ALMAR WATER SOLUTIONS B.V.

GLOBAL SANCTIONS AND EXPORT CONTROLS POLICY

Revision 2 - Adopted September 28, 2022

Mission Statement

Almar Water Solutions, B.V. and its subsidiaries (collectively, "ALMAR" or the "Company") are committed to adhering to all applicable financial and economic sanctions and export controls ("Sanctions and Export Controls"). Specifically, the Company is committed to ensuring compliance with all applicable Sanctions and Export Control laws and regulations of the United States, European Union, Spain, the United Kingdom, Canada, Australia, and other jurisdictions in which the Company operates (collectively, the "Sanctions and Export Control Laws"), to the extent permissible under local law.[1] This Global Sanctions and Export Controls Policy (this "Policy") is intended to facilitate the Company's compliance with the Sanctions and Export Control Laws and to reduce reputational, operational, and legal risks that could arise from a potential breach of such laws.

The Company expects all of its directors, officers, and employees to comply with the terms of this Policy at all times. Although employees are not expected to master the Sanctions and Export Control Laws, it is important that employees know when to seek advice from supervisors or other appropriate persons. If you do not understand a provision of this Policy or are confused as to what actions you should take in a given situation, you should contact your supervisor or the Compliance Lead. If you wish to report a possible violation of the law or this Policy, you should follow the procedures referenced below.

Failure to comply with the Sanctions and Export Control Laws may result in civil, administrative, and criminal penalties, including, but not limited to, freezing or blocking of assets, monetary fines, damage to the Company's reputation or a limitation of the Company's business activities. Violations can also result in civil, administrative, and criminal penalties against the director, officer, or employee that engaged in the prohibited activity, and may include fines or even imprisonment. Failure to comply with this Policy or with the Sanctions and Export Control Laws is grounds for disciplinary action up to and including termination.

[1] Certain jurisdictions, such as the European Union and United Kingdom, have adopted blocking statutes that prohibit adherence to certain U.S. sanctions. If you encounter such a conflict, or if a local law conflicts with a requirement set forth in this Policy, you should consult with the Compliance Lead to determine the appropriate course of action.

Overview of the Company's Sanctions and Export Control Compliance Program

The Sanctions and Export Control Compliance Program consists of this (1) Policy, (2) the procedures implementing this Policy (including relevant sections of the Company's Third Parties Relationships Protocol), and (3) the appendices to this Policy:

Appendix 1: Restricted and High-Risk Jurisdictions
Appendix 2: Overview of U.S. Sanctions and Export Control Laws
Appendix 3: Overview of EU Sanctions and Export Control Laws
Appendix 4: Overview of UK Sanctions and Export Control Laws
Appendix 5: Overview of Australian Sanctions and Export Control Laws
Appendix 6: Other Sanctions Regimes

The Sanctions and Export Control Compliance Program is designed to provide for ongoing compliance with the Sanctions and Export Control Laws by:

- assigning responsibility for coordinating and monitoring the Sanctions and Export Control Compliance Program to the Compliance Lead;
- establishing a system of internal controls to comply with the Sanctions and Export Control Laws;
- providing for ongoing training of appropriate personnel; and
- conducting risk-based periodic reviews of the Sanctions and Export Control Compliance Program as described below.

Roles and Responsibilities

Senior Management

The Board has approved this policy and the Executive Committee is responsible for overseeing the implementation of the Sanctions and Export Control Compliance Program. In addition, management is responsible for designating a qualified employee to serve as the Compliance Lead for Sanctions and Export Controls compliance. Senior management is responsible for ensuring that the Board of Directors, or a designated committee of the Board, as appropriate, receives periodic reports regarding the adequacy and effectiveness of the Sanctions and Export Control Compliance Program.

Business Operations

The Chief Operations Officer and the Chief Business and Development Officer are the first line of defense and have primary responsibility for operating in a lawful and ethical manner, in accordance with Sanctions and Export Control Laws and this Policy. The Chief Operations Officer and the Chief Business and Development Officer shall not violate Sanctions and Export Control Laws or assist or facilitate persons seeking to violate Sanctions and Export Control Laws and shall identify and escalate possible violations.

Compliance Lead

The Compliance Lead is responsible for coordinating and monitoring the Company's day-to-day compliance with this Policy and the Sanctions and Export Control Laws. The Compliance Lead may perform the following tasks, amongst others, in coordination as appropriate with other Company departments:

- providing guidance to management and the relevant business and operations areas on compliance with the Sanctions and Export Control Laws;
- apprising management of ongoing compliance with the Sanctions and Export Control Laws and carrying out the directions of senior management and the Board of Directors with respect to Sanctions and Export Control matters;
- escalating potential breaches of Sanctions and Export Control Laws to management;
- monitoring legal and regulatory developments and best practices with respect to Sanctions and Export Control Laws;
- recommending changes to the Sanctions and Export Control Compliance Program based on such developments;
- communicating updates to the Sanctions and Export Control Compliance Program to management and all employees;
- developing and administering Sanctions and Export Control training for designated personnel;
- filing any reports that may be required by the Sanctions and Export Control Laws; and
- ensuring compliance with all applicable Sanctions and Export Control recordkeeping requirements.

The current Compliance Lead is the Corporate Assurance Director.

Approach to Business with Sanctioned Jurisdictions and Persons

To minimize the Company's exposure to legal, compliance, and reputational risks – not only with respect to Sanctions and Export Controls but also money-laundering, corruption, and other illicit activity – **it is the Company's policy not to conduct or pursue any business with, in or involving a "Restricted Jurisdiction" (currently, Cuba, Iran, North Korea, Syria, and the Crimea, so-called Donetsk People's Republic and so-called Luhansk People's Republic regions of Ukraine) or any "Prohibited Person" even if such business is not prohibited under applicable law. "Prohibited Person"** means (i) any person (individual or entity) that is subject to U.S., EU, Spanish, or UK blocking sanctions (i.e., asset-freezing sanctions) or (ii) any person located or resident in or established under the laws of any Restricted Jurisdiction.

Any business involving other High-Risk Jurisdiction must be approved before any such business is initiated. It is the Company's policy not to conduct business with, in, or involving any High-Risk Jurisdictions (for a list of High-Risk Jurisdictions, see Appendix 1), including any person located or resident in or established under the laws of a High-Risk Jurisdiction, without prior approval from the Corporate Assurance Director.

