China Molybdenum Co., Ltd.

Export Controls Policy

1 Edition [2020]

CMOC_HQ_ZD_007 **Approver: Chaochun Li**

February 21, 2020

CONTENTS

Chapter 1 Purpose and Scope

The purpose of this Export Controls Policy (the "Policy") is to help ensure compliance by China Molybdenum Co., Ltd. ("Group") and all of its directly or indirectly controlled or majority-owned subsidiaries (collectively, "CMOC") with applicable export control laws enforced in the United States, the United Kingdom, European Union ("EU"), Australia, Brazil, People's Republic of China and other jurisdictions where they conduct business or from where they otherwise transfer controlled items and technology. Together with economic sanctions, these laws govern how CMOC conducts business with agents, customers, dealers, distributors, suppliers, and other similar third parties (collectively "Business Partners"). They also require CMOC to classify and control certain goods, services, and technical data to prevent transferring these items to prohibited countries and parties, as required under applicable law.

CMOC maintains this Policy to promote compliance with applicable laws. This Policy applies to all CMOC employees, officers, directors, agents, consultants, and any other persons acting on behalf of CMOC (collective "CMOC Personnel") anywhere in the world. Violations of export controls can result in severe consequences, including civil penalties, criminal fines, and possible incarceration. Accordingly, any violations of this Policy will result in disciplinary action, up to and including termination.

Chapter 2 What are Export Controls

Export Controls govern the export, shipment, transfer, or disclosure (and in some cases brokering, i.e., the arrangement of supply) of certain CMOC products, software, technology, and technical data (collectively "Products") that are controlled under applicable law. Export Controls may apply to certain products sent to various foreign countries ("Restricted Countries") and parties ("Restricted Parties"). Many of these controls arise from international agreements designed to limit the proliferation of dangerous materials and technologies. These restrictions are generally product-specific (e.g., specified by category or on a detailed list, often regardless of the export destination). These laws fall into three general categories:

1. Dual-Use Controls. Dual-Use Controls regulate certain specified commercial products, software, technology, and technical data that could be modified to serve military or harmful purposes ("Dual-Use Products"). In the United States, Dual-Use Products are subject to the Export Administration Regulations ("EAR") and appear on the corresponding Commerce Control List ("CCL"). The EU regulates many of the same Dual-Use Products, but there are certain differences compared to the CCL, under Annex I of the EU Dual-Use Regulation. The UK implements the EU's dual-use controls, but also has certain unilateral export controls (including when goods are shipped within the EU). Australia maintains similar controls under its Defense and Strategic Goods List.

   Collectively these lists classify Dual-Use Products using codes that reflect their unique characteristics and uses ("Export Codes"). Based on these Export Codes, the export of Dual-Use Products is restricted and a government authorization is generally required before they are exported. Often, this will be based on the following four factors:

   (a) Classification: What is the Product's Export Code (and what are the relevant conditions for export under this Code)?

(b) End-Destination: Where are the Products going (as the precise restrictions may vary depending on the export destination)?
(c) End-User: Who will ultimately obtain and use the Products?
(d) End-Use: How will the Products actually be used?

The EAR governs all Dual-Use Products located in the United States or manufactured in the United States. It also governs certain foreign-manufactured products that contain U.S.-origin content or are made using certain U.S.-origin technology. This means that U.S. requirements may follow Dual-Use Products regardless of who owns them or where they are located.

2. Defense-Related Controls. Defense-Related controls regulate specified defense articles, related technical data, and in some cases defense services ("Defense Products or Defense Services"). In the United States, Defense Products or Defense Services are subject to the International Traffic in Arms Regulations ("ITAR") and appear on the corresponding U.S. Munitions List ("USML"). In the EU, each Member State (including the UK) has its own regime for control of Defense Products or Defense Services but they are all largely based on the EU's Common Military List. Like the Dual-Use Controls described above, these lists classify Defense Products or Defense Services using Export Codes that reflect their unique characteristics and uses. Unlike the Dual-Use Controls, however, the ITAR also covers certain items that are "specially designed" for military purposes, even if they do not appear on the USML. Similarly, certain EU Member States may apply controls on unlisted products if they are supplied to military or law enforcement in foreign countries.

