Military Rule. If any item is so subject, companies should consider (i) conducting additional due diligence on customers to determine military ties; (ii) obtaining information regarding how and where the customer intends to use the requested items; and (iii) confirming the legitimacy of the intended end-use.

- Screening customers and conducting due diligence, mindful of linguistic nuances. Companies should screen customers, suppliers, vendors, freight forwarders, banks, and other parties against U.S. watchlists prior to engaging in transactions. Because the U.S. government does not make Chinese-language versions of its lists available, names will need to be properly translated or romanized to be screened effectively.
- Implementing policies on travel to/from China. Because of the significant potential risks associated with inadvertently traveling to China with controlled technical data or technology, many U.S. companies have implemented policies requiring employees traveling to China to travel with a clean loaner laptop, phone, tablet, and/or other storage device(s) borrowed from the IT department.
- Training. Training to employees on both sides of the Pacific to avoid inadvertent errors. In China, ensure training is conducted in Chinese by a qualified trainer who knows the nuances of U.S. export control regulations. Training should also have an ethics dimension to ensure that corporate values are well understood.
- Assigning dedicated export compliance staff in China. Deploying staff on-the-ground in China can help ensure that the often complex U.S. export controls and economic sanctions regulatory regimes are appropriately translated into reasonable policies and procedures that ensure compliance with the law without unnecessarily restricting business opportunities. This may be particularly important if the company has a joint venture with a Chinese company. If China operations do not warrant a full-time expert, consider designating in China as a part-time “export compliance ambassador” or “export compliance champion” to serve as a single point of contact for these issues, and provide additional training to that person.

¹ U.S. Department of Commerce Bureau of Industry and Security, Keynote Speech of David W. Mills, Assistant Secretary for Export Enforcement UPDATE Conference, July 30, 2014, *available at* <https://www.bis.doc.gov/index.php/about-bis/newsroom/speeches/148-about-bis/newsroom/speeches/speeches-2014/719-keynote-speech-of-david-w-mills-assistant-secretary-for-export-enforcement-update-conference-july-30-2014>.

² U.S. Department of State Bureau of Political-Military Affairs Consent Agreement with United Technologies Corporation (June 19, 2012), *available at* http://www.pmdtc.state.gov/compliance/consent_agreements/pdf/UTC_CA.pdf

³ “Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases,” Department of Justice, Aug. 2015, *available at* <http://www.pmdtc.state.gov/compliance/documents/OngoingExportCaseFactSheet.pdf>.

⁴ *Id.*

⁵ *U.S. v. Roth*, 628 F.3d 827 (6th Cir. 2011).

⁶ “Former University of Tennessee Professor John Reece Roth Sentenced to 48 Months in Prison for Illegally Exporting Military Research Technical Data,” U.S. Federal Bureau of Investigation, Knoxville Division Press Release, July 1, 2009, *available at* <http://www.fbi.gov/knoxville/press-releases/2009/kx070109.html>.

⁷ Covered items include certain aircraft, avionics, computers, cameras, and telecommunications equipment. Impacted items are identified in Supplement No. 2 to Part 744 of the EAR.

⁸ “Military end-use” is defined in EAR § 744.21 as (i) incorporation into a military item described on the U.S. Munitions List (USML) or Wassenaar Arrangement Munitions List; (ii) incorporation into items listed under

ECCNs ending in “A018” on the CCL in Supplement No. 1 to Part 774 of the EAR; (iii) for the “use”, “development”, or “production” of military items described on the USML or the International Munitions List, or items listed under ECCNs ending in “A018” on the CCL; or (iv) “deployment” of items classified under ECCN 9A991 as set forth in Supplement No. 2 to Part 744.

⁹ 15 C.F.R. § 772.1.

¹⁰ *Id.*

¹¹ For instance, a Chinese company was added to the Entity List in April 2015 for transshipping U.S.-origin items to Iran via China. Addition of Certain Persons to the Entity List, Bureau of Industry and Security, U.S. Department of Commerce Federal Register Notices 2015, April 23, 2015, *available at* <http://bis.doc.gov/index.php/regulations/federal-register-notices#FR22638>.

¹² “Former Managing Director of PPG Paints Trading (Shanghai) Co., Ltd., Sentenced to Year in Prison for Conspiring to Illegally Export High-Performance Coatings to Nuclear Reactor in Pakistan,” U.S. Department of Justice Press Release, Dec, 20, 2012, *available at* <https://www.bis.doc.gov/index.php/2011-09-13-13-22-03/98-about-bis/newsroom/press-releases/press-releases-2012/483-ppg-paints-trading-shanghai-co-ltd-sentenced-to-a-year-in-prison-export-to-pakistan>.