Any business with a High-Risk Person must be approved before any such business is initiated. "High-Risk Person" means (i) any person located or resident in or established under the laws of a High-Risk Jurisdiction, (ii) persons subject to U.S., EU, Spanish, or UK sanctions other than blocking sanctions (for example, persons subject to U.S. sectoral sanctions under Executive Order 13662 or EU sectoral sanctions under Council Regulation (EU) 833/2014, as amended), and (iii) persons identified on U.S. restricted lists identified on the U.S. International Trade Administration's Consolidated Screening List, including persons identified on the Department of Commerce's Entity List or Denied Persons List or the Department of State's Debarred List. The Compliance Lead will not approve any business with a High-Risk Person unless he or she has determined, upon careful review, that such business would not violate any applicable Sanctions and Export Control Laws and would not raise other significant compliance or reputational risks.

Due Diligence

Due diligence related to Sanctions and Export Control Laws must be performed to ensure that ALMAR counterparties, including ALMAR customers/clients, joint venture partners, agents, contractors and their supply chains (pursuant to the procurement compliance process that has been established), sponsors, suppliers and consultants, representatives, other intermediaries or other persons who act on behalf or for the benefit of ALMAR are bona fide and legitimate entities and that the Company is permitted to do business with them under this Policy. Diligence should be tailored to the particular Sanctions and Export Control risks of the situation. Diligence should be enhanced if a counterparty is located in or established in a High-Risk Jurisdiction or there are reasons to suspect improper activity. *See Third Parties Relationships Protocol for additional information regarding the Company's Sanctions and Export Control diligence procedures.*

The Company employees should seek advice from the Corporate Assurance Director in the following circumstances:

- There is reason to suspect, based on due diligence or otherwise, that:
  - a transaction involves, directly or indirectly: (i) a Prohibited or High-Risk Person (or anyone acting on their behalf), (ii) an entity owned or controlled by a Prohibited Person or High-Risk Person, or (iii) a Restricted or High-Risk Jurisdiction;
  - a third party or proposed transaction demonstrates one or more indicators of suspicious or improper activity, examples of which are provided in the Third Parties Relationships Protocol.
- There is reason to believe that a license is required for the export of Company products or associated materials;
- The Company is faced with applicable laws of different nations that conflict; or
- An employee otherwise has questions or concerns regarding a potential transaction.

Reporting and Recordkeeping

The Company will timely file any reports that it is required to file under the Sanctions and Export Control Laws such as reports of blocked/frozen property or reports of rejected transactions. All records related to the Sanctions and Export Control Laws must be retained for at least five (5) years from the date of the transaction and be readily retrievable for examination or upon request. If applicable Sanctions and Export Control Laws prescribe a longer record-keeping period, the Company will follow that longer period.

Escalation of Sanctions and Export Control Compliance Concerns

Consistent with the Company's Code of Conduct, directors, officers and employees are responsible for reporting any perceived violations of this Policy or any Sanctions and Export Control Laws. For additional information, please see Section 21 of the Company's Code of Conduct: Reporting Obligations.

Training

Corporate Assurance will provide training to employees whose job responsibilities are within the scope of the Sanctions and Export Control Laws at onboarding and on an annual basis. Where changes occur in Sanctions and Export Control Laws more frequently, targeted training sessions will be held on these updates as required. Corporate Assurance shall maintain records of training materials and employee attendance at training sessions.

Compliance Program Review and Testing

The Company performs risk-based testing of its Sanctions and Export Control Compliance Program. The testing shall be performed in the same manner as compliance audits conducted by the Company. The Compliance Lead will determine, on a risk basis, the frequency of such testing. The results of such reviews shall be reported to senior management and the Board of Directors.

Risk Assessment

The Company performs a periodic risk assessment to assess and control the Company's Sanctions and Export Control risk profile. Understanding the Sanctions and Export Control risk profile enables Senior Management to evaluate the nature and quantity of Sanctions and Export Control risks, to appropriately adjust the control environment to mitigate identified gaps and to make risk management judgments as to the acceptability of the identified risks.

Policy Review and Update

This Policy shall be reviewed and updated by the Compliance Lead (and subject to board approval where appropriate) periodically as warranted by changes to the Sanctions and Export Control Laws and the Company's risk assessment. Every time the Policy is updated, it shall be distributed to relevant employees and, as appropriate, representatives.

Contacts

Company employees and representatives may contact the Compliance Lead with all questions or concerns related to this Policy.

APPENDIX 1 RESTRICTED AND HIGH-RISK JURISDICTIONS (AS OF JUNE 22)

Country	Risk
Jurisdictions Subject to Comprehensive Sanctions ("Restricted Jurisdictions")	
Crimea region	Restricted
Cuba	Restricted
Donetsk region	Restricted
Iran	Restricted
Korea, North	Restricted
Luhansk region	Restricted
Syria	Restricted
High-Risk Jurisdictions Subject to More Limited Sanctions	
Afghanistan	High
Belarus	High
Burma	High
Burundi	High
Central African Republic	High
China	High
Congo, Democratic Republic of the	High
Ethiopia	High
Iraq	High
Lebanon	High
Libya	High
Mali	High
Nicaragua	High
Russia	High
Somalia	High
South Sudan	High
Sudan	High
Ukraine	High
Venezuela	High
Yemen	High
Zimbabwe	High
Other "High Risk" Countries	
Armenia	High
Turkey	High
United Arab Emirates	High

APPENDIX 2

OVERVIEW OF U.S. SANCTIONS AND EXPORT CONTROL LAWS

U.S. SANCTIONS

(a) Background on U.S. Sanctions

In the United States, the Office of Foreign Assets Control ("**OFAC**") administers economic restrictions and trade sanctions against targeted non-U.S. countries, organizations, and individuals based on U.S. foreign policy and national security goals. The "**U.S. Sanctions**" laws and regulations administered by OFAC generally prohibit or restrict transactions involving specified countries or groups, entities, and individuals, which are listed on OFAC's Specially Designated Nationals List (the "**SDN List**"), the Sectoral Sanctions Identification List (the "**SSI List**"), or the Foreign Sanctions Evaders List (the "**FSE List**") or other lists maintained by OFAC, or which are otherwise the target of U.S. Sanctions. U.S. Sanctions consist of trade embargoes, asset blocking/freezing measures, prohibitions on certain types of commercial and financial transactions, and/or involve a combination of these measures.

