DORSEY
DORSEY+WHITNEY LLP

United States to Restrict Items to Data Centers that Provide Remote Access to China and Other Countries

November 16, 2026
by Lawrence Ward, Dave Townsend, T. Augustine Lo, and Paula Ortiz Cardona

On November 16, 2026, the U.S. Department of Commerce Bureau of Industry and Security ("BIS") announced restrictions on exports, re-exports, and in-country transfers of certain items to data centers worldwide that offer remote access to companies located in the so-called "D:5 countries," which includes China and 21 other locations.[1] BIS released an interim final rule ("IFR"), effective shortly upon publication in the *Federal Register*, that imposes significant new obligations and due diligence requirements under the U.S. Export Administration Regulations ("EAR") on companies involved in supplying goods, software, and technology to data centers, as well as the data centers themselves. The IFR targets remote access to computing technology needed to create super intelligence ("SI") products. In issuing the IFR, BIS would end a longstanding interpretation of the EAR that treated the provision of remote access to equipment as largely outside the scope of the EAR. In addition, the IFR makes certain other changes to the EAR, as described below.

The IFR will require significant compliance changes by U.S. and non-U.S. companies who are involved with equipment, software, or technology that is used for SI products, or certain SI-related services. Companies involved in the supply chain to data centers, or in creating computing equipment with integrated circuits ("ICs") controlled under the EAR accordingly will have to enhance visibility into their downstream customers and end-users.

Remote Access EAR Restrictions

The IFR creates a new data center end-use restriction (the "Data Center Rule") under the EAR. The Data Center Rule restricts the provision of certain computing equipment, related software, and related technology to data centers if an exporter, re-exporter, or transferor (in-country) has knowledge that those items will be used by a data center, worldwide, that provides remote computing services to companies headquartered in or whose ultimate parent company is headquartered in any D:5 country. As described below, the Data Center Rule combines several well-known concepts under the EAR with novel ones. Here are the key elements of the Data Center Rule:

Related People

- Lawrence Ward
- Dave Townsend
- T. Augustine Lo
- Paula Ortiz Cardona

Related Capabilities

- International Trade
- Government Enforcement & Corporate Investigations
- Government Contracts Counseling & Litigation

- **Data Centers.** The Data Center Rule restricts export, re-exports, and in-country transfers to data centers worldwide if the data center provides or will provide access to more than 12,000,000 aggregate total processing performance ("TPP"). Before the IFR, BIS had taken the position that remote access to hardware was not an export of that hardware. Thus, a data center was permitted to allow usage of computing equipment under certain circumstances where provision of that hardware directly to the end-user could have required a BIS export license. The Data Center Rule can apply to one data center or multiple "linked" data centers that share resources or balance workloads. Guidance on the 12,000,000 TPP threshold is provided in Export Control Classification Number ("ECCN") 3A090, which describes the TPP requirement as aggregated over all processing units on an IC, and certain other technical thresholds.
- **Knowledge.** The Data Center Rule restricts exports, re-exports, or in-country transfers if the exporter, re-exporter, or transferor has knowledge under the EAR that the items would be used by data centers permitting remote computing services to companies in or based in D:5 countries, and at the aggregate TPP threshold. Under the EAR, knowledge includes actual knowledge. However, it also includes imputed knowledge, such as where publicly-available information indicates a customer would divert something contrary to the EAR. Likewise, BIS may find that knowledge exists based on facts indicating that a high probability exists for unlawful diversion, or where a company disregards red flags that require further investigation.
- **Entities Headquartered, or Whose Ultimate Parent is Headquartered, in D:5 Countries.** BIS intends that the Data Center Rule will restrict remote access to computing equipment used in SI-related applications to companies headquartered or whose ultimate parents are headquartered in D:5 countries. Data centers will need, accordingly, to demonstrate whether their customers include those based in D:5 countries. Likewise, companies involved in supplying hardware, software, and technology to data centers will need to implement measures to confirm whether the data centers are, or may in the future be, involved with providing remote access to D:5 country-based companies.
- **Exports, Re-Exports, and In-Country Transfers.** The Data Center Rule would restrict certain exports from the United States, re-exports from a non-U.S. location to another non-U.S. location, and to in-country transfers of items outside of the United States. The Data Center Rule, therefore, applies to U.S. and non-U.S. companies. An in-country transfer can be prohibited for items lawfully within a non-U.S. location, but that ultimately would be transferred to data centers involved in restricted end-uses (e.g., in a case where a distributor acquired the equipment consistent with the EAR but has knowledge that a subsequent consignee will send the item to data centers contrary to the Data Center Rule).
- **Restricted Computing Equipment, Software and Technology.** The Data Center Rule covers items specified in certain ECCNs, particularly ICs in ECCN 3A090; computer equipment containing those ICs, which are covered in the "z" sub-paragraphs of ECCNs 3A001.z, 4A003.z, 4A004.z, 4A005.z, 5A002.z, 5A004.z, 5A992.z; computers in ECCN 4A090; and software and technology controlled under related ECCNs in Commerce Control List ("CCL") Categories 3D, 3E, 4D, 4E, 5D, and 5E. The Data Center Rule clarifies that where U.S.-origin ICs or U.S.-origin computing equipment under the ECCNs have been incorporated or commingled into or with a foreign made-item, the restriction still applies. The scope of the Data Center Rule, accordingly, would cover certain foreign-made equipment.

