

GLOBAL SANCTIONS AND EXPORT CONTROL POLICY

ALMAR WATER SOLUTIONS, S.L.U.

and SUBSIDIARIES

Revision 4, adopted 15th September 2026

INDEX

1. INTRODUCTION	3
2. PURPOSE.....	3
3. SCOPE.....	3
4. GOVERNANCE.....	4
5. THE PRINCIPLES OF COMPANY’S SANCTIONS AND EXPORT CONTROL PROGRAM	4
6. GUIDELINES OF CONDUCT.....	5
7. COMPLIANCE & REPORTING	7
8. REVIEW AND APPROVAL.....	8
APPENDIX 1	9
APPENDIX 2.....	11
APPENDIX 3.....	19
APPENDIX 4.....	22
APPENDIX 5.....	26
APPENDIX 6 OTHER SANCTIONS REGIMES	30

1. INTRODUCTION

Almar Water Solutions, S.L.U. and its affiliates (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, the 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 permitted by applicable local law.¹

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 for employees to know when to seek advice from supervisors or other appropriate individuals. If you do not understand a provision of this Policy or are confused as to the actions you should take in a given situation, you should contact your supervisor, the Compliance Committee or the local person/function expressly designated by it for this purpose. If you wish to report a potential violation of the law or this Policy, you must follow the procedures referenced below.

2. PURPOSE

This Global Export Sanctions and Controls Policy (this "Policy") is intended to facilitate the Company's compliance with Sanctions and Export Control Laws and to reduce legal, operational, and reputational risks that could arise from a potential breach of such laws.

3. SCOPE

This Policy applies to all directors, employees, agents, consultants, and representatives of the Company, whether belonging to ALMAR or any of its affiliates (all collectively referred to as "**Personnel**" or the "**Company**"), as well as to ALMAR's agents, contractors and their supply chains, consultants, joint venture partners, sponsors, suppliers, and

¹Certain jurisdictions, such as the European Union and the United Kingdom, have adopted blocking statutes that restrict compliance with certain U.S. sanctions. Where compliance with this Policy would conflict with applicable law, the applicable law shall prevail, and the matter must be escalated to the Compliance Committee without delay.



representatives ("**Third Parties**").

Each ALMAR entity and subsidiary included within the scope of this Policy shall be responsible for ensuring that this Policy is implemented and complied with in its respective activities, operations and business relationships, and without prejudice to applicable local laws and corporate governance requirements.

Each ALMAR entity and subsidiary, through its local management, business owners and relevant functions, shall be responsible for applying the ordinary controls required under this Policy and ALMAR's applicable third-party due diligence, procurement, contracting and approval procedures. Ordinary relationships or transactions that do not present sanctions or export control concerns may be managed through the applicable local or business approval processes, provided that the required screening, due diligence and documentation have been completed.

4. GOVERNANCE

ALMAR's Compliance Committee is responsible for supervising and controlling, at corporate level, compliance with the values, principles and guidelines of conduct set out in this Policy.

Personnel and Third Parties may raise any questions or concerns regarding this Policy with the Compliance Committee, which will be ALMAR's point of contact in relation to this Policy.

Business owners remain responsible for monitoring the sanctions and export control risk associated with the relationships and transactions under their supervision and for promptly notifying the Compliance Committee or the designated compliance function of any change in circumstances, red flag, sanctions-related concern or information that may require further review or escalation under this Policy.

Business owners are responsible for identifying transactions or Third Parties that may present sanctions or export control concerns and for ensuring that the required information is obtained before entering into or continuing the relevant relationship. Any transaction involving a Restricted Jurisdiction, Prohibited Person, High-Risk Jurisdiction, High-Risk Person, potential sanctions match, export control restriction or conflict of laws shall be escalated to the local compliance responsible and, where material or high-risk, to the Compliance Committee and/or the relevant governance body for decision prior to execution.

Any sanctions or export control matter that is escalated for review shall be appropriately documented, including the information assessed, the risk considerations considered, the decision adopted, any conditions imposed and the approving authority. Such documentation shall be retained in accordance with the Company's record retention requirements.

5. THE PRINCIPLES OF COMPANY'S SANCTIONS AND EXPORT CONTROL PROGRAM

The Sanctions Compliance and Export Control Program consists of (1) the Policy, (2) the implementation procedures for this Policy (including the relevant sections of the Company's Third-Party Relationships Procedure), 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: Summary of EU sanctions and export control laws

Appendix 4: Summary of UK Sanctions and Export Control Laws

Appendix 5: Overview of Australia's Sanctions and Export Control Laws

Appendix 6: Other sanctions regimes

The Sanctions Compliance and Export Control Program is designed to ensure continued compliance with the Sanctions and Export Control Acts. To do this the following principles must follow:

- Assigns responsibility for coordinating and overseeing the Sanctions Compliance and Export Control Program to the Compliance Committee at corporate level and any person/function expressly designated by it for this purpose.
- Establishes a system of internal controls to comply with the Sanctions and Export Control Laws.
- Provides ongoing training of appropriate personnel.
- Conducts periodic risk-based reviews of the Sanctions Compliance and Export Control Program.