OFAC acts under authority granted by specific legislation to impose restrictions on transactions and freeze assets under U.S. jurisdiction. OFAC carries out its mandate often with other U.S. government agencies, including the United States Department of State and the United States Department of Commerce. Some U.S. Sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

There are two broad types of U.S. Sanctions. "Primary" sanctions risk are prohibitions enforceable with respect to U.S. Persons or transactions with a U.S. nexus and punishable with civil and criminal penalties. "Secondary" sanctions may be imposed on either U.S. or non-U.S. persons for, among other things, certain dealings with sanctioned persons even without any U.S. nexus.

(b) OFAC Jurisdiction and Primary Sanctions

When assessing whether an activity raises U.S. Sanctions risks, it is important to consider (1) whether the activity or transaction is subject to U.S. jurisdiction; (2) whether the persons involved, both directly and indirectly, are the target of U.S. Sanctions; and (3) whether the activity or transaction is within the scope of U.S. Sanctions. If the answer to the first question is "yes," the transaction must comply with all U.S. primary Sanctions.

Generally, OFAC exercises jurisdiction over (1) U.S. Persons; and (2) transactions involving non-U.S. persons with a nexus to the territory of the United States.

(i) U.S. Persons

In general, all transactions and activities involving a U.S. Person anywhere in the world must comply with U.S. primary Sanctions. "**U.S. Person**" includes:

- any U.S. citizen, wherever located (and including dual citizens);
- any permanent resident alien of the United States (such as a green card holder), wherever located;
- any person located in the United States; and
- any entity organized under the laws of a U.S. jurisdiction, including such entity's overseas branches or divisions.

As a result, any U.S. citizen or permanent resident alien of the United States employed by ALMAR anywhere in the world, including officers and directors of ALMAR, must comply with U.S. Sanctions. Similarly, any ALMAR employee must comply with U.S. Sanctions while located in the United States, regardless of their citizenship or residence.

Under certain circumstances, entities owned or controlled by U.S. Persons must also comply with U.S. Sanctions. Under the Cuba and Iran programs, non-U.S. entities that are owned or controlled by U.S. Persons must comply at all times with all Cuban and Iranian sanctions. Under the North Korea program, foreign subsidiaries of U.S. financial institutions must comply with the sanctions applicable to the Government of North Korea and any person on the SDN List pursuant to North Korean authorities.

(ii) Transactions with a Nexus to U.S. Territory

Non-U.S. Persons must comply with U.S. primary Sanctions if they conduct transactions that are subject to U.S. jurisdiction. For example, transactions involving U.S.-origin Items or services that are exported or re-exported to a sanctioned person or to or through a sanctioned country, and financial transactions that clear through a U.S. financial institution and that directly or indirectly involve a sanctioned person or country may raise issues under U.S. Sanctions. Most U.S. dollar-denominated transactions clear through a U.S. bank, meaning they are processed by a bank within the territory of the United States.

Additionally, U.S. primary Sanctions prohibit anyone, including a non-U.S. Person, from aiding, abetting, or causing a violation of U.S. Sanctions. Thus, U.S. Sanctions prohibitions can reach the conduct of non-U.S. Persons if they aid or abet or cause a violation of U.S. Sanctions by a U.S. Person.

(c) Comprehensive Sanctions

OFAC has implemented "**comprehensive sanctions**" laws that prohibit virtually all trade and commercial transactions with certain jurisdictions. As of the date of this Policy, the jurisdictions subject to comprehensive sanctions are: **Cuba, Iran, Syria, North Korea, and the Crimea, so-called Donetsk People's Republic and so-called Luhansk People's Republic regions of Ukraine**.

While there are differences among the regulations applicable to each jurisdiction, as a general matter, the sanctions prohibit importing, exporting, or otherwise providing, directly or indirectly, goods, services, and technology to or from any of these countries or where the benefit of the transaction is felt in these countries. The sanctions also prohibit U.S. Persons from dealing in any property in which any of these governments (including government owned or controlled entities) and other blocked persons have an interest. Certain governments of sanctioned jurisdictions are blocked; if any asset in which any of these governments has an interest comes into the possession or control of a U.S. Person, the U.S. Person (such as a U.S. employee of ALMAR) must block the assets and report the transaction to OFAC.

(d) Targeted/List-Based Sanctions

OFAC maintains sanctions on designated terrorists, narcotics traffickers, weapons of mass destruction proliferators, transnational criminal organizations, vessels/aircraft, and individuals and entities that have been determined to be acting on behalf of countries subject to U.S. economic sanctions. For example, in response to Russia's invasion of Ukraine, a number of key Russian entities, including some of Russia's largest banks, have been added to the SDN List. Similarly, many Russian government officials and oligarchs have been added to the SDN List. These persons have been added to OFAC's SDN List. The SDN List is updated regularly and the cumulative list is available through OFAC's website.

U.S. Persons are prohibited from engaging in any transactions with a person on the SDN List, and U.S. Persons must also block any property in which such persons have an interest that comes into their possession or control. These sanctions apply by operation of law to any entity owned in the aggregate, directly or indirectly, 50% or more by one or more persons on the SDN List, such that the entity itself is considered to be a blocked person and all the same restrictions apply to it regardless of whether the person is added to the SDN List ("**50% Rule**"). As used in OFAC's 50% Rule, "indirectly" refers to one or more blocked persons' ownership of shares of an entity through another entity or entities that are 50% or more owned in the aggregate by the blocked person(s). Traditional corporate notions of dilution do not apply. For example, if two SDNs collectively own 50% of Entity A, and Entity A owns 50% of Entity B, Entity B is considered to be blocked. The SDNs ownership of Entity A makes Entity A blocked person. Entity A's 50% ownership of Entity B in turn makes Entity B a blocked person.

The United States also maintains a number of other sanctions lists of persons subject to restrictions that are more limited than full blocking sanctions. For example, since 2014, the United States has imposed so-called sectoral sanctions against certain companies in Russia's financial, energy, and defense sectors identified on the SSI List. These sectoral sanctions have generally targeted the companies' access to U.S. oil and gas technology and debt and equity markets. In response to the 2022 invasion of Ukraine, the United States adopted additional restrictions on dealing in debt and equity of, certain companies in Russia. The 50% Rule also applies to entities on the SSI List. The SSI List is updated regularly and the cumulative list is available through OFAC's website.

