Industry Guidance to Prevent Diversion of Advanced Computing Integrated Circuits

May 13, 2025

The Bureau of Industry and Security (BIS) is providing guidance to help increase industry's awareness of illegal diversion schemes involving advanced computing integrated circuits (ICs) and commodities that contain such ICs, which have been subject to BIS export restrictions since October 2022, as updated several times since then.[1]

BIS has determined that advanced computing ICs have the potential to enable military-intelligence and weapons of mass destruction (WMD) end uses. As noted when BIS first implemented controls on advanced computing ICs and in subsequent regulations issued since, such chips and systems containing them are being used by the People's Republic of China (PRC or China), as part of "military modernization efforts to improve the speed and accuracy of its military decision making, planning, and logistics, as well as of its autonomous military systems, such as those used for cognitive electronic warfare, radar, signals intelligence, and jamming."[2] The PRC also uses these items to "improve calculations in weapons design and testing including for WMD, such as nuclear weapons, hypersonics and other advanced missile systems, and to analyze battlefield effects."[3] BIS subsequently expanded the controls to other destinations to address PRC operations inside and outside of China and Macau that seek to acquire advanced ICs through transshipment and diversion, and by accessing datacenters with advanced ICs.

In response to diversion schemes that BIS has identified with regard to advanced computing ICs, below is a non-exhaustive list of transactional and behavioral red flags (in addition to the *"Know Your Customer"* and *Red Flag Guidance* available on the BIS website and set forth at supplement no. 3 to part 732 of the Export Administration Regulations (EAR) (15 CFR parts 730-774)) and due diligence actions that can assist companies in evaluating whether a party or an identified activity may be connected to export control evasion. BIS also is identifying catch-all controls that may apply to advanced computing ICs for training[4] AI models.

New Transactional and Behavioral Red Flags:

1. The customer (domestic or foreign) never received exports of advanced computing ICs and/or commodities that contain such ICs (*i.e.*, items that meet or exceed the parameters in ECCNs 3A090.a, 4A090.a, or associated .z ECCNs such as 5A992.z) prior to October 2022.
2. The customer received exports involving advanced computing ICs and/or commodities that contain such ICs prior to October 2022, but also saw a significant increase in exports thereafter.

[1] Advanced computing ICs and commodities that contain such ICs include Export Control Classification Numbers (ECCNs) 3A090.a, 4A090.a, and .z items in Categories 3, 4, and 5, such as servers classified as ECCN 5A992.z. *See* 15 CFR Supp. No. 1 to part 774.
[2] 87 Fed. Reg. 62186 at 62187 (October 13, 2022).
[3] *Id*.
[4] Training involves feeding large quantities of data into the model while using optimization algorithms to evaluate the quality of the program's outputs and improve its performance.

3. A domestic or foreign customer has a residential address and provides no alternative location where the advanced computing ICs and/or commodities that contain such ICs will be used. This red flag applies only where the quantity of advanced computing ICs is inconsistent with its individual/personal use.
4. The company and/or ship-to company, wherever located, has little to no presence online or there are differences between the English and non-English versions of the company's website that raise red flags.
5. The ultimate delivery or installation address is unknown. You are unable to determine whether the headquarters of the customer or its ultimate parent is located in a destination specified in Country Group D:5 (including China) or Macau, or the customer refuses to disclose or provides incomplete information about the location of its headquarters or ultimate parent company.
6. Parties to transactions listed as ultimate consignees or listed in the "consign to" field (*e.g.*, other financial institutions, mail centers, freight forwarders, retailers not involved in electronics, logistics companies) do not typically engage in business consistent with requiring a large quantity of advanced computing ICs (including servers containing such ICs).
7. The customer is co-located with, or its address is similar to, one of the parties on the Consolidated Screening List, including the BIS Entity List, the Office of Foreign Assets Control's Specially Designated Nationals (SDN) List, or the U.S. Department of State's Statutorily Debarred Parties List.
8. The reported end user, wherever located, is not a unique storefront for that organization (for example, a legal office, a virtual office, a shipping and receiving company).
9. The address of the purchaser is in a destination specified in Country Groups D:1, D:4, or D:5 (except A:5 or A:6), *i.e.*, is in a destination that requires an export license for advanced computing ICs and/or commodities that contain such ICs, and the compliance date for that license requirement has already passed.
10. The data center to which the advanced ICs and/or commodities containing such ICs are being exported does not or cannot affirm it has the infrastructure (*e.g.*, power/energy, cooling capacity, or physical space needed to run servers containing advanced ICs) to operate the advanced computing ICs and/or commodities that contain such ICs.
11. The customer providing Infrastructure as a Service (IaaS) does not or cannot affirm that users of its services are not headquartered in the PRC, whether or not such customer is located inside or outside of China and Macau.

