

Client Alert

Special Matters and Government Investigations

OCTOBER 15, 2024

For more information, contact:

Barry Kamar
+ 305 462 6044
bkamar@kslaw.com

Sumon Dantiki
+ 202 626 5591
sdantiki@kslaw.com

Christine Savage
+ 202 686 5541
csavage@kslaw.com

Jamieson Greer
+ 202 626 5509
jgreer@kslaw.com

Michael Galdo
+1 512 457 2081
mgaldo@kslaw.com

Danielle Pressler
+ 202 626 9122
dpressler@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20006
Tel. +1 202 737 0500

Austin
500 West 2nd Street
Suite 1800
Austin, Texas 78701
Tel. +1 512 457 2000

Miami
200 S Biscayne Boulevard
Suite 4700
Miami, Florida 33131
Tel. +1 305 462 6100

New Data Center Validated End User Program Creates Pathway To Export Advanced U.S. Technology; Rigorous Review and Vetting Required

Effective October 2, 2024, the U.S. Department of Commerce, Bureau of Industry and Security (BIS), amended the Export Administration Regulations (EAR), 15 C.F.R. Parts 730 – 774, to expand the Validated End User (VEU) Authorization program to include a VEU Authorization for overseas data centers in certain countries (“Data Center VEU Authorization”). The Data Center VEU Authorization is designed to allow easier shipment of advanced computing items, including circuits and computers, to pre-approved overseas data centers that undergo a thorough review to ensure, among other things, their physical and cybersecurity. Exports, reexports, and in-country transfers would generally require licenses. The Data Center VEU Authorization would allow the export or reexport to these data centers without the need to obtain licenses from BIS. In-country transfers are not permitted under the Data Center VEU Authorization unless the in-country transfer is to an authorized location by the same VEU.

Although the Data Center VEU Authorization offers a new authorization opportunity, the program requires a considerable application process and strict compliance with any granted authorization, including reporting requirements. Companies interested in leveraging the Data Center VEU Authorization program either as a prospective validated end user or supplier of eligible items must carefully consider the Data Center VEU Authorization requirements and will want to have a comprehensive compliance plan in place to ensure they operate in accordance with the authorization, including managing the reporting requirements.



BACKGROUND

BIS has the authority to regulate and issue licenses for the export of items subject to the EAR, including goods, software, and technology, from the United States, the reexport of items subject to the EAR from one non-U.S. country to another, and the in-country transfer of items subject to the EAR to new end uses or end users in the same non-U.S. country. The EAR includes the Commerce Control List (CCL), which lists Export Control Classification Numbers (ECCNs) that describe items and provide information about the reasons for control of the items.ⁱ An authorization, in the form of a license exception or license from BIS, may be required for the export, reexport, or in-country transfer of an item depending on the destination country, end-user, and/or end use. For example, a semiconductor classified under a certain ECCN may not require an authorization to a certain country because the semiconductor is not controlled for the country, unless it is destined for certain restricted end users or end uses. An export of the same item to a different country may require authorization to be shipped to the country, regardless of the end-user or end use.

In October 2022, BIS announced export controls related to certain advanced computing semiconductor chips and integrated circuits, supercomputer end uses, and semiconductor manufacturing. These controls were part of a broader strategy by the United States to prevent China and other countries of concern from acquiring sensitive U.S. advanced computing technologies that could be used to advance their military or artificial intelligence (AI) capabilities to pursue mass surveillance and intelligent weapons systems. Subsequently, in October 2023, BIS announced the broadening of the export controls to impose license requirements for certain additional countries and a world-wide license requirement for certain specified end uses related to China and other countries. The result of these licensing requirements has raised the regulatory burden on businesses wishing to build data centers using U.S. technology in many countries around the world.

VEU PROGRAM

BIS established the VEU Authorization program to identify entities, or VEUs, located in eligible destinations to which eligible items may be exported, reexported, or transferred under a general authorization instead of a license. VEUs are reviewed and approved by the U.S. Government in accordance with the EAR. The End-User Review Committee (ERC), composed of representatives from the U.S. Departments of State, Defense, Energy, Commerce, and other agencies as appropriate, are responsible for administering the VEU program.

On September 30, 2024, BIS announced that in October the VEU Authorization at Section 748.15 of the EAR would expand to include Data Center VEU Authorizations, establishing a new pathway for overseas data centers to potentially acquire advanced U.S. technology. BIS recognizes the critical role that data centers play in developing AI and seeks to facilitate international AI development in a way that minimizes risks to U.S. national security. As a result of this expansion, the VEU Authorization now has two types of VEU authorization mechanisms for which qualifying companies can apply: (1) the preexisting General VEU Authorization, which permits the export, reexport, and transfer to validated end-users of eligible items that will be used in specific locations in China and India, and the new Data Center VEU Authorization, which permits the export and reexport to validated end-users of eligible items that will be used in specific data centers.