While Russia itself is not subject to comprehensive sanctions, it is now also generally prohibited to engage in transactions involving the Central Bank of the Russian Federation and the National Wealth Fund of the Russian Federation. Additionally, the United States currently maintains a ban on new investment in Russia, and prohibits the exportation, re-exportation, sale or supply, directly or indirectly, from the United States or by a U.S. Person of certain services.

Finally, the United States maintains sanctions on the Government of Venezuela. The term "Government of Venezuela" includes the state and Government of Venezuela, any political subdivision, agency, or instrumentality thereof, including Petroleos de Venezuela, S.A., any person owned or controlled, directly or indirectly, by the foregoing, and any person who has acted or purported to act directly or indirectly for or on behalf of, any of the foregoing, including as a member of the Maduro regime. As the Government of Venezuela is involved in a number of commercial activities, trade with Venezuela can readily implicate U.S. sanctions.

(e) Secondary Sanctions

"**Secondary sanctions**" are measures that principally target non-U.S. Persons and entities for engaging in certain enumerated activities. Such activities need not have any U.S. jurisdictional nexus (*i.e.*, no U.S. Person involvement; no U.S. origin items; no U.S. dollar payments; and no other nexus with U.S. territory). Unlike primary sanctions, violation of which can lead to civil and/or criminal penalties, the penalty for engaging in the enumerated activities is the imposition of sanctions. These sanctions can be relatively minor to severe, including blocking the targeted person. The U.S. government must first determine that an individual or entity has engaged in sanctionable conduct before sanctions can be imposed. If blocking sanctions are imposed, U.S. Persons would be prohibited from undertaking most transactions with the sanctioned person.

Secondary sanctions regimes exist, for example, in the Iran, Russia, and North Korea sanctions programs, as well the sanctions program targeting terrorism pursuant to Executive Order 13886.

(f) General Prohibitions on Facilitation and Evasion

U.S. Sanctions generally prohibit U.S. Persons from approving, financing, facilitating, or guaranteeing any transaction by a non-U.S. Person that would be prohibited if performed by a U.S. Person or within the United States and from taking any actions to circumvent, evade or avoid U.S. Sanctions. If a U.S. Person is prohibited from participating in a transaction by U.S. Sanctions, that U.S. Person may not refer the transaction to a party outside the United States. Similarly, if a transaction is prohibited by U.S. Sanctions, a U.S. Person may not assist in helping to restructure the transaction in order to evade the OFAC prohibitions.

U.S. EXPORT CONTROLS

(a) Background on U.S. Export Controls

The U.S. government regulates certain activities including the export, reexport, and transfer of commodities, technology, and software (collectively, "Items") around the globe.

As relevant to the Company, U.S. export controls are primarily administered by the Bureau of Industry and Security of the U.S. Department of Commerce ("BIS")[2] through the Export Administration Regulations ("EAR"), which apply to Items with purely commercial applications, both commercial and military or proliferation applications (what are called "dual-use" Items), and certain purely military applications. The EAR regulates exports (shipments or transmission out of the U.S., including sending or taking Items subject to the EAR out of the United States in any manner), reexports (shipments between foreign countries), and transfers (shipments between parties in the same foreign country) of all Items subject to U.S. jurisdiction, known as "subject to the EAR." U.S. export controls also apply to intra-company transfers as well as to the release of Items to foreign nationals within the United States, including ALMAR employees.[3]

Items that are subject to the EAR include (1) all Items located in the U.S. (including foreign Items moving in transit through the U.S. and Items located in a U.S. Foreign Trade Zone), (2) all U.S.-origin Items, wherever located, (3) foreign-produced Items that incorporate more than a *de minimis* amount of controlled U.S.-origin content, and (4) certain foreign-produced Items that are the direct product of U.S.-origin technology or software, or the direct product of a controlled plant or plant component that is itself the direct product of U.S.-origin technology or software. Items subject to the highest level of controls under the EAR are identified on the Commerce Control List ("CCL"). The CCL has 10 categories, each of which is divided into functional groups listed A-E that cover: equipment, assemblies, and components; test, inspection, and production equipment; materials; software; and technology. Each category in the CCL contains several five-digit alphanumeric Export Control Classification Numbers ("ECCNs"), organized by functional group, that specify the export controls rules applicable to the Items covered by the ECCN. Each ECCN contains a general description of the controlled Item(s), the reason(s) for control,

[2] The Department of State's DDTC has primary responsibility for the regulation and oversight of exports and temporary imports of defense articles and defense services through the International Traffic in Arms Regulations ("ITAR"). If products may be a defense article or defense service, please review the ITAR to determine relevant controls.

[3] Under the EAR, releasing technology or source code to a foreign person is a "deemed export" to the foreign person's most recent country of citizenship or permanent residency. A "release" includes visual or other inspection that reveals technology or source code, oral or written exchanges, and any act causing a release through the use of access information or otherwise.

available license exceptions, and additional details on related controls and more specific Item definitions. Items that are subject to the EAR but are not covered by any ECCN in the CCL are classified as "EAR99." EAR99 Items are subject to the lowest level of controls of any Items on the CCL and do not require a license for export, reexport or transfer in most circumstances. Controls on EAR99 Items apply only to exports, reexports, or transfers for certain end-uses *(e.g.*, terrorist activities), end-users (*e.g.*, companies appearing on certain restricted parties lists maintained by the U.S. Department of Commerce), or to particular jurisdictions.

(b) Licenses

Export controls may prohibit a particular export, reexport, or transfer unless a governmental authorization in the form of a license was been issued by BIS. Some exports, reexports or transfers are prohibited because an entity involved is restricted, regardless of the nature of the Item. Other activities may be prohibited based on the end-use or nature of the Item involved and its intended destination. The CCL and other relevant provisions of the EAR provide guidance on whether a license may be required for a particular export, reexport or transfer. If a license is required, the EAR provides certain license exceptions that may be relied upon if the transaction meets the criteria and satisfies all requirements of said license exception. The EAR also include recordkeeping and reporting requirements that must be complied with. Some of these requirements apply to all export-related transactions, and others apply in specific circumstances or to specific types of Items such as encryption Items.