Due Diligence Actions:

BIS has identified due diligence actions that companies should take for new customers, as well as evaluating IaaS providers, involved with the export or use of advanced computing ICs and/or commodities that contain such ICs subject to the EAR, especially those located in destinations outside of Country Group A:1 as identified in supplement no. 1 to part 740 of the EAR:

1. Evaluate the customer's date of incorporation (*e.g.*, incorporation after October 2022).
2. Evaluate the customer's ownership structure to determine if parties are headquartered or have an ultimate parent headquartered in a destination specified in Country Group D:5 (including China) or Macau.
3. Evaluate the end user and end use of the item (*e.g.*, whether the customer's line of business is consistent with the ordered items).

4. Before engaging in business with domestic or foreign customers, notify potential customers that your items are subject to the EAR and would require a license if exported, reexported, or transferred (in-country) to or within destinations specified in Country Group D:1, D:4, or D:5 (excluding destinations also specified in A:5 or A:6).
5. Before engaging in business with domestic or foreign customers, seek an end-user certification with detailed information on all proposed transaction parties (see § 748.5 of the EAR), including the end user, and the intended end use for specific transactions. The customer should also certify that it will not export, reexport, or transfer (in-country) advanced computing ICs for restricted 'military-intelligence end uses' or 'military-intelligence end users,' or for WMD. This would include transactions where the exporter, reexporter, or transferor has knowledge that a party to the transaction, such as an IaaS provider, will conduct training of an AI model for or on behalf of parties headquartered in destinations specified in Country Group D:5 (including China) or Macau, where such activities may support WMD or military-intelligence end uses/end users (see §§ 744.22; 744.2-744.5).
6. Request a written attestation from the data center that affirms that (1) the end user is authorized to operate at its location, and (2) it has the infrastructure to operate the type of server containing advanced ICs being exported. It is also a best practice that suppliers conduct on-site visits at the data center, or alternatively, utilize independent third-party certified auditors to confirm attestations.
7. Evaluate data centers to determine whether they have the infrastructure to operate servers containing advanced ICs greater than 10 megawatts. Data centers at or above this threshold merit additional scrutiny as they may be able to provide access to a large quantity of advanced computing ICs for training AI models for or on behalf of parties headquartered in countries of concern, where such activities may support WMD or military-intelligence end uses/end users.

Controls that May Apply to Advanced Computing Integrated Circuits and Other Commodities Used to Train AI Models

Access to advanced computing integrated circuits (ICs) and commodities subject to the EAR for training AI models has the potential to enable military-intelligence and weapons of mass destruction (WMD) end uses in Country Group D:5 countries (including China) or Macau.

Advanced computing ICs and commodities that contain such ICs include items classified under Export Control Classification Numbers (ECCNs) 3A090.a, 4A090.a, and .z items in Categories 3, 4, and 5, such as servers classified as ECCN 5A992.z.