6. GUIDELINES OF CONDUCT

Risk assessment

The Company conducts 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 the Company to assess the nature and number of sanctions and export control risks, appropriately adjust the control environment to mitigate identified deficiencies, and make risk management judgements as to the acceptability of the risks identified.

To minimize the Company's exposure to legal, compliance and reputational risks, not only with respect to Sanctions and Export Controls, but also with respect to money laundering, corruption and other illicit activities, **it is the Company's policy:**

- **Not conduct any business with, in, or involving a "Restricted Jurisdiction" (see Appendix 1)) or any "Prohibited Person", even if such business is not prohibited by applicable law. "Prohibited Person" means (i) any person (individual or entity) that is subject to U.S., EU, Spain, Australia, or UK blocking**

sanctions (i.e., asset freeze sanctions) or (ii) any person located or resident or established under the laws of any Restricted Jurisdiction.

- **Any business involving another high-risk jurisdiction must be approved before such a business is started, in accordance with the escalation and approval process set out in the Governance section of this policy.** It is the Company's policy not to conduct business with, in, or involving high-risk jurisdictions (for a list of high-risk jurisdictions, see Appendix 1), including any person located or resident or established under the laws of a high-risk jurisdiction, without prior approval from the Compliance Committee or the person/function expressly designated by it for this purpose.
- **Any business with a high-risk person must be approved before such a business is started, in accordance with the escalation and approval process set out in the Governance section of this policy.** "High-Risk Person" means (i) any person located or resident or established under the laws of a High-Risk Jurisdiction, (ii) persons subject to U.S., EU, Spain, Australia or United Kingdom sanctions other than blocking sanctions (e.g., individuals 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 the U.S. restricted lists identified on the U.S. International Trade Administration's Consolidated Screening List, including individuals identified on the Department of Commerce's Entity List or Denied Persons List or the Department of State's Debarred List. The Compliance Committee or the person/function expressly designated by it will not approve any business with a High-Risk Person unless it has determined, upon careful review, that such business would not violate any of the applicable Sanctions and Export Control Laws and would not pose other significant compliance or reputational risks.

Due Diligence

As part of the due diligence process, the Company may obtain and assess information regarding the ownership and control structure of counterparties, including, where appropriate, the identification of ultimate beneficial owners and persons exercising effective control over the relevant entity.

Due diligence related to Sanctions and Export Control Laws must be conducted to ensure that ALMAR's counterparties, including ALMAR's clients/customers, joint venture partners, agents, contractors and their supply chains (subject to the due diligence requirements established in the Third-Party Relationships Procedure), sponsors, suppliers and consultants, representatives, other intermediaries or other persons acting on behalf of or for the benefit of ALMAR are legitimate and bona fide entities and that the Company is authorized to do business with them under this Policy. Diligence must be adapted to the particular risks of the sanctions and export control situation. Diligence should be enhanced if a counterparty is located or established in a high-risk jurisdiction or if there is reason to suspect improper activity. Please refer to the Third-Party Code of Ethics and the Third-Party Relationships Procedure for additional information on the procedures applied.

Counterparties shall be subject to ongoing monitoring on a risk-based basis throughout the duration of the business relationship. Additional screening or due diligence reviews shall be conducted whenever material changes are

identified in ownership, control, management, business activities, jurisdictions involved or other circumstances that may affect the sanctions or export control risk profile of the relationship.

Potential sanctions screening matches shall not be automatically treated as confirmed sanctions concerns. Where a potential match is identified, reasonable steps shall be taken to verify the identity of the relevant party and determine whether the match constitutes a true match or a false positive before a final decision is taken.

Employees of the Company should seek advice from the Compliance Committee or the person/function expressly designated by it in the following circumstances:

- There are reasons 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 its behalf), (ii) an entity owned or controlled by a Prohibited 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-Party Relationships Procedure.
- 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
- Otherwise, an employee has questions or concerns regarding a potential transaction.

Reporting and Record Keeping

The Company will timely file any reports required to be filed under the Sanctions and Export Control Laws, such as reports of blocked/frozen property or reports of rejected transactions. All records relating 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 request. If the applicable Sanctions and Export Control Laws prescribe a longer record-keeping period, the Company shall follow that longer period.

Compliance Program Review and Testing

The Company conducts risk-based testing of its Sanctions and Export Control Compliance Program. The tests will be carried out in the same manner as compliance audits are conducted by the Company. The Compliance Committee or the person/function expressly designated by it will determine, based on the risk, the frequency of such testing. The results of those reviews shall be communicated to senior management and the Board of Directors.

7. COMPLIANCE & REPORTING

The Compliance Committee will periodically organize mandatory training sessions, face-to-face or online, on the contents of this Policy for all Personnel of the Company's main offices and workplaces.



Personnel and Third Parties have a duty to report any knowledge or reasonable suspicion about possible breaches of this Policy in any part of our business or supply chains of any supplier level, for which, in addition to direct communication with their line manager, the Compliance Committee or any member of senior management, will have a confidential and anonymous **Communication Channel**, accessible through the Intranet and the Corporate Website, or directly by entering the following address in the Internet search engine:

<https://almarwater.i2-ethics.com/#/>

ALMAR **will not tolerate any form of retaliation, discrimination or penalization** against those who report in good faith. For the purposes of Australian law, “good faith” is not required to obtain protection; it is sufficient that the person has reasonable grounds to suspect that the reported information concerns misconduct or an improper state of affairs or circumstances. Notwithstanding the foregoing, the Company reserves the right to take disciplinary measures in accordance with the provisions of the disciplinary regime if the complaint submitted is found to be false and in bad faith.

