



# California ISO

## **Export Controls Policy** **Version # 1.0**

**Effective Date May 20, 2025**

ISO Public

## TABLE OF CONTENTS

<b>1.0</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>2.0</b>	<b>SCOPE.....</b>	<b>1</b>
<b>3.0</b>	<b>ROLES AND RESPONSIBILITIES.....</b>	<b>1</b>
3.1	CA ISO Personnel.....	1
3.2	Management .....	1
3.3	Accountability and Ownership.....	1
<b>4.0</b>	<b>OVERVIEW OF EXPORT CONTROL LAWS AND REGULATIONS.....</b>	<b>2</b>
4.1	Export Administration Regulations .....	2
4.2	Foreign Asset Controls .....	3
4.3	Anti-Boycott Regulations.....	4
<b>5.0</b>	<b>COMPLIANCE.....</b>	<b>4</b>
5.1	Asking the Right Questions.....	4
<b>6.0</b>	<b>COMMUNICATIONS.....</b>	<b>6</b>
<b>7.0</b>	<b>CONTACTS .....</b>	<b>6</b>
<b>8.0</b>	<b>CONCLUSION.....</b>	<b>6</b>
<b>9.0</b>	<b>REVISION HISTORY.....</b>	<b>7</b>
<b>10.0</b>	<b>APPROVAL .....</b>	<b>8</b>

---

## 1.0 INTRODUCTION

---

Although the California ISO (“CAISO”) does very little exporting of products and services, CAISO is committed to complying with all U.S. Government Export Control and Trade Sanctions Laws and Regulations. CAISO has implemented this Export Controls Policy to help CAISO employees, agents, vendors, contractors, consultants and other personnel (collectively, “Personnel”) understand those laws and regulations, and to help you identify when they may apply to the CAISO. This Policy will provide you with a basic understanding of export and trade sanctions restrictions so that you can recognize potential issues and seek assistance from the CAISO Legal Department.

---

## 2.0 SCOPE

---

This Export Controls Policy contains guidance for any Personnel involved with exporting any hardware, software (including source code), technology (collectively, “Export Items”) or services to any country outside the United States, or providing Export Items or services within the United States to persons who are foreign nationals ( *i.e.*, non-citizens, non-permanent residents), which can be a “deemed export.”

---

## 3.0 ROLES AND RESPONSIBILITIES

---

### 3.1 Personnel

All Personnel are responsible for complying with the provisions described in this policy, identifying any new or additional Export Items that may raise potential compliance issues and communicating those issues to John Spomer, Lead Counsel, in the Legal Department for further analysis.

### 3.2 Management

Management is responsible for implementing any controls needed to ensure that any Export Items belonging to CAISO comply with the U.S. Government Export Control and Trade Sanctions Laws and Regulations.

### 3.3 Accountability and Ownership

The Legal Department and IT Infrastructure, Architecture and Information Security Department are responsible for maintaining and implementing the Export Controls Policy and ensuring that it is available to all Personnel. The Legal Department will also advise Personnel and Management on whether any Export Items raise potential compliance issues.

---

## 4.0 OVERVIEW OF EXPORT CONTROL LAWS AND REGULATIONS

---

The United States government regulates the transfer of information, commodities, technology, and software considered to be strategically important to the United States to protect national security, foreign policy, and economic interests without imposing undue regulatory burdens on legitimate international trade. There is a network of federal agencies and regulations that govern exports that are collectively referred to as “Export Controls.” These regulations:

- Govern the export, re-export and transfer (in-country) of dual-use (items with commercial and military applications) hardware, software and technology from the U.S. and their subsequent re-export from one foreign country to another. (See Section 4.1);
- Impose comprehensive or limited economic and trade sanctions on specific countries, and listed individuals and entities. These regulations can prohibit virtually all transactions, or specific activities. (See Section 4.2); and
- Prohibit U.S. companies from participating in or cooperating with a foreign boycott which is not sanctioned by the U.S. (See Section 4.3)

Violations of Export Controls could subject CAISO to substantial civil and criminal penalties in addition to other consequences including adverse publicity, loss of export privileges, and time and money incurred for its defense.

### 4.1 Export Administration Regulations

Under the Export Administration Regulations (“EAR”), the Bureau of Industry and Security (“BIS”) of the Department of Commerce regulates the majority of U.S. commercial exports.