   In addition to these restrictions, the ITAR also requires manufacturers, exporters, or brokers of Defense Products or Defense Services operating in the United States to register with the U.S. State Department's Directorate of Defense Trade Controls ("DDTC") before manufacturing, brokering, or exporting any Defense Products or Defense Services. Additionally, registrants cannot conduct defense-related business with non-U.S. parties (including foreign national individuals) unless the U.S. State Department authorizes these activities under a separate export license.

3. Deemed Exports. The EAR and ITAR both prohibit the disclosure of controlled technology or technical data to unauthorized foreign nationals located within the United States ("Deemed Exports"). Deemed Exports can occur whenever Dual-Use Products and Defense Products or Defense Services are made available to individuals from Restricted Countries in the United States. This is true even if the foreign nationals are employed in the United States, have a valid U.S. work visa, or do not actually use the controlled items. These Deemed Export requirements do not apply to U.S. Citizens or U.S. Legal Permanent Residents (i.e., "Green Card" holders) because these individuals are not considered foreign nationals under the relevant regulations. The EU and the UK do not apply the Deemed Exports principle, but any risk of potential transfer of Dual-Use Products or Defense Products or Defense Services from the EU (including in an employee's luggage or on an employee's laptop) should be monitored as a prior authorization will generally be required.

Chapter 3 How do I Comply

To the extent required under applicable law, CMOC Personnel must not knowingly export, re-export, sell, ship, transfer or otherwise disclose Dual-Use Products, including to Restricted Countries or Restricted Parties. This specifically includes any transfer of software, technology, or technical information regarding Dual-Use Products or Defense Products or Defense Services via cloud-based computer servers, electronic mail, file transfer protocols, or other forms of electronic communication. Electronic transfers are treated the same way as actual exports, and must follow the same requirements.

CMOC Personnel who observe or identify any potential transactions involving export of Dual-Use Products or Defense Products or Defense Services where a required prior authorization has not been obtained, including to Restricted Countries or Restricted Parties, must immediately suspend the underlying transaction(s) and escalate the matter internally for further guidance. No further dealings or activities involving such products may occur until the risks have been evaluated and the transaction(s) authorized in writing (and, generally, any required export license obtained).

Additionally, CMOC Personnel must never approve, conduct, facilitate, or oversee any commercial transactions or information transfers involving Dual-Use Products or Defense Products or Defense Services being exported without a prior authorization, as required under applicable law, including where they directly or indirectly implicate Restricted Countries or Restricted Parties. The sole exception is for those transactions that receive prior written authorization, including from the relevant governmental authorities (where applicable).

In addition to these requirements, all CMOC Personnel must comply with all applicable EAR and ITAR requirements whenever Dual-Use Products or Defense Products or Defense Services are (1) made in the United States; (2) shipped from or through the United States; (3) contain de minimis U.S. content, or (4) are the foreign-produced direct product of certain controlled U.S.-origin technology. These requirements reflect the fact that such

products remain subject to U.S. jurisdiction regardless of where they are located or who may own them.

Chapter 4 Product Classification

To ensure compliance with applicable requirements, all Products used by CMOC across its international locations and facilities shall be reviewed regularly to determine the appropriate export classification for such items under the EAR, ITAR, or other relevant export control laws, as applicable.

Relevant information for Products controlled under the EAR, ITAR, or other applicable export control laws shall include the Export Codes for these Dual-Use Products and Defense Products or Defense Services, as well as any Restricted Countries associated with each of the relevant Export Codes (i.e., under U.S. export controls).

Chapter 5 Export Licensing & Registration

Before making an export, CMOC Personnel shall determine whether export licenses are required, including for a particular end-destination, end-user, or end use, under applicable law. If so, then the necessary export licenses shall be obtained. No CMOC Personnel may export, re-export, disclose, or otherwise transfer any Products requiring an export license until they receive written confirmation that CMOC possesses the necessary authorizations. Depending on the Product's Export Code, this could potentially include certain transfers, export, or disclosures.

Additionally, any CMOC entities operating in the United States shall register with the DDTC before manufacturing, brokering, or exporting any Defense Products or Defense Services in the future. CMOC shall maintain this DDTC registration continuously whenever it engages in ITAR-controlled activities. This includes facilitating the sale of third-party Defense Products or Defense Services located in the United States to CMOC affiliates operating in other countries.