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 who engaged in the prohibited activity, and may include fines or even imprisonment. Failure to comply with this Policy or the Sanctions and Export Control Laws are grounds for disciplinary action by ALMAR, including suspension, dismissal, and, in some cases, civil and/or criminal liability, in accordance with the applicable disciplinary regime and employment regulations. In addition, Third Parties should likewise expect their contracts to be terminated for cause if they violate this Policy, and ALMAR reserves the right to seek compensation for damages arising from breaches of this Policy.

8. REVIEW AND APPROVAL

This Policy will come into force after its approval by the Board of Directors and must be communicated to all Personnel and Third Parties.

This Policy shall be reviewed at least annually from a risk and regulatory monitoring perspective and formally updated whenever required due to relevant legislative, organizational, business, risk or control changes, as justified by changes in the Sanctions and Export Control Laws and the Company's risk assessment.

APPENDIX 1

RESTRICTED AND HIGH-RISK JURISDICTIONS (JULY 2026)

For the purposes of this Policy, a “**Restricted Jurisdiction**” is a jurisdiction with respect to which ALMAR prohibits business activities due to the sanctions and export control risks associated with that jurisdiction. ALMAR will not conduct business with, in, or involving a Restricted Jurisdiction, regardless of whether such activity may be permitted under applicable law.

A “**High-Risk Jurisdiction**” is not necessarily a sanctioned or prohibited jurisdiction. This classification is used by ALMAR for sanctions and export control risk management purposes and indicates that enhanced due diligence and prior approval requirements may apply under this Policy.

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
High-risk jurisdictions subject to more limited penalties	
Afghanistan	High
Belarus	High
Burma	High
Burundi	High
Central African Republic	High
China	High

Congo, Democratic Republic of the Congo	High
Ethiopia	High
Iraq	High
Lebanon	High
Libya	High
Mali	High
Nicaragua	High
Russia	High
Somalia	High
South Sudan	High
Sudan	High
Syria	High
Ukraine <i>(excluding the Crimea, Donetsk and Luhansk regions, which are classified as Restricted Jurisdictions under this Policy)</i>	High
Venezuela	High
Yemen	High
Zimbabwe	High

APPENDIX 2

SUMMARY OF U.S. SANCTIONS AND EXPORT CONTROL LAWS

US SANCTIONS

Background on U.S. sanctions

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

OFAC acts under the authority granted by specific legislation to impose restrictions on transactions and freeze assets under U.S. jurisdiction. OFAC often carries out its mandate with other U.S. government agencies, including the U.S. Department of State and the U.S. 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 main types of U.S. sanctions. The risk of "primary" sanctions are enforceable prohibitions with respect to U.S. persons or transactions with a nexus to the U.S. and punishable by civil and criminal penalties. "Secondary" sanctions may be imposed on U.S. or non-U.S. persons for, among other things, certain dealings with sanctioned persons, even without any nexus to the United States.

OFAC Jurisdiction and Primary Sanctions

When assessing whether an activity poses risks of U.S. sanctions, it is important to consider (1) whether the activity or transaction is subject to U.S. jurisdiction; (2) whether the individuals involved, either directly or indirectly, are subject to 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 primary U.S. sanctions.

In general, 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.

U.S. Persons

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

- any U.S. citizen, wherever located (and including dual nationals);



- any U.S. permanent resident alien (such as a green card holder), wherever located;
- anyone located in the United States; and
- any entity organized under the laws of a U.S. jurisdiction, including any foreign branches or divisions of such entity.

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

Under certain circumstances, entities that are owned or controlled by U.S. persons must also comply with U.S. sanctions. Under the Cuba and Iran programs, non-U.S. countries. 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 affiliates of U.S. financial institutions must comply with sanctions applicable to the Government of North Korea and anyone included on the SDN List in accordance with North Korean authorities.

Transactions with a nexus to U.S. territory

Non-U.S. persons must comply with U.S. primary sanctions if they engage in transactions that are subject to U.S. jurisdiction. For example, transactions involving items or services originating in the U.S. that are exported or re-exported to a sanctioned person or to or through a sanctioned country, and financial transactions that are cleared through a U.S. financial institution and that directly or indirectly involve a sanctioned person or country may pose problems under U.S. sanctions. Most transactions denominated in U.S. dollars are settled through a U.S. bank, which means they are processed by a bank within the territory of the United States.

In addition, the primary U.S. sanctions prohibit anyone, including non-U.S. persons, from aiding, abetting, or causing a violation of U.S. sanctions. Therefore, U.S. sanctions prohibitions can reach the conduct of non-Americans. Individuals if they aid, abet, or cause a violation of U.S. sanctions by a U.S. person.