U.S. ANTI-BOYCOTT LAWS AND REGULATIONS

(a) Background on U.S. Anti-boycott Laws and Regulations

The U.S. has adopted laws that seek to counteract certain foreign boycotts or embargoes that do not align with U.S. foreign policy and national security interests. The chief target of the U.S. anti-boycott laws and regulations is the Arab League boycott of Israel, but these laws apply more broadly to all foreign boycotts that are inconsistent with the foreign policy of the United States. The anti-boycott laws are found in the EAR, administered by the U.S. Department of Commerce through BIS, and in the Internal Revenue Code ("IRC"), which is administered by the U.S. Department of the Treasury. Depending on the circumstances, anti-boycott laws can apply to activities both within and outside of the United States and to U.S. and non-U.S. persons and businesses.

The EAR's anti-boycott rules prohibit participation in and cooperation with boycotts inconsistent with U.S. foreign policy and require quarterly reporting to BIS of requests to take actions that support unsanctioned boycotts. This covers U.S. exports and imports, financing, forwarding and shipping, and certain other transactions that may take place wholly offshore. Violations of the EAR's anti-boycott requirements can results in civil and criminal penalties, including fines, imprisonment, and denial of export privileges.

Commerce's anti-boycott rules apply to the conduct of U.S. persons when they are engaged in the interstate or foreign commerce of the United States. In other words, persons are subject to U.S. anti-boycott laws when their activities relate 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. The anti-boycott provisions of the EAR apply to the activities of all U.S. Persons, defined to include:

- any person who is a U.S. resident or citizen, no matter where located;
- any U.S. "concern," which refers to any corporation, partnership, or similar entity organized under U.S. law, wherever located;

- any non-U.S. branch office of a U.S. concern;

- any U.S. branch of any non-U.S. concern; and

- any non-U.S. affiliate that is deemed to be "controlled in fact" by a U.S. concern, regardless of whether or where the affiliate is incorporated or doing business. "Controlled in fact" refers to entities for which a U.S. company has the authority or ability to establish the general polices or to control day-to-day operations.

In addition, Commerce's anti-boycott provisions specifically provide that a transaction between a person or entity located in the United States and a non-U.S. subsidiary that is controlled in fact by any U.S. concern is considered an activity in U.S. commerce. Any ensuing sales transaction by the foreign subsidiary with another non-U.S. party may also be deemed within U.S. commerce under certain circumstances.

Treasury's anti-boycott rules do not prohibit conduct, but instead impose reporting requirements on U.S. taxpayers and their related companies, and deny certain tax benefits as a penalty for participating in or cooperating with an unsanctioned international boycott. The U.S. Department of the Treasury periodically publishes a list of current countries which require or may require participation in, or cooperation with, an international boycott. Treasury's rules require annual reporting to the IRS of (1) operations in or related to countries maintaining unsanctioned boycotts; (2) participation in unsanctioned boycotts; and (3) requests to participate in unsanctioned boycotts. Willful failure to report can result in criminal penalties. Treasury's rules apply to U.S. taxpayers, including members of a controlled group, regardless of whether a transaction involves any U.S. goods or services.

Treasury's anti-boycott rules have a slightly broader application than Commerce's anti-boycott rules. Treasury's rules apply not only to U.S. companies and persons, but also to U.S. companies' "affiliates." Affiliates include entities in which a U.S. corporate taxpayer has an ownership interest, direct or indirect, and can include some joint ventures. Treasury's anti-boycott rules cover all affiliated companies that are owned 10 percent or more, directly or indirectly, by a U.S. corporate taxpayer and to all partnerships in which a U.S. company is a partner, regardless of the percentage of partnership interests in the U.S. company.

(b) Anti-Boycott Prohibited Conduct

Prohibited conduct under the Commerce anti-boycott laws includes:

- Agreements to refuse or actual refusal to do business with or in a country or with blacklisted companies for boycott reasons;

- Agreements to discriminate or actual discrimination against other persons based on race, religion, sex, or national origin;

- Agreements to furnish or actual furnishing of information about business relationships with or in a country or with blacklisted companies for boycott reasons;

- Agreements to furnish or actual furnishing of information about any person's association with charitable and fraternal organizations which supports a boycotted country;

- Agreements to furnish or actual furnishing of information about the race, religion, sex, or national origin of another person; and

- Implementing letters of credit containing prohibited boycott terms or conditions.

(c) Anti-Boycott Reporting Requirements

The receipt of a boycott request triggers compliance obligations. Both the IRC and the EAR include reporting obligations.

The IRC requires taxpayers to report operations in, with or related to a country identified on Treasury's current list of boycotting countries or its nationals and requests received to participate in or cooperate with an international boycott on an annual basis. See above for the current list of boycotting countries.

However, participation in an unsanctioned foreign boycott by a country not identified on Treasury's list can result in the same tax penalties as participation with a country on the list. U.S. taxpayers must also report where they have reason to know that a country requires participation in an unsanctioned foreign boycott.

The EAR require U.S. persons to report on a quarterly basis any requests they have received to take certain actions to comply with, further or support an unsanctioned foreign boycott, whether or not the request was acted upon. The report must be filed with the U.S. Department of Commerce within one month following the end of the quarter during which the request was received if it was received in the United States, and within two months if received outside the United States. BIS does not maintain a list of boycotting countries. Boycott-related requests are actionable regardless of whether the issuing country or entity is on Treasury's list.

APPENDIX 3

OVERVIEW OF EU SANCTIONS AND EXPORT CONTROL LAWS

EU SANCTIONS

EU sanctions can take different forms with the most common measures being asset freezes ("**EU Financial Sanctions**") and general or specific sectoral trade restrictions or comprehensive sanctions ("**EU Economic Sanctions**," together with EU Financial Sanctions, "**EU Sanctions**"). The EU Commission maintains an EU Sanctions Map (accessible at: www.sanctionsmap.eu), which provides an overview of various EU sanctions programs.

EU Financial Sanctions are imposed on listed natural or legal persons, entities, or bodies ("**designated persons**"). EU Economic Sanctions typically are imposed on a country or specific economic sectors of a country. These sanctions involve prohibiting or restricting certain types of commercial and financial transactions with either all or specifically designated natural or legal persons in the respective country.