¹³ “Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases,” Department of Justice, Aug. 2015, *available at* <http://www.pmdtc.state.gov/compliance/documents/OngoingExportCaseFactSheet.pdf>.

¹⁴ Order Relating to ArvinMeritor, Inc. (March 22, 2011), *available at* http://efoia.bis.doc.gov/index.php/component/docman/doc_view/594-e2202?Itemid=f.

¹⁵ “Don’t Let This Happen to You! An Introduction to U.S. Export Control Law, Actual Investigations of Export Control and Antiboycott Violations,” U.S. Department of Commerce, Bureau of Industry and Security (Sept. 2010) at 19, *available at* https://www.bis.doc.gov/index.php/forms-documents/doc_view/535-don-t-let-this-happen-to-you.

¹⁶ “Don’t Let This Happen to You! Actual Investigations of Export Control and Antiboycott Violations,” U.S. Department of Commerce, Bureau of Industry and Security (July 2008) at 22, *available at* https://www.bis.doc.gov/index.php/forms-documents/doc_view/152-don-t-let-this-happen-to-you; “Suntek Microwave, Inc. and Company President Settle Charges of Illegal Exports,” U.S. Department of Commerce Press Release, May 6, 2004, *available at* <http://www.bis.doc.gov/news/2004/sunteckmay04.htm>.

¹⁷ In July 2012, BIS imposed a \$110,000 civil penalty on Technetics Group Singapore Ptd. for transferring controlled technology to Chinese nationals working for the company in Singapore. See Order Relating to Technetics Group Singapore Pte. Ltd. (July 24, 2012), *available at* http://efoia.bis.doc.gov/index.php/component/docman/doc_view/788-e2276?Itemid=f.

¹⁸ See Deemed Exports and I-129 Forms, Update 2011.

¹⁹ “Former Employee of New Jersey Defense Contractor Sentenced to 70 Months in Prison for Exporting Sensitive Military Technology to China,” U.S. Department of Justice Press Release, Mar. 25, 2013, *available at* <http://www.justice.gov/usao/nj/Press/files/Liu,%20Sixing%20Sentencing%20News%20Release.html>.

²⁰ Defense services are defined broadly to include “[t]he furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles.” 22 C.F.R. § 120.9.

²¹ Order in the Matter of The DIRECTV Group Inc. Hughes Network Systems Inc. (Jan. 26, 2005), *available at* http://www.pmdtc.state.gov/compliance/consent_agreements/pdf/DirectTV_Order.pdf ; Draft Charging Letter, Investigation of the DIRECTV Group, Inc. and Hughes Network Systems, Inc., *available at* http://www.pmdtc.state.gov/compliance/consent_agreements/pdf/DirectTV_DraftChargingLetter.pdf.

²² “Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases,” Department of Justice, Aug. 2015, *available at* <http://www.pmdtc.state.gov/compliance/documents/OngoingExportCaseFactSheet.pdf>.

²³ “Don’t Let This Happen to You! An Introduction to U.S. Export Control Law, Actual Investigations of Export Control and Antiboycott Violations,” U.S. Department of Commerce, Bureau of Industry and Security (Sept. 2010) at 23, *available at* https://www.bis.doc.gov/index.php/forms-documents/doc_view/535-don-t-let-this-happen-to-you.

²⁴ “U.S. Corporation Fined for Biological Toxins Export,” U.S. Department of State Bureau of International Information Programs, Nov. 4, 2002, *available at*

<http://iipdigital.usembassy.gov/st/english/texttrans/2002/11/20021104152523odessey@pd.state.gov0.1797296.html#axzz3yGe6uquq>.

²⁵ Order in the Matter of Hughes Electronics Corporation Boeing Satellite Systems, Inc. (March 4, 2003), *available at*

https://www.pmdtc.state.gov/compliance/consent_agreements/pdf/HughesElectronic_Order.pdf.

²⁶ A thorough trade controls due diligence review could examine the target's (i) international footprint and compliance practices, including product, technology, and software jurisdiction and classification; and (ii) exports, including physical shipments, technology exchanges, deemed exports, and the provision of defense services. The review might encompass the target and any subsidiaries, operating divisions, branches, business units and controlled joint ventures involved in the transaction. Joint ventures in which the target holds a minority or non-controlling interest also may be considered.