Comprehensive sanctions

OFAC has implemented "**comprehensive sanctions**" laws that prohibit virtually all business transactions with certain jurisdictions. The jurisdictions currently subject to comprehensive U.S. sanctions include the following jurisdictions: **Cuba, Iran, North Korea and Crimea, the regions of the so-called Donetsk People's Republic, and the so-called Luhansk People's Republic of Ukraine.**

While there are differences between the regulations applicable to each jurisdiction, in general, sanctions prohibit importing, exporting, or otherwise providing, directly or indirectly, goods, services, and technology into 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 trading 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 lock the assets and report the transaction to OFAC.

Targeted/List-Based Sanctions

OFAC maintains sanctions on designated terrorists, drug traffickers, proliferators of weapons of mass destruction, transnational criminal organizations, ships/aircraft, and individuals and entities 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 individuals have been added to OFAC's SDN List. The SDN List is updated regularly, and the cumulative list is available through the OFAC 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 passes into their possession or control. These sanctions are applied by operation of law to any entity that is owned, directly or indirectly, 50% or more by one or more persons included in the SDN List, so that the entity itself is considered a blocked person and the same restrictions apply to it, regardless of whether the person is included in the SDN List ("50% Rule"). As used in the OFAC 50% Rule, "indirectly" refers to the ownership by one or more blocked persons of shares of an entity through another entity or entities that are owned by 50% or more in aggregate by the blocked person(s). Traditional corporate notions of dilution do not apply. For example, if two SDNs collectively own 50% of party A and party A owns 50% of party B, party B is considered blocked. The SDN property of party A makes party A a blocked person. In turn, ownership of 50% of Entity A of Entity B 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 total lockdown 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 companies' access to U.S. oil and gas technology and debt and equity markets. In response to the invasion of Ukraine in 2022, the United States adopted additional restrictions on the debt and equity trading of certain companies in Russia. The 50% rule also applies to entities listed on the SSI List. The SSI list is updated regularly, and the cumulative list is available through the OFAC website.

While Russia itself is not subject to comprehensive sanctions, transactions involving the Central Bank of the Russian Federation, and the National Wealth Fund of the Russian Federation are now generally prohibited as well. In addition, the United States currently maintains a ban on new investment in Russia, and prohibits the export, re-export, 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 against 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, even as a member of Maduro's regime. Since the Government of Venezuela is involved in a number of commercial activities, trade with Venezuela can easily involve U.S. sanctions.

Secondary sanctions

"Secondary **sanctions**" are measures that primarily target non-U.S. persons. Persons and entities to perform certain listed activities. Such activities need not have any jurisdictional nexus to the U.S. (*i.e.*, any involvement by a U.S. person; any U.S.-origin items; any payment in U.S. dollars; and no other nexus to U.S. territory). Unlike primary sanctions, the violation of which may result in civil and/or criminal penalties, the penalty for engaging in the listed activities is the imposition of penalties. These penalties can range from relatively mild 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 conducting most transactions with the sanctioned person.

Secondary sanctions regimes exist, for example, in the sanction's programs against Iran, Russia, and North Korea, as well as in the counterterrorism sanctions program pursuant to Executive Order 13886.

General prohibitions on facilitation and evasion

U.S. sanctions generally prohibit U.S. persons from approving, financing, facilitating, or guaranteeing any transaction made by a non-U.S. citizen. A person who would be prohibited if performed by a U.S. person or within the United States and who took any action to circumvent, evade, or avoid U.S. sanctions. If U.S. sanctions prohibit a U.S. person from participating in a transaction, that U.S. person may not remit the transaction to a party outside the United States. Similarly, if a transaction is prohibited by U.S. sanctions, a U.S. person cannot help restructuring the transaction to evade OFAC's prohibitions.

U.S. EXPORT CONTROLS

(a) Background to U.S. export controls

The U.S. government regulates certain activities, including the export, re-export, and transfer of commodities, technology, and software (collectively, "Items") worldwide.

As far as the Company is concerned, U.S. export controls are primarily administered by the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") through² the Export Administration Regulations ("EAR"), which

² The Department of State's DDTC has primary responsibility for the regulation and oversight of temporary exports and imports of defense articles and defense services through the International Traffic in Arms

apply to items with purely commercial applications, both commercial and military or proliferation (referred to as "dual-use" items), and certain purely military applications. The EAR regulates exports (shipments or transmissions outside the U.S., including shipping or taking items subject to the EAR outside the United States in any way), re-exports (shipments between foreign countries), and transfers (shipments between parties in the same foreign country) of all items subject to U.S. jurisdiction, known as "AR subjects". U.S. export controls also apply to intracompany transfers, as well as the delivery 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 items originating in the U.S., wherever found, (3) foreign-produced items that incorporate more than a *minimum amount* of controlled content of U.S. origin, 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.-sourced technology or software. Items subject to the highest level of controls under the EAR are identified on the Trade Control List ("CCL"). The CCL has 10 categories, each of which is divided into functional groups listed from A to E covering: equipment, assemblies, and components; testing, inspection and production equipment; materials; software; and technology. Each category of the LCC contains several five-digit alphanumeric export control classification ("ECCN") numbers, organized by functional groups, that specify the export control rules applicable to the items covered by the ECCN. Each ECCN contains an overview of the controlled items, the reasons for the control, the available license exceptions, and additional details about 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 all CCL items and do not require a license to

Regulations ("ITAR"). If the products may be a defense article or a defense service, review the ITAR to determine the relevant controls.