EU Financial Sanctions include measures against government or ex-public officials and others suspected of human rights abuses, violations of public international law, internal repression or political instability, theft of state assets or funds, war crimes or assassination, terrorism and terrorist financing, membership in Al Qaida or other terrorist groups, and assisting in nuclear proliferation. EU Financial Sanctions also target persons profiting from any such violations, crimes, or abuses. The EU maintains a "Consolidated List of Persons, Groups and Entities subject to EU Financial Sanctions," which is regularly updated. Individual EU Member States may maintain their own lists that contain additional persons.

The EU "Consolidated List of Persons, Groups and Entities subject to EU Financial Sanctions" is accessible at: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions/overview-sanctions-and-related-tools_en#list

Although no two sanctions regimes are exactly alike, it is generally prohibited for an EU individual or entity anywhere in the world to: (i) deal with the funds or economic resources belonging to, owned, held or controlled by a designated person; (ii) make funds or economic resources available, directly or indirectly, to, or for the benefit of a designated person; (iii) intentionally circumvent financial sanctions; or (iv) fail to notify the regulator of possession of funds owned or controlled by one or more designated persons. The definition of "funds" is broadly construed to include cash, all kinds of payment instruments, deposits, shares, derivatives, interest, guarantees, letters of credit and rights of set-off. The definition of "economic resources" is also extremely broad, and essentially includes anything of value (including goods and services and other benefits). An entity is considered to be owned by a designated person if one or more designated persons respectively own more than 50% of the interest in the entity.

The question whether an entity is controlled by one or more designated persons has to be determined based on a fact-intensive assessment of the circumstances in the individual case (*e.g.*, the criterion of control can be seen to be established when a designated shareholder has the right to remove or appoint the majority of the board members).

EU Economic Sanctions include restrictions or prohibitions in various sectors and/or specific stakeholders in targeted countries or territories including: oil and gas, mining and drilling, iron and steel, fossil fuels, aviation, road transportation, maritime navigation and the naval sector, dual-use goods, financial services, access to capital markets and banknotes denominated in any official currency of an EU Member State[4], luxury goods, certain computer software and advanced technologies. Therefore, even when not all imports or exports are prohibited, restrictions may apply with respect to particular items as well as with respect to certain destinations, end uses or end users. Exports and imports may also be subject to authorization requirements, and these authorizations have to be sought from the national competent authority of the respective EU Member State. EU Economic Sanctions on Russia following Russia's invasion of Ukraine also include a transaction ban for certain Russian state-owned entities, an investment ban for the Russian energy sector as well as debt and equity restrictions covering certain transferable securities (including crypto-assets) and money-market instruments issued by the Russian Central Bank and listed Russian companies.[5]

EU sanctions are enforced by individual EU Member States. Depending on the law of the Member State, it can constitute a criminal and/or administrative offense to violate applicable sanctions. Penalties vary across EU Member States, but they generally include fines, forfeiture of profits or revenues, as well as imprisonment. There will generally be no liability for a sanctions violation unless the person knows or had reasonable cause to suspect that their actions would violate EU Sanctions. Willful blindness will *not* protect a person from liability.

To whom do EU Sanctions apply?

EU sanctions generally apply

- within the territory of the EU;
- on board any aircraft or vessel under the jurisdiction of an EU Member State;
- to any person inside or outside the territory of the EU who is a national of an EU Member State;
- to any legal person inside or outside the territory of the EU, which is incorporated or constituted under the laws of an EU Member State, including non-EU branches of such legal persons; and
- to any legal person, entity or body in respect of any business done in whole or in part within the EU.

---

4 Including Bulgarian lev, Croatian kuna, Czech koruna, Danish krone, Hungarian forint, Polish zloty, Romanian leu, Swedish krona.

5 *See*, Council Regulation No. 833/2014.

EU Export Controls

Prohibitions or restrictions will apply in relation to specified items, including items that can be used for military purposes, internal repression, or nuclear proliferation; for example, exporting or supplying arms or dual-use items and associated services including technical assistance, training, or financing. Such items will generally be listed on the EU Dual Use List[6] or the EU Common Military List. Individual EU Member States may maintain similar lists containing additional items.

While the EU retains authority to issue certain authorizations (such as the "Union general export authorization" in the context of the EU dual-use goods regulatory regime), the responsibility for deciding on individual, global, or national general export authorizations for the export of regulated items outside of the EU (or in certain cases, transit between individual EU Member States) and for the provision of related services generally lies with the authority of each individual EU Member State. Moreover, as with EU Sanctions, each EU Member State sets the penalties for breaches of export control rules.

The scope of export control jurisdiction may vary based on the specific legislation. As a general matter, the any individual or entity engaging in the export of Items out of the EU is subject to EU export controls and it is the Company's policy to adhere to all the requirements of EU export controls and the applicable export controls legislation of EU Member States. Employees must abide by these export controls and under no circumstances should employees structure transactions to avoid them or frustrate their purpose.

6 *See* EU Council Regulation (EU) No. 2021/821 of May 20, 2021 (as amended).

APPENDIX 4

OVERVIEW OF UK SANCTIONS AND EXPORT CONTROL LAWS

UK SANCTIONS

UK sanctions can take different forms with the most common measures being asset freezes ("UK Financial Sanctions") and general or specific sectoral trade or export embargos ("UK Economic Sanctions", together "UK Sanctions").

UK Financial Sanctions are imposed on listed natural or legal persons, entities or bodies (so called "designated persons"). UK Economic Sanctions typically are imposed on a country or specific economic sectors of a country. These sanctions involve prohibiting or restricting certain types of commercial and financial transactions with either all or specifically designated natural or legal persons in the respective country.

UK Financial Sanctions include measures against government or ex-public officials and others suspected of human rights abuses, violations of public international law, internal repression or political instability, theft of state assets or funds, war crimes or assassination, terrorism and terrorist financing, membership of Al Qaida or other terrorist groups, and assisting in nuclear proliferation. UK Financial Sanctions also target persons profiting from any such violations, crimes or abuses.