#### What is an “export”?

An export is a shipment or transmission out of the United States in any manner or releasing or transferring technology or source code (but not object code) to a foreign person in the United States (a “deemed export”). Items include hardware such as circuit boards or retail software packages. Technology is information necessary for the development, production or use of an item (the latter is defined as operation, installation, maintenance, repair, overhaul and refurbishing). Technology can be exported through blueprints or design plans, or can occur over the telephone, via the internet, email or faxes. An item is considered an export even if it is leaving the United States temporarily. Exports include foreign-origin items that are transmitted through the United States but later exported, including to their foreign country of origin, and some foreign-origin items incorporating U.S. items.

A deemed export can occur entirely inside the United States when sharing technology or source code with a foreign national (i.e., a person who is not a U.S. Citizen or a lawful

permanent resident (Green Card holder)) of the United States, even if the foreign national is living or working in the United States under a visa. Sharing technology with the foreign national is deemed an export to the foreign national's country. So, if the foreign national is from a country where certain export restrictions apply, CAISO must determine whether exporting that technology or source code: (1) is prohibited, (2) requires an export license, or (3) is permitted under a license exception, or an exemption from the EAR. For example, if CAISO hires an employee from a foreign country under a working visa, CAISO must determine whether the individual may have access to technology or source code that is regulated by EAR and then determine whether the item is prohibited from export to that same country, whether a license exception applies, or whether a license must be obtained.

The EAR also applies to re-exports and transfers (in-country). "Re-export" means the shipment or transmission of an Export Item from one foreign country to another foreign country. "Transfer" (in-country) is a change in end-use or end-user of an item within the same foreign country.

## 4.2 Foreign Asset Controls

Foreign asset controls are economic sanctions or embargoes that the U.S. imposes on certain foreign countries or foreign persons in an effort to cause them to modify certain practices. The Office of Foreign Asset Control ("OFAC") regulations prevent U.S. Citizens, residents, and companies from comprehensive or specific dealings with certain countries, individuals or entities. These countries and regions have included Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk People's Republic and Luhansk People's Republic regions of Ukraine. For the most recent list of sanctions, see this OFAC website: <https://ofac.treasury.gov/sanctions-programs-and-country-information>.

U.S. export control laws have a significant extraterritorial reach, meaning they also apply to actions taken outside the U.S. by U.S. persons or entities. For example, foreign subsidiaries of a U.S. entity are generally prohibited from engaging in certain transactions or activities with a sanctioned country.

Comprehensive sanctions are very broad in scope and prohibit almost all transactions. For example, the Iran sanctions provide that (unless otherwise authorized) no property or interest in property of the government of Iran that is in the U.S. or is within the possession or control of a U.S. person (including overseas branches), may be transferred, paid, exported, withdrawn, or otherwise dealt in. The definition of property or interest in property is complex and includes all types of contacts, instruments, goods, intellectual property, etc. "Transfer" is also defined broadly and, in this Iranian example, would prohibit (with limited exceptions) exports or re-exports of goods, technology, and services to Iran, imports of goods and services from Iran, or engaging in any activity that promotes or is intended to promote imports from, or exports to, Iran. Travel, transportation, performance of contracts, and transfers of funds would also be restricted transfers.

In order to determine if the CAISO should not be dealing with a particular person or entity, CAISO must check during onboarding to see if that “person” is on the “Consolidated Screening List” (“CSL”), and if so, whether that listing prevents all or only some types of transactions with that person. The CSL is available on the U.S. Department of Commerce’s International Trade Administration website as both an online search and a downloadable database: <https://www.trade.gov/consolidated-screening-list>. Searching the CSL, and eliminating potential false positive matches, can require prior experience and knowledge of the applicable regulations.

### 4.3 Anti-Boycott Regulations

The U.S. anti-boycott laws are enforced by BIS and the Department of the Treasury, Internal Revenue Service (“IRS”). These laws generally prohibit U.S. persons (including controlled-in-fact foreign subsidiaries of U.S. persons, and U.S. offices of foreign persons) from participating in boycotts that are not sanctioned by the United States Government. Although the anti-boycott laws primarily address the Arab League boycott of Israel, they apply to all foreign boycotts that are not sanctioned by the United States. A boycott-related request may be oral or written and may or may not require U.S. persons to take any specific action. Boycott requests may be hidden in contractual agreements, purchase orders and other transaction documents. Boycott violations include providing information about business relationships with a boycotted country or a blacklisted entity.

