



U.S. Department of Commerce Rescinds Biden Administration's AI Diffusion Export Control Rule and Issues New Guidance on Huawei, Chips for AI Purposes, and Diligence Expectations

What You Need to Know

Key takeaway #1

The new guidance amounts to prohibitions on U.S. and non-U.S. persons using, selling, transferring, financing, or servicing Huawei's Ascend 910B, 910C, and 910D chips, as well as other comparable chips from other Chinese companies.

Key takeaway #2

While the U.S. Department of Commerce Bureau of Industry and Security (BIS) has issued some advanced computing-related license exceptions, none are applicable for these chips because the restriction is based upon "General Prohibition 10," which requires a separate waiver.

Key takeaway #3

Companies within the advanced computing and semiconductor industry should review the new BIS list of red flags and diligence requirements and update their internal policies accordingly. If not, BIS could consider this an aggravating factor in a future enforcement action.

Client Alert | 9 min read | 05.19.25

On May 13, 2025, the Department of Commerce's Bureau of Industry and Security (BIS) formally rescinded the Framework for Artificial Intelligence Diffusion interim final rule published by the Biden Administration, on the basis that it stifled innovation, was overly complex, and undermined U.S. diplomatic relations.

BIS also issued three new guidance documents that:

1. Clarify Huawei's Ascend 910B, 910C, and 910D (and likely other comparable Chinese chips) are prohibited for all persons (U.S. and non-U.S.) to use, sell, export, or finance, among other restrictions;
2. Emphasize end-use controls on the export, reexport, or transfer of advanced computing ICs and commodities subject to the EAR, and on U.S. persons providing support for training AI models for, when

there is “knowledge” that the AI model will be used for Chinese, Russian, and other U.S. arms embargoed country companies; and

3. Describe red flags exporters should identify and new diligence expectations when exporting chips for the AI sector.

Below is a summary of these developments.

I. Huawei’s Ascend Chips, and Other Similar Chinese Chips, Are Now Subject to a Presumption of a General Prohibition 10 (GP10) Violation

In the **first guidance** document, BIS explains that Huawei’s Ascend 910B, 910C, and 910D models are subject to the presumption that any activity involving the integrated circuit (IC) required – but did not receive – prior BIS authorization. The failure to receive necessary authorization taints the ICs, as described in GP10 of the Export Administration Regulations (EAR) (736.2(b)(10)). Therefore, any further activity involving these ICs (e.g., future exports, reexports, transfers, financing, servicing, repairing, or using the ICs) constitutes an ongoing violation of the EAR, if no previous authorization from BIS was granted.

BIS explains that other ICs may be subject to the same presumption if those ICs:

- Meet the technical requirements described in ECCN 3A090, which controls advanced node ICs; **and** are
- Developed or produced by a company that is located in, headquartered in, or has an ultimate parent company headquartered in a U.S. arms embargoed country such as China (e., a country in Country Group D:5) or Macau (particularly if that company is on the Entity List designated with a footnote).

In both cases, these presumptions can be overcome; although practically, this will be challenging.

These controls apply to U.S. and non-U.S. persons anywhere, with no U.S. nexus other than the asserted Foreign Direct Product (FDP) rule application. BIS explains that it has found that ICs that meet the technical requirements described in ECCN 3A090 (including the three named Huawei chips that are provided as examples) and are developed or produced by one of the companies described above likely are subject to the EAR (and thus U.S. jurisdiction) because there is a high probability that these items were made using U.S. technology, software, or machinery.

II. Catch-All Controls that May Apply to Advanced Computing Integrated Circuits for Training AI Models

BIS’ **second guidance** document explains the following activities may trigger a license requirement under the U.S. person and military-intelligence end use/user prohibitions in the EAR when there is “knowledge” that the AI model will be used for a Weapons of Mass Destruction (WMD) or military-intelligence end use/user. BIS explains three scenarios where a license could be required:

- A U.S. or non-U.S. person exports, reexports, or transfers advanced computing ICs and related commodities subject to the EAR to any party, such as foreign Infrastructure as a Service (IaaS) providers (e.g., data center providers), **and** 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.

- A U.S. or non-U.S. person transfers (e., changes the end user or end use in-country) advanced computing ICs and commodities subject to the EAR, which are already in the possession of parties such as IaaS providers, **and** the transferor has 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” (g., shipping, transmitting, transferring, facilitating a shipment, transmission, or transfer, or performance of a contract) 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 in D:5 countries (including China) or Macau.

In each of these instances, “knowledge” means both active and passive knowledge (e.g., you cannot be willfully blind).

Importantly, BIS reminds everyone that it can add non-U.S. parties to the Entity List if BIS determines the non-U.S. party is acting contrary to U.S. national security and foreign policy interests, even if there is no violation of U.S. law. Functionally, this type of potential restriction overhanging transactions outside the jurisdiction of the EAR functions as a type of “secondary sanction.”

III. Industry Guidance to Prevent Diversion of Advanced Computing Integrated Circuits

The last BIS **guidance document** urges exporters to take action to address “*illegal diversion schemes involving advanced computing integrated circuits (ICs) and commodities that contain such ICs*.” BIS organized this guidance into two categories: (1) New Transactional and Behavioral Red Flags and (2) Due Diligence Actions.

The transactional and behavioral red flags list describes suspicious behaviors of counterparties that indicate a higher risk of potential diversion (e.g., no ultimate delivery or installation address is provided; 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). If companies observe any of these behaviors, they should follow their internal process to further investigate and resolve the red flag before proceeding.

In the due diligence actions list, BIS articulates expected actions companies should take for all “*new customers, as well as evaluating IaaS providers*” prior to any transactions for the export or use of advanced computing ICs and/or commodities that contain such ICs. BIS expects companies to take these actions regardless of any red flags present.

Below in the Appendix we provide copies of both lists in full.

IV. What’s Next

- The Trump Administration has made targeting China’s semiconductor and AI sector a priority. Companies should expect an increase in enforcement actions, particularly non-U.S. companies that have products covered by the FDP rule or engage in activities that constitute the equivalent of “U.S. secondary sanctions,” under U.S. export controls (e.g., supporting the PRC government’s Military-Civil Fusion (MCF) Development Strategy).

- Since the BIS guidance notes that the list of Huawei chips is only an “illustrative list,” expect more chips and related items (made by Chinese companies) to be specifically identified by BIS in the future.
- The Trump Administration has hinted that, when it ultimately replaces the AI Diffusion rule, it will simplify the rule and take into account U.S. partners that were otherwise disadvantaged in the prior rule (particularly those countries in the Gulf Cooperation Council and in ASEAN, as well as India and Israel).

Appendix – Red Flags and Diligence Questions

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.
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, or 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.

New Advanced Computing ICs Due Diligence Actions for New Customers and IaaS

Providers:

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:
 - i. the end user is authorized to operate at its location, and
 - ii. 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.

Contacts

Jeffrey L. Snyder

Partner

Washington, D.C. D | +1.202.624.2790

jsnyder@crowell.com

Jeremy Iloulia

Counsel

He/Him/His

Chicago D | +1.312.840.3269

© 2025 Crowell & Moring LLP. All Rights Reserved.

jiloulia@crowell.com

Chandler S. Leonard

Associate

She/Her/Hers

Washington, D.C. D | +1.202.624.2905

cleonard@crowell.com