Although no two sanctions regimes are exactly alike, it is generally prohibited for a UK individual or entity anywhere in the world to: (i) deal with the funds or economic resources owned, held or controlled by a designated person; (ii) make funds or economic resources available, directly or indirectly, to, or for the benefit of a designated person; and (iii) circumvent financial sanctions. The definition of "funds" is broadly construed to include cash, all kinds of payment instruments, deposits, shares, interest, guarantees, letters of credit and rights of set-off. The definition of "economic resources" is also extremely broad, and essentially includes anything of value (including goods and services and other benefits). The UK maintains the UK Sanctions List and the Consolidated List of Financial Sanctions Targets in the UK.

The UK Sanctions List and the Consolidated List of Financial Sanctions Targets in the UK is accessible at https://www.gov.uk/government/publications/the-uk-sanctions-list https://sanctionssearchapp.ofsi.hmtreasury.gov.uk/

UK Economic Sanctions include embargos with respect to certain items (including goods, technology, and services) exported to or imported from a particular country. UK Economic Sanctions can include restrictions or prohibitions in various sectors and/or specific stakeholders in targeted countries or territories including: oil and gas, mining and drilling, aviation, maritime navigation and the naval sector, dual-use goods, financial services, access to capital markets, luxury goods, internet related providers, professional services, certain computer software and advanced technologies. Therefore, even when not all imports or exports are prohibited, restrictions may apply with respect to particular items as well as with respect to certain

destinations, end uses or end users. Exports and imports may also be subject to authorization requirements.

Among other sanctions regimes, the UK has also adopted Financial Sanctions and Economic Sanctions on investment, services and trade in the Crimea Region, and the People's Republics of Donetsk and Luhansk. These sanctions prohibit certain activities, including the export of certain goods and technology to these territories; import of items from these territories, new investments in these territories, and the provision of tourism services in these territories. In addition, the UK has adopted a list of designated persons related to the Ukraine crisis.

The UK has also introduced a number of new sanctions over the past months against Russia. These include: (i) list-based blocking sanctions against Russian banks, companies, government entities, and several Russian individuals; (ii) transport restrictions on flying in UK airspace and entering UK ports; (iii) financial restrictions designed to (a) ban selected Russian state companies, persons connected with Russia as well as the Russian Government from dealing with securities and making loans or credit on UK markets, (b) restrict correspondent banking relationships and processing of sterling payments for select Russian banks, and (c) prohibit provision of financial services for the purpose of foreign exchange reserve and asset management to certain Russian Government bodies; (iv) social media and internet restrictions; and (v) research and innovation sanctions.

***

The UK's Office of Financial Sanctions Implementation ("OFSI") is the primary agency responsible for the interpretation, administration, and civil enforcement of UK sanctions. Any person (including a non-UK person) who engages in a prohibited activity subject to UK sanctions jurisdiction can be subject to civil and/or criminal penalties. UK sanctions legislation currently requires knowledge or reasonable cause to suspect for liability to attach to engaging in a prohibited activity. This requirement will be removed in the next three months, moving the UK to a strict liability regime instead. In the civil context, the penalty for a violation of UK sanctions can be up to £1,000,000 or 50% of the estimated value of the funds or economic resources involved in the prohibited activity, whichever is greater. In the criminal context, the penalty for a sanctions violation may be a criminal fine (generally unlimited) or imprisonment of up to 10 years.

The Company has operations in the UK, and it is the Company's policy to adhere to all the requirements of UK Sanctions. Employees must abide by these sanctions and under no circumstances should employees structure transactions to avoid these sanctions or frustrate their purpose.

<u>To whom do UK Sanctions apply?</u>

UK sanctions apply to activities that have certain touchpoints with the United Kingdom – a UK nexus. Post-Brexit, UK sanctions apply (1) to conduct within the United Kingdom (i.e., within the territory or territorial sea of the United Kingdom) by any person, and (2) to all UK persons (i.e., a UK national, or a body incorporated or constituted under the law of any part of the United Kingdom) wherever they are in the world.

OFSI published guidance further explaining that UK nexus "might be created by such things as a UK company working overseas, transactions using clearing services in the UK, actions by a local subsidiary of a UK company (depending on the governance), action taking place overseas but directed from within the UK, or financial products or insurance bought on UK markets but held or used overseas." OFSI notes that these examples "are not exhaustive or definitive – whether or not there is a UK nexus will depend on the facts in the case."[7]

UK EXPORT CONTROLS

Prohibitions or restrictions will apply in relation to items which can be used for military purposes, internal repression or nuclear proliferation; for example, exporting or supplying arms or dual-use items and associated services including technical assistance, training or financing. Such items will be listed on the UK Strategic Export Controls Lists. The UK also has other specific export restrictions, including in relation to hazardous chemicals, pesticides and drugs.

The UK has introduced a number of additional export control measures over the past months against Russia. These include expanding the scope of its existing export controls on "military goods and technology" to also cover "critical-industry goods and technology" as well as "dual-use goods and technology." The exportation from the UK of "aviation or space-related items and technology" to Russia is also prohibited. The UK has also extended its prohibitions around the export, supply and delivery of luxury goods, oil refining and quantum computing goods/technology to Russia or for use in Russia, as well as the import, acquisition and supply of iron and steel products from Russia or located in Russia. Increased import tariffs have been imposed on imports of key products from Russia and Belarus including paper, cement, glass, silver, iron, steel, works of art and antiques (amongst others). The UK Government has also announced its intention to gradually phase out the import of Russian coal and oil over the course of the year.

***

The main enforcement body for export control in the UK is Her Majesty's Revenue and Customs (HMRC). HMRC is able to refer cases to the Crown Prosecution Service, as well as issue administrative penalties to settle investigations. Export control violations can trigger a number of criminal offences in the UK. The Export Control Joint Unit (ECJU) is responsible for administering the UK's system of export controls and licensing.

It is the Company's policy to adhere to all the requirements of UK export controls and the applicable UK export controls legislation. Employees must abide by these export controls and under no circumstances should employees structure transactions to avoid them or frustrate their purpose.

[7] Monetary Penalties for Breaches of Financial Sanctions, available at: https://www.gov.uk/government/publications/ofsi-guidance-html-documents/monetary-penalties-for-breaches-of-financial-sanctions-guidance

APPENDIX 5

OVERVIEW OF AUSTRALIAN SANCTIONS AND EXPORT CONTROL LAWS

AUSTRALIAN SANCTIONS

Australia implements two types of sanctions regimes:

- UNSC sanctions, which Australia is obligated to implement as part of its membership of the United Nations; and
- autonomous sanctions, which the Australian government implements at its own discretion.