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



export, re-export, or transfer in most circumstances. The controls in EAR99 apply only to exports, re-exports, or transfers for certain end-uses (*e.g.*, terrorist activities), end-users (*e.g.*, companies on certain restricted party lists maintained by the U.S. Department of Commerce), or to certain jurisdictions.

(b) Licencies

Export controls may prohibit a particular export, re-export, or transfer, unless the BIS has issued a government authorization in the form of a license. Some exports, re-exports, or transfers are prohibited because an entity involved is restricted, regardless of the nature of the Article. Other activities may be prohibited depending on the end use or nature of the Item in question 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, re-export, or transfer. If a license is required, the EAR provides certain license exceptions that can be relied upon if the transaction meets the criteria and satisfies all of the requirements of that license exception. The EAR also includes recordkeeping and reporting requirements that must be met. Some of these requirements apply to all export-related transactions, and others apply in specific circumstances or to specific types of Items, such as Crypto Items.

U.S. ANTI-BOYCOTT LAWS AND REGULATIONS

(a) Background on U.S. anti-boycott laws and regulations

The United States has adopted laws that seek to counter certain boycotts or foreign embargoes that do not align with U.S. foreign policy and national security interests. The primary goal of U.S. anti-boycott laws and regulations is the Arab League's boycott of Israel, but these laws apply more broadly to all foreign boycotts that are inconsistent with U.S. foreign policy. Anti-boycott laws are found in the EAR, administered by the U.S. Department of Commerce through the 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 may apply to activities both inside and outside the United States and to the United States and outside the United States. people and companies.

The EAR's anti-boycott rules prohibit participation in and cooperation with boycotts inconsistent with U.S. foreign policy and require that requests to act supporting unauthorized boycotts be reported quarterly to the BIS. This covers U.S. exports and imports, financing, forwarding and shipping, and some other transactions that may take place entirely overseas. Violations of the EAR's anti-boycott requirements can result in civil and criminal penalties, including fines, imprisonment, and denial of export privileges.

The Department of Commerce's anti-boycott rules apply to the conduct of U.S. persons when engaged in U.S. interstate or foreign commerce. In other words, individuals 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 EAR's anti-boycott provisions apply to the activities of all U.S. persons, defined to include:

- anyone who is a resident or citizen of the U.S., no matter where they are;

- any U.S. "business," which refers to any corporation, partnership, or similar entity organized under U.S. law, wherever located;
- any non-U.S. branch of a U.S. company;
- any U.S. branch of any non-U.S. entity of concern; and
- any non-U.S. affiliate that is considered "de facto controlled" by a U.S. company, regardless of whether the affiliate is incorporated or doing business. "De facto controlled" refers to entities for which a U.S. company has the authority or capacity to set general policies or control day-to-day operations.

In addition, the Department of Commerce's anti-boycott provisions specifically state that a transaction between a person or entity located in the United States and a non-U.S. person. A subsidiary that is in fact controlled by any U.S. company is considered an activity in U.S. commerce. Any subsequent sale transaction by the foreign subsidiary with another non-U.S. company. it can also be considered within U.S. commerce under certain circumstances.

The Treasury Department's anti-boycott rules do not prohibit conduct, but rather 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 that require or may require participation in or cooperation with an international boycott. Treasury rules require annual reports to the IRS of (1) operations in or related to countries that maintain unsanctioned boycotts; (2) participation in unauthorized boycotts; and (3) requests to participate in unauthorized boycotts. Failure to report deliberately may result in criminal sanctions. Treasury rules apply to U.S. taxpayers, including members of a controlled group, regardless of whether a transaction involves U.S. goods or services.

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

(b) Prohibited conduct against the boycott

Conduct prohibited under the Commerce Department's anti-boycott laws includes:

- Agreements to refuse or refuse to do business with or in a country or with blacklisted companies for boycott

reasons;

- Agreements to discriminate or effectively discriminate against others on the basis of race, religion, sex, or national origin;
- Agreements to provide or provide actual information on business relations with or in a country or with companies blacklisted for boycott reasons;
- Agreements to provide or provide actual information about anyone's association with charitable and fraternal organizations that support a boycotted country;
- Agreements to provide or provide information about another person's race, religion, sex, or national origin; and
- Implement letters of credit that contain prohibited boycott terms or conditions.

(c) Anti-boycott reporting requirements

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

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

However, participation in an unsanctioned foreign boycott by a country not identified on the Treasury list may result in the same tax penalties as participation in a country on the list. U.S. taxpayers should also report when they have reason to know that a country requires participation in an unsanctioned foreign boycott.

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

APPENDIX 3

OVERVIEW OF EU SANCTIONS AND EXPORT CONTROL LEGISLATION

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 global 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 the various EU sanctions programs.

EU financial sanctions are imposed on listed natural or legal persons, entities or bodies ('**designated persons**'). EU economic sanctions are usually imposed on a country or specific economic sectors within a country. These sanctions consist of prohibiting or restricting certain types of commercial and financial transactions with all specifically designated natural or legal persons in the respective country.