Chapter 6 Restricted Countries & Parties

To conduct appropriate export control due diligence by CMOC on its Business Partners will be an effective method to identify Restricted Countries and Restricted Parties, where applicable. To this end, all new Business Partners should be screened using applicable Restricted Party Lists ("RPLs"). If this screening and a general review of the transaction for relevant red flags identifies a possible match or flag for any Restricted Countries or Restricted Parties under applicable law, then CMOC Personnel must immediately suspend all pending transactions with the relevant Business Partners until authorized by responsible CMOC personnel.

CMOC Personnel should screen all new Business Partners for Restricted Countries and Restricted Parties as necessary under applicable law. The company will also screen its existing Business Partners for export control risks on an annual basis to account for periodic changes in the relevant laws. In some instances, screening may also be required for intermediary banks, carriers, freight forwarders, or other parties participating in a transaction.

If such screening identifies a possible match for any Restricted Countries or Restricted Parties under applicable law, then CMOC must immediately suspend all pending transactions with the relevant Business Partners until the screening results are reviewed and the business authorized in writing.

Existing Business Partners will also be screened for these risks periodically to account for changes to the underlying laws programs and any associated RPLs. If this periodic screening identifies a possible match for any Restricted Countries or Restricted Parties under applicable law, then CMOC Personnel must immediately suspend all pending transactions with the relevant Business Partners until the matches are reviewed and the business has been authorized in writing.

Chapter 7 Third Party Risks

All CMOC Personnel must be alert to suspicious activity, suspend transactions when suspicions arise, and contact the relevant authority if any uncertainty exists. Examples of "red flags" that merit further inquiry appear in the Appendix. CMOC Personnel who observe any of the suspicious activities described in the Appendix must immediately suspend the underlying transaction(s) and obtain guidance before conducting any further business with the relevant Business Partners.

Chapter 8 Recordkeeping Requirements

In some instances, information may be requested so that CMOC can file disclosures or other reports with government agencies. All CMOC Personnel should maintain and immediately produce any information that would assist with such filings. Additionally, they should retain any records and correspondence relating to registrations, export licenses, and transactions involving Dual-Use Products or Defense Products or Defense Services as required under applicable law (for example, for a minimum of five (5) years in the United States), or longer if required under the conditions of the license. Failure to maintain such records can undermine CMOC's ability to respond to inquiries from government enforcement agencies in the United States and other relevant jurisdictions.

Chapter 9 Internal Reporting of Violations

CMOC is committed to conducting business with honesty and integrity. To that end, any CMOC Personnel who observe any potential or actual violations of this Policy or the underlying laws must immediately contact the relevant authority, to the extent that such internal reporting is permissible under applicable national law. CMOC does not permit any form of retaliation against employees who report suspect violations of the relevant laws or company policies in good faith.

Chapter 10 Appendix

Export Controls "Red Flags"

1. Business Partners have addresses in Restricted Countries or names and addresses that are similar to entities on Restricted Party Lists.
2. Business Partners or other transaction parties are suspected of involvement in export diversion or smuggling to Restricted Countries or Restricted Parties.
3. Business Partners or other transaction parties are suspected of involvement in the development, production, or use of ballistic missiles.
4. Business Partners or other transaction parties are suspected of involvement in the development, production, or use of biological, chemical, or nuclear weapons.
5. Business Partners or other transaction parties are involved in the defense industry or provided goods and services to foreign militaries and security services.
6. Business Partners attempt to act as agents for undisclosed parties and refuse to provide information regarding those parties.
7. Business Partners are evasive about whether the Products they plan to purchase are for domestic use or export.
8. Business Partners place orders without being familiar with the Products' characteristics, maintenance, purpose, or use.
9. Business Partners request instructions, parts, or warranty repairs that they did not purchase, or that were shipped to another party.
10. Business Partners use Post Office boxes, names with different spellings, or other information that is inconsistent with their business.
11. The ultimate consignee listed on the bill of lading (or airway bill) is a freight forwarder, trading company, shipping company, or bank.

Chapter 11 Effectiveness and Interpretation

This Policy shall come into force on the date of signing by the Chairman of the Group and its promulgation.

If any policy previously issued by CMOC conflicts with this Policy, this Policy shall prevail.

This Policy shall be interpreted by the Legal and Compliance Department of the Group.