The anti-boycott laws contain specific reporting and recordkeeping requirements, including mandatory reporting of boycott requests to the Department of Commerce. Many recent Anti-boycott enforcement actions involve failures to report boycott requests.

In short, anti-boycott regulations are designed to ensure that U.S. persons and others covered by the act take no action in support or furtherance of unsanctioned foreign boycotts. It is unlikely that CAISO will be in a situation where it will be asked to participate in an unsanctioned boycott, but this discussion is here to make you aware that these regulations exist and that if faced with such a request, you must notify the Legal Department immediately.

---

## 5.0 COMPLIANCE

---

### 5.1 Asking the Right Questions

As of 2025, the Legal Department understands that CAISO’s primary export outside the boundaries of the United States is a limited set of information it transmits electronically to cloud servers in the United Kingdom. It is up to each Business Unit to identify any new or additional exports that may raise potential compliance issues and to communicate those issues to the Legal Department for further analysis. To help you determine whether the sharing of a certain product, information or technology may constitute an export and whether any potential compliance issues may arise, ask yourself the following:

### **A. What is the CAISO product, information or technology being exported?**

A relatively small percentage of Export Items require an export license. CAISO is responsible for determining the proper classification of Export Items under the applicable Export Control Classification Number (ECCN) of the Commerce Control List (“CCL”) (located at: <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-774/appendix-Supplement%20No.%201%20to%20Part%20774>). To determine whether an Export Item is listed on the CCL, and whether an export license is required, contact the CAISO Legal Department.

### **B. Where is it going?**

Although the CAISO typically does not export its products, information or technology to other countries, it is important to know if the export will be sent to a foreign country, or if technology or source code will be provided to a foreign national, even if located in the U.S.

For example, even if the export does not require a license, the ultimate end-user cannot be a prohibited end-user, such as persons who are on the BIS Entity List or the OFAC Specially Designated Nationals List, or who are located in countries subject to comprehensive sanctions. These users are identified in the CSL referenced in Section 4.2 above. In addition, virtually all transactions are prohibited with Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk People's Republic and Luhansk People's Republic regions of Ukraine. You should also consider whether the product, information or technology will be used or accessed by a foreign national from an embargoed country, even if the export itself is going to a country that is not subject to an embargo. Note, however, that normally allowing a foreign national to use hardware or software (but not source code) is not a deemed export. Finally, the CAISO may be prohibited from dealing with companies who perform services such as contracting, financing, and freight forwarding in support of a “bad end-use.”

If you believe that CAISO will be exporting a product, information, or technology to another country, confirm with the recipient where the export will be delivered and stored. Then contact the CAISO Legal Department who can help you determine if the proposed export is allowed by law.

### **C. What will they do with it?**

It is very unlikely that any CAISO product, information or technology will be used for a prohibited end-use by the recipient. Such restricted end-uses include nuclear, chemical and biological weaponry, certain military or military intelligence end-uses or end-users. However, if you have any concerns about how a recipient may use a CAISO export, please contact the CAISO Legal Department.

---

## 6.0 COMMUNICATIONS

---

A current version of this policy will be available on the CAISO website.

---

## 7.0 CONTACTS

---

Please contact John Spomer, Lead Counsel, in the CAISO Legal Department if you have any questions.

---

## 8.0 CONCLUSION

---

We all share the responsibility of complying with export control regulations. CAISO cannot comply without your help; so, we thank you in advance for your assistance.



---

**9.0 REVISION HISTORY**

---

**REVISION HISTORY**

VERSION NO.	EFFECTIVE DATE	REVISED BY	DESCRIPTION
1.0	05/20/2025	J. Spomer D. Shonkwiler	Initial Draft. Content ported over from the Export Control Standard.

---

**10.0 APPROVAL**

---

This policy has been reviewed and approved by:

**Vice President, General Counsel, Chief Compliance Officer, Corporate Secretary:**

Roger Collanton

Name

Signature on File

Signature

5/17/2025

Date

**Director, Architecture, Integration and Information Security Compliance:**

Rene Dupre

Name

Signature on File

Signature

5/20/2025

Date