EU financial sanctions include measures against government officials or former 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 murder, terrorism and terrorist financing, membership of al-Qaeda or other terrorist groups, and assistance to nuclear proliferation. EU financial sanctions also target individuals who profit from such breaches, crimes or abuses. The EU maintains a "Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions", which is regularly updated. EU Member States can maintain their own lists containing additional people.

The EU's "Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions" can be found at:

<https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=es>

<https://www.sanctionsmap.eu/#/main>

Although no two sanctions regimes are exactly alike, it is generally prohibited for an EU person or entity anywhere in the world to: (i) deal with funds or economic resources owned, owned, held or controlled by a designated person; (ii) make funds or financial resources available, directly or indirectly, to or for the benefit of a designated person; (iii) intentionally circumventing financial sanctions; or (iv) failing to notify the regulator of the possession of funds owned or controlled by one or more designated persons. The definition of "funds" is interpreted broadly to include cash, all types of payment instruments, deposits, shares, derivatives, interest, guarantees, letters of credit, and set-off rights. The definition of "economic resources" is also extremely broad, and includes, essentially, 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 own, respectively, more than 50% of the interest in the entity. The question of whether an entity is controlled by one or more nominees should be determined on the

basis of a thorough assessment of the circumstances of the individual case (e.g., the control criterion may be considered to be established when a nominee shareholder has the right to remove or appoint a majority of the board members).

EU economic sanctions include restrictions or bans on various sectors and/or specific stakeholders in specific countries or territories, including: oil and gas, mining and drilling, iron and steel, fossil fuels, aviation, road transport, maritime navigation and shipping, dual-use goods, financial services, access to capital markets, and banknotes denominated in any official currency of a state ⁴EU membership, luxury goods, certain software and advanced technologies. Thus, even where not all imports or exports are prohibited, restrictions may apply with respect to certain 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 must be applied to the national competent authority of the respective EU Member State. The EU's economic sanctions on Russia following Russia's invasion of Ukraine also include a transaction ban for certain Russian state 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 Central Bank of Russia and Russian listed companies.⁵

EU sanctions are applied by each of the EU Member States. Depending on the legislation of the Member State, infringement of the applicable penalties may constitute a criminal and/or administrative offence. Penalties vary from EU member state to EU state, but typically include fines, confiscation of profits or income, as well as prison sentences. There will generally be no liability for a sanctions violation unless the person knows or has reasonable grounds to suspect that their actions would violate EU sanctions. Willful blindness will *not* protect a person from liability.

Who do EU sanctions apply to?

EU sanctions are usually applied:

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

⁵ See, Council Regulation (EU) No 833/2014.

- 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 incorporated under the law of an EU Member State, including branches of such legal entities outside the EU.
- To any legal person, entity or body in respect of any business conducted in whole or in part within the EU.

EU export controls

Prohibitions or restrictions will apply in relation to specific items, including items that can be used for military, internal repression or nuclear proliferation purposes; for example, the export or supply of arms or dual-use items and related services, including technical assistance, training or financing. These items will usually be included in the EU Dual-Use List⁶ or the EU Common Military List. EU Member States may maintain similar lists containing additional elements.

While the EU retains the power to issue certain authorizations (such as the "Union general export authorization" in the context of the EU dual-use regulatory regime), the responsibility to decide on individual, global or national general export authorizations for the export of regulated goods outside the EU (or, in certain cases, transit between different EU Member States) and for the provision of related services usually falls under the authority of each EU Member State. In addition, as with EU sanctions, each EU Member State sets the penalties for non-compliance with export control rules.

The scope of export control jurisdiction may vary depending on specific legislation. In general, any person or entity involved in the export of items outside the EU is subject to EU export controls and it is the Company's policy to comply with all requirements of EU export controls and applicable EU Member States export control legislation. Employees must comply with these export controls and under no circumstances should employees structure transactions to avoid them or defeat their purpose.

⁶ See EU Council Regulation (EU) No 2021/821 of 20 May 2021 (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 embargoes ("UK Economic Sanctions", collectively, "UK Sanctions").

UK financial sanctions are imposed on listed individuals, entities or bodies (so-called "designated persons"). UK economic sanctions are usually imposed on a country or specific economic sectors within a country. These sanctions consist of prohibiting or restricting certain types of commercial and financial transactions with all specifically designated natural or legal persons in the respective country.

The UK's financial sanctions include measures against government officials or former 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 murder, terrorism and terrorist financing, membership of Al Qaeda or other terrorist groups, and assistance to nuclear proliferation. The UK's financial sanctions also target individuals who profit from such violations, crimes, or abuses.

Although no two sanctions regimes are exactly alike, it is generally prohibited for a person or entity of the United Kingdom anywhere in the world to: (i) deal with funds or economic resources held, possessed or controlled by a designated person; (ii) make funds or financial resources available, directly or indirectly, to or for the benefit of a designated person; and (iii) circumventing financial sanctions. The definition of "funds" is interpreted broadly to include cash, all types 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 includes essentially anything of value (including goods and services and other benefits). The UK maintains the UK Sanctions List and the UK Consolidated Financial Sanctions Target List.