Practical Implications

Companies will need to carefully consider how each of these elements may be met, or

not met, under the circumstances of their transactions. As described below, we expect that throughout the supply chain to data centers, companies will need enhanced due diligence measures to identify and avoid transactions contrary to the Data Center Rule.

Data centers, in particular, will need to begin to identify where they may offer services to companies headquartered in or ultimately owned by companies in D:5 locations. The data centers should expect significant new demands for documentation and contractual assurances related to compliance with the Data Center Rule. Likewise, suppliers to non-U.S. data centers now will need to be able to confirm that their customers are not involved in violations of the Data Center Rule.

The IFR describes expected diligence to include information from the foreign data center to suppliers regarding the data center's compliance measures. In the absence of sufficient information to verify compliance with the Data Center Rule, BIS will deem suppliers to such data center to have knowledge under the EAR (i.e., the failure to confirm compliance can be deemed tantamount to violating the Data Center Rule).

In short, we expect the Data Center Rule to reverberate widely within the computing and software industries, impacting data centers, their suppliers, IC manufacturers, and those involved with software or technology required at data centers.

Other IFR Changes

In addition to the Data Center Rule, the IFR makes several other notable changs to the EAR. The IFR will restrict exports of certain ICs to Brazil, Indonesia, Malaysia, Singapore, and Thailand (countries where Chinese companies, in particular, are known to have established data centers and related operations in recent years). Those countries are deemed at higher risk for diversion contrary to the EAR under the IFR. The IFR also would adjust EAR restrictions relating to advanced-node logic chips. Finally, the IFR formally rescinds the Biden Administration AI-Diffusion rule, which the Trump Administration had declined to enforce but had not formally withdrawn. Companies should review these changes to assess whether they impact their sales or purchases.

Conclusion

Dorsey & Whitney’s National Security Law practice group has experienced counsel to help companies assess the impact of the IFR on their supply chains.

[1] As of the date of this update, the full list of D:5 countries under the EAR includes: Afghanistan, Belarus, Burma, Central African Republic, China (including Hong Kong), Cuba, the Democratic Republic of the Congo, Eritrea, Haiti, Iran, Iraq, North Korea, Lebanon, Libya, Nicaragua, Russia, Somalia, South Sudan, Sudan, Syria, Venezuela, and Zimbabwe. While Macau is not listed under Country Group D:5, this rule applies to Macau, and the references to D:5 countries in this update include Macau.