The following activities may trigger a license requirement under the catch-all controls of part 744 of the EAR when there is "knowledge" that the AI model will be used for a WMD or military-intelligence end use/user:

- Exports, reexports, or transfers (in-country) of advanced computing ICs and commodities subject to the EAR to any party, such as foreign Infrastructure as a Service (IaaS) providers (*e.g.*, data center providers), when the exporter, reexporter, or transferor has "knowledge" that the IaaS provider will use these items to conduct training of AI models for or on behalf of parties headquartered in D:5 countries (including China) or Macau.

- Transfers (in-country), defined as a change in end use or end user, of advanced computing ICs and commodities subject to the EAR already in the possession of parties such as IaaS providers, if there is "knowledge" that the items will be used by the transferee to train AI models for or on behalf of parties headquartered in D:5 countries (including China) or Macau.

- A "U.S. person" provides any 'support' or performs any contract, service, or employment, when there is "knowledge" such activity will be used for or may assist the training of AI models for or on behalf of parties headquartered D:5 countries (including China) or Macau.

Parties that do not obtain prior BIS authorization to engage in these transactions or activities may be subject to potential civil or criminal enforcement action if a violation of the EAR occurs. In addition, foreign parties acting contrary to U.S. national security and foreign policy interests, including by training AI models that could support WMD or military-intelligence end uses for or on behalf of parties headquartered in Country Group D:5 (including China) or Macau, may be added to the Entity List, even where no violation of the EAR occurs.

Parties are prohibited from proceeding with a transaction when parties have "knowledge," as defined in part 772 of the EAR, that a violation has occurred, is about to occur, or is intended to occur. Exporters, reexporters, and transferors also may not self-blind to avoid license requirements.

Due Diligence Best Practices

BIS has identified the following information and assurances that can help prevent the unauthorized diversion of advanced computing ICs for restricted end uses and end users, including scenarios where there is knowledge that a party to the transaction will use the advanced computing ICs to conduct training of AI models for or on behalf of parties headquartered in D:5 countries (including China) or Macau, where such activities may support WMD or military-intelligence end uses (see §§ 744.22; 744.2-744.5). For customers that are already using customer certifications or end-use statements, BIS's suggestions below are not meant to replace what you have already determined best mitigates diversion risk. BIS encourages you to review the information below and consider whether it is worth adding any of the suggestions to your existing practices and documentation to help prevent diversion.

- Full name, address, and contact information of the customer, line of business, website address, and role in the transaction (*i.e.*, purchaser, intermediate consignee, ultimate consignee, or end user).
    - For new customers, request a copy of the business license.
- Activity the customer intends to take with the item(s):
    - Consumed/used by the customer
    - Maintained for stock, including the likelihood for reexport v. transfer (in-country)
    - Resold with a specification as to who the next customer is (name and address)
    - Provide Infrastructure as a Service (IaaS) – e.g., enable AI model training
    - Other (specify)
- If the customer is not the end user, the name and address of the known end user.
- Addresses where item(s) will be delivered and installed, if applicable.
- Location of the customer's headquarters or ultimate parent company's headquarters.
- Location of the end user's headquarters or ultimate parent company's headquarters, if different from the customer.
- List of the items involved in the transaction, including ECCNs corresponding to the item(s).
- If the customer is an IaaS provider, attestation that it is not providing access to advanced computing ICs for training AI models on behalf of parties headquartered in destinations specified in Country Group D:5 (including China) or Macau.
- Attestation that the customer will comply with the EAR and flow-down these EAR requirements to its customers and other parties to any subsequent reexport or transfer (in-country) transaction(s) of items subject to the EAR.
- Certification by the customer, including name, title, phone number, email address, date, and signature.

Exporters should review the information received to identify errors, omissions, or red flags (*e.g.*, line of business does not match with the exported item, phone number mismatch with the country where the purported customer or end user is located). Additionally, the unwillingness of a customer to attest to one or more requests for information may be a red flag.

This guidance can help exporters more effectively harden their supply chains to prevent diversion and violations of the EAR.