The UK Sanctions List and the UK Consolidated Financial Sanctions Target List can be found at

<https://www.gov.uk/government/publications/the-uk-sanctions-list>

<https://sanctionssearchapp.ofsi.hmtreasury.gov.uk/>

UK economic sanctions include embargoes on certain items (including goods, technology, and services) exported or imported from a particular country. UK economic sanctions may include restrictions or bans on various sectors and/or specific stakeholders in specific countries or territories, including: oil and gas, mining and drilling, aviation, maritime shipping and shipping, dual-use goods, financial services, access to capital markets, luxury goods, internet-related providers, professional services, certain software and advanced technologies. Thus, even where not all imports or exports are prohibited, restrictions may apply with respect to certain 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 United Kingdom has also adopted financial and economic sanctions on investment, services and trade in the Crimea region and the Donetsk and Luhansk People's Republics. These sanctions prohibit certain activities, including the export of certain goods and technology to these territories; the importation of goods from these territories, new investments in these territories and the provision of tourist services in these territories. In addition, the UK has adopted a list of designated persons related to the Ukraine crisis.

The UK maintains a range of sanctions measures against Russia. These include: (i) list-based blocking sanctions against Russian banks, companies, government entities, and various individuals; (ii) transport restrictions for flying in United Kingdom airspace and entering United Kingdom ports; (iii) financial restrictions designed to (a) prohibit certain Russian state-owned enterprises, persons associated with Russia and the Russian Government from dealing in securities and granting loans or credit in UK markets, (b) restricting correspondent banking relationships and the processing of payments in pounds sterling for certain Russian banks, and (c) prohibiting the provision of financial services for the purpose of reserving foreign exchange and managing assets through the United Kingdom. certain Russian government agencies; (iv) restrictions on social networks and the Internet; and (v) sanctions in the field of research and innovation.

The UK Financial Sanctions Implementation Office ("OFSI") is the primary agency responsible for the interpretation, administration and civil enforcement of UK sanctions. Any person (including a non-British person) who engages in a prohibited activity subject to the UK sanctions jurisdiction may be subject to civil and/or criminal penalties. Currently, UK sanctions legislation requires knowledge or suspicion of reasonable cause for liability to be attributed to participation in a prohibited activity. 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 violation of sanctions can be a criminal fine (usually unlimited) or a prison sentence of up to 10 years.

The Company has operations in the United Kingdom, and it is the Company's policy to comply with all requirements of the United Kingdom sanctions. Employees must comply with these sanctions and under no circumstances should employees structure transactions to avoid these sanctions or defeat their purpose.

Who do UK sanctions apply to?

The UK sanctions apply to activities that have certain points of contact with the UK, a nexus with the UK. After Brexit, UK sanctions apply (1) to conduct within the UK (i.e. within the territory or territorial sea of the UK) by any person, and (2) to all persons in the UK (i.e. a UK national or body incorporated or incorporated under the law of any part of the UK) anywhere in the world.

The OFSI published a guide further explaining that the link to the UK "could be created by such things as a UK company working overseas, transactions using clearing services in the UK, shares in a local subsidiary of a UK company (depending on governance), actions that take place overseas but directed from within the UK, or financial or insurance products purchased in UK markets but held or used abroad". The OFSI notes that these examples "are not exhaustive or definitive: whether or not there is a nexus with the UK will depend on the facts of the case".⁷

UK EXPORT CONTROLS

Prohibitions or restrictions shall apply in relation to items that may be used for military, internal repression or nuclear proliferation purposes; for example, the export or supply of arms or dual-use items and related services, including technical assistance, training or financing. These items will be included in the UK's Strategic Export Control Lists. The UK also has other specific export restrictions, including in relation to hazardous chemicals, pesticides and medicines.

The UK maintains a range of export control measures and trade restrictions in relation to Russia. These include expanding the scope of its current export controls on "military goods and technology" to also cover "goods and technology from critical industries" as well as "dual-use goods and technology". The export from the United Kingdom of "articles and technology related to aviation or space" to Russia is also prohibited. The UK has also expanded its bans 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,

⁷ Monetary penalties for non-compliance with financial sanctions, available at: <https://www.gov.uk/government/publications/ofsi-guidance-html-documents/monetary-penalties-for-breaches-of-financial-sanctions-guidance>

procurement and supply of iron and steel products from or located in Russia. Higher import tariffs have been imposed on key products from Russia and Belarus, such as paper, cement, glass, silver, iron, steel, works of art, and antiques (among others). The UK government has also announced its intention to phase out the import of Russian coal and oil throughout the year.

The main body responsible for enforcing export control in the UK is His Majesty's Revenue and Customs (HMRC). HMRC can refer cases to the Crown Prosecution Service, as well as impose administrative sanctions to resolve investigations. Export control breaches can lead to a number of criminal offences in the UK. The Joint Export Control Unit (JEC) is responsible for administering the UK's export control and licensing system.

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

APPENDIX 5

OVERVIEW OF AUSTRALIAN SANCTIONS AND EXPORT CONTROL LAWS

AUSTRALIAN SANCTIONS

Australia has two types of sanctions regimes:

- United Nations Security Council sanctions, which Australia is required to implement as part of its membership in 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 autonomous sanctions from both the UN and Australia.

Australian sanctions are applied as "regimes". Most regimes target specific countries or regions, although some target terrorist organizations (such as Al-Qaida) or specific activities (such as serious human rights violations).