Some jurisdictions, such as Iran and North Korea, are subject to both UNSC and Australian autonomous sanctions.

Australian sanctions are implemented as "regimes". Most regimes target specific countries or regions, although some target terrorist organisations (such as Al-Qaida) or specific activities (such as serious abuses of human rights).

UNSC sanctions are primarily implemented under the Charter of the United Nations Act 1945 and related regulations. There is a separate set of regulations for each UNSC sanctions regime.

Autonomous sanctions are implemented under the Autonomous Sanctions Act 2011 and the Australian Autonomous Sanctions Regulation 2011, together with related instruments issued in respect of them.

The Australian Government's primary sanctions regulator is the Australian Sanctions Office ("ASO"), an office of the Department of Foreign Affairs and Trade ("DFAT"). The ASO works in conjunction with a number of other government entities, most notably the Department of Defence, Australian Border Force, and Australian Federal Police, and the Australian Transaction Reports and Analysis Centre ("AUSTRAC").

Types of sanctions

Australian sanctions are issued as prohibitions that relate to:

- making a "sanctioned supply" of export sanctioned goods (this is separate and additional too the Australian export controls described below);
- making a "sanctioned import" of "import sanctioned goods";
- providing a "sanctioned service";
- engaging in a "sanctioned commercial activity";
- dealing with a "dealing with a designated person or entity";
- using or dealing with a "controlled asset"; or

- the entry into or transit through Australia of a "designated" or "declared" person.

Each of these areas involve embedded definitions and concepts that are important to understand when applying the rules.

Sanctions targets

Australian sanctions can target government entities, private entities, organisations and individuals. They can also target the country more broadly – for example, sanctioning the supply or import of certain goods to or from a country, together with related services.

For example, the sanctions against Russia in connection with Ukraine targeted the Central Bank of the Russian Federation, Rossiya Bank, and associates of Vladimir Putin.

It should be noted that the name of a sanctions regime does not necessarily indicate the location of that regime's sanctioned persons. For example, a significant number of Russian citizens are subject to the "Ukraine sanctions regime".

To whom do Australian sanctions apply?

Australian sanctions laws apply to all activities undertaken in Australia, and to all activities undertaken overseas by Australian citizens or Australian-registered bodies corporate. In addition, sanctions laws can apply to conduct by non-Australian persons outside of Australia if a result of the conduct wholly or partly occurs in Australia or on an Australian aircraft or vessel, provided the act is also a criminal offence under the laws of the jurisdiction in which it takes place.

Ensuring sanctions compliance

The ASO maintains a public list of active sanctions regimes,[8] and a list of all persons or entities who are subject to targeted financial sanctions called the "Consolidated List".[9]

The Consolidated List is designed to make sanctions compliance as easy as possible, and contains information such as passport numbers, alternate names, and physical descriptions as indicators of the targets to enable effective screening. DFAT also provides a free software package called "LinkMatchLite" which assists in checking for possible matches between clients and the names on the Consolidated List.[10]

It is possible to obtain a permit from the Minister for Foreign Affairs to engage in an activity that would otherwise be prohibited by sanctions. Criteria for the granting of a permit differs between sanctions regimes. For example, the export of military equipment to South Sudan is prohibited by the Sudan and South Sudan Sanctions Regime, but a permit could be issued if the supply was of non-lethal military equipment that was intended for United Nations personnel.

AUSTRALIAN EXPORT CONTROLS

8 https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes.

9 https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list.

10 https://www.dfat.gov.au/international-relations/security/sanctions/Pages/consolidated-list/linkmatchlite-software.

In addition to its various sanctions' regimes, Australia also subjects a number of goods to export controls. These export controls are regulated by Defence Export Controls ("DEC"), a branch of the Department of Defence.

Export controls are enshrined in rules that are distinct from the sanctions regime, although the two areas may overlap. This means it is possible to violate export controls without violating sanctions and vice-versa, or to violate both simultaneously.

Australian export controls apply to every person in Australia, whether an Australian citizen or not. They apply when a person is undertaking a controlled activity with goods or technology listed as controlled on the Defence and Strategic Goods List ("DSGL").

The DSGL is an instrument issued by the Minister of Defence and updated regularly.[11] Goods and technology on the DSGL cannot be exported, supplied, published or brokered from Australia unless a permit has been obtained, or a legislative exemption applies.

The DGSL is split into two parts. Firstly, the munitions list, which lists military goods (eg grenades) and non-military lethal goods (eg commercial explosives). Secondly, the dual-use list, which lists a wide range of goods which, though they may be intended for commercial use, can also have a military application. For example, a sufficiently accurate gyroscope can be used in both a commercial plane or a military aircraft, so the dual-use list includes gyroscopes of certain specifications. Other items on the dual-use list include telecommunications devices, microchips, lasers, and certain types of steel.

Intangible assets such as software or intellectual property can also be subject to export controls. "Exporting" in the context of these assets can include communication via email, telephone, video conferencing, or presentations.

The DEC maintains an online self-assessment tool to help exporters determine if their activities are subject to export controls.[12]

[11] The latest version of the list, as of 23 June 2022: https://www.legislation.gov.au/Details/F2021L01198.

[12] https://www.defence.gov.au/business-industry/export/controls/assess-apply/self-assessment-tool

APPENDIX 6

OTHER SANCTIONS REGIMES

It is the Company's policy to adhere to all applicable Sanctions and Export Control laws and regulations jurisdictions in which the Company operates, to the extent permissible under local law.[13]

CANADA

The Company has operations in Canada and also complies with such other Sanctions and Export Control laws that Canada implements from time to time.

For additional information on Canadian Sanctions and Export Controls:
https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/current-actuelles.aspx?lang=eng
https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/russia-russie.aspx?lang=eng
https://www.international.gc.ca/controls-controles/about-a_propos/expor/before-avant.aspx?lang=eng

[13] Certain jurisdictions, such as the European Union and United Kingdom, have adopted blocking statutes that prohibit adherence to certain U.S. sanctions. If you encounter such a conflict, or if a local law conflicts with a requirement set forth in this Policy, you should consult with the Compliance Lead to determine the appropriate course of action.