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

Autonomous sanctions are implemented under the Autonomous Sanctions Act 2011 and the Australian Autonomous Sanctions Regulations 2011, together with related instruments issued thereon.

The Australian Government's primary sanctions regulatory body is the Australian Sanctions Office ("ASO"), an office of the Department of Foreign Affairs and Trade ("DFAT"). The ASO works in collaboration with other government entities, particularly the Department of Defense, the Australian Border Force and the Australian Federal Police, as well as the Australian Transaction Analysis and Reporting Centre (AUSTRAC).

Types of sanctions

Australian sanctions are issued as bans related to:

- The realization of a "sanctioned supply" of goods subject to export sanctions (this is separate from and in addition to the Australian export controls described below).
- Engage in a "sanctioned importation" of "sanctioned import goods".
- The provision of a "sanctioned service".
- Engaging in a "sanctioned commercial activity".
- Dealing with a "deal with a designated person or entity".
- Use or deal in a "controlled asset"; or
- The entry into or transit through Australia of a "designated" or "declared" person.

Each of these areas involves built-in definitions and concepts that are important to understand when applying the rules.

Objectives of sanctions

Australian sanctions can target government entities, private entities, organizations, and individuals. They can also target the country more broadly, for example, by sanctioning the supply or import of certain goods into or from a country, along with related services.

For example, sanctions against Russia in relation to Ukraine targeted the Central Bank of the Russian Federation, Bank Rossiya and Vladimir Putin's associates.

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

Who do Australian sanctions apply to?

Australian sanctions laws apply to all activities conducted in Australia and all activities conducted overseas by Australian citizens or legal entities registered in Australia. In addition, sanctions laws may apply to the conduct of non-Australian persons outside Australia if the result of the conduct occurs wholly or partly in Australia or on an Australian aircraft or vessel, provided that the act is also a criminal offence under the laws of the jurisdiction in which it is carried out.

Ensuring compliance with sanctions

The ASO maintains a public list of active sanctions regimes and a list of all individuals or entities that are subject to targeted financial sanctions, referred to as the "Consolidated List".

The Australia sanctions regime and consolidated list can be found at

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

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

The Consolidated List is a list of all persons and entities listed under Australian sanctions laws. It is designed to make sanctions compliance as easy as possible, and contains information such as passport numbers, alternative names and physical descriptions as indicators of targets to enable effective screening.

It may be possible to obtain a permit from the Minister for Foreign Affairs to engage in an activity that would otherwise be prohibited by sanctions. The criteria for granting a permit differ between sanction regimes. For UNSC sanctions, the Foreign Minister may need to notify or receive the approval of the UNSC before granting a sanctions

permit. The Australian Sanctions Portal (Pax⁸) administered by DFAT enables registered users to ask questions about sanctions and apply for a sanctions permit.

AUSTRALIA EXPORT CONTROLS

In addition to its various sanctions regimes, Australia also subjects a number of products to export controls. These export controls are regulated by the Defense Export Control (DEC), a branch of the Department of Defense.

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

Australian export controls apply to all persons in Australia, whether or not they are Australian citizens. They are primarily governed by the Defence Trade Controls Act 2012 (Cth), as amended by the Defence Trade Controls Amendment Act 2024 (Cth), together with related legislative instruments, including the Defence and Strategic Goods List ("DSGL"). These controls apply when a person carries out a controlled activity involving goods, software or technology listed as controlled on the DSGL.

The DSGL is an instrument issued by the Minister of Defense and regularly updated.⁹ Goods and technology covered by the DSGL may not be exported, supplied, published or brokered from Australia unless a permit has been obtained or a legislative exemption applies.

The DSGL is divided into two parts. First, the munitions list, which lists military goods (e.g., grenades) and non-military lethal goods (e.g., commercial explosives). Secondly, the list of dual-use items, which lists a wide range of items that, although they may be intended for commercial use, may also have a military application. For example, a sufficiently accurate gyroscope can be used on both a commercial aircraft and 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.

⁸ <https://pax.dfat.gov.au/sncPortal/s/>

⁹ The latest version of the list is linked via:- <https://www.defence.gov.au/business-industry/exporting/export-controls-framework/defence-strategic-goods-list>

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

As of 1 September 2024, Australia's defense export control laws were updated to establish a license-free environment between Australia, the UK and US (AUKUS) partners and creation of new controls in relation to DSSL goods and services.

DEC maintains an online self-assessment tool, accessible via My Australian defense exports portal, to help exporters determine whether their activities are subject to export controls.¹⁰

¹⁰ <https://www.defence.gov.au/business-industry/exporting/applications-and-pre-notification/my-australian-defence-exports-portal>

APPENDIX 6

OTHER SANCTIONS REGIMES

It is the Company's policy to adhere to all applicable Sanctions and Export Control laws and regulations in the jurisdictions in which the Company operates, to the extent permitted by local law.¹¹

CANADA

The Company has operations in Canada and complies with 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

¹¹ Certain jurisdictions, such as the European Union and the United Kingdom, have adopted blocking statutes that restrict compliance with certain U.S. sanctions. Where compliance with this Policy would conflict with applicable law, the applicable law shall prevail, and the matter must be escalated to the Compliance Committee without delay.