Specifically, the new Data Center VEU Authorization program allows for the export or reexport of all items on the CCL that require a license to the eligible destination that are necessary for a data center, excluding items controlled for missile technology and crime control reasons or “600 series” items.ⁱⁱ If approved, a Data Center VEU Authorization may be used for destinations for which a license is required for ECCN 3A090 and 4A090 items, and .z items in CCL Categories 3, 4, and 5, except for destinations in Country Groups D:5 countries. ECCN 3A090 items are integrated circuits designed or



marketed for use in data centers with a total processing performance of 4800 or more. ECCN 4A090 items are computers and components that contain ECCN 3A090 integrated circuits. The items in the “.z category” are items that are not described in ECCNs 3A090 and 4A090, but have similar processing performance. Under current rules, these items require licenses to be exported or reexported to countries in Country Groups D:1, D:4, and D:5ⁱⁱⁱ (except for those countries listed in A:5 or A:6). Therefore, data centers located in countries listed in Country Groups D:1 and/or D:4 that are not also listed in Country Group D:5 may be able to apply for a Data Center VEU Authorization. As of October 2024, examples of eligible countries include: Egypt, Laos, Oman, Moldova, Pakistan, Qatar, Saudi Arabia, Turkmenistan, UAE, and Vietnam.

To be considered for a Data Center VEU Authorization and become a validated VEU end-user, a detailed advisory opinion request must be submitted to BIS. The application must include, among other information:

- the list of items, including goods, software, and technology proposed for the Data Center VEU Authorization and their end-use;
- the physical addresses of the locations where the items will be used;
- complete applicant information, including contact information, business ownership and structure, and any business activity or corporate relationships with government or military organizations;
- description of record-keeping processes that will support compliance with the Data Center VEU Authorization reporting requirements;
- description of the physical and logical security requirements for each location in which the items will be housed, including cybersecurity, third-party monitoring, and physical security requirements, such as employee access;
- an overview of the data center’s information security plan, including with respect to cybersecurity, technology control, personnel security, and incidents;
- an overview of the data center’s supply chain risk management plan designed to prevent China-origin equipment entering the data center environment and Chinese vendors in the supply chain; and
- an overview of the export control training and compliance program procedures.

A Data Center VEU Authorization applicant must certify that, among other things, the applicant will comply with all applicable VEU requirements and allow on-site reviews by U.S. Government officials to verify compliance. Importantly, a VEU application is deemed to be a continuing representation by the applicant. As a result, any material or substantive change of the information submitted must be promptly reported to BIS, whether the VEU authorization has been granted or is under consideration.

The ECR will review the Data Center VEU Authorization application. In addition to the information supplied in the application, the review process will consider the applicant’s compliance record, capabilities to comply with the VEU requirements and guard against the misuse and diversion of computing resources, and relationships with U.S. and non-U.S. entities. Furthermore, the prospective Data Center VEU host country must provide assurances to the U.S. Government about the safe and secure use of the technology. The U.S. Government will consider the status of export controls in the host country and its support and adherence to multilateral export control regimes.

After the review, BIS may then issue a Data Center VEU Authorization in the form of a letter. The Data Center VEU Authorization may include conditions related to physical security of the facility, prohibiting access to individuals



associated with certain entities or countries, or not providing computing power over certain levels to entities or countries of concern. Data centers will also have certain semiannual reporting requirements to BIS to help ensure compliance with the VEU Authorization program. The only permitted end-users under a Data Center Authorization are those validated end-users that are specifically identified by BIS in Supplement No. 7 to Part 748 of the EAR.

Items obtained under a Data Center VEU Authorization may not be used for any activities prohibited in Part 744 of the EAR, which concern end-user and end use controls. Eligible Data Center VEUs who obtain items under the program may only use the items at the end user's own facility located in an authorized destination, consume the items during use, or reexport the items if specifically authorized by BIS. As mentioned, in-country transfer are not permitted, unless the transfer is to a Data Center VEU authorized location by the same Data Center VEU.

TAKEAWAYS

China, Russia, and other countries restricted from acquiring advanced U.S. semiconductor technology have repeatedly employed transshipment networks to circumvent U.S. export controls by working with individuals or businesses located in countries with less restrictive controls who purchase U.S. technology and then divert the items. These transshipment concerns animate certain of the licensing requirements surrounding AI-related semiconductor goods.

The Data Center VEU Authorization program imposes significant hurdles at the application process. Non-U.S. data centers must undergo a rigorous review and vetting process to reap the significant commercial advantage of not requiring individualized licenses to acquire U.S. semiconductor technology.

King & Spalding has a global footprint, substantial industry experience, and a deep bench of former trade and national security government officials. It is uniquely positioned to help guide companies in complying with and navigating complex U.S. export controls and regulatory framework.



Special Matters & Government Investigations Partners

Gary Adamson
New York
+1 212 556 2113
gadamson@kslaw.com

Adam Baker
New York
+1 212 556 2376
abaker@kslaw.com

J.C. Boggs
Washington, DC
+1 202 626 2383
jboggs@kslaw.com

Christopher C. Burris
Atlanta
+1 404 572 4708
cburris@kslaw.com

Craig Carpenito
New York
+1 212 556 2142
ccarpenito@kslaw.com

Steve Cave
Northern Virginia
+1 703 245 1017
scave@kslaw.com

Michael J. Ciatti
Washington, DC
+1 202 661 7828
mciatti@kslaw.com

Daniel R. Coats
Washington, DC
+1 202 626 2642
dcoats@kslaw.com

Patrick M. Collins
Chicago
+1 312 764 6901
pcollins@kslaw.com

Alexander M. Crenshaw
Washington, DC
+1 202 626 8996
acrenshaw@kslaw.com

Sumon Dantiki
Washington, DC
+1 202 626 5591
sdantiki@kslaw.com

Ethan P. Davis
San Francisco
+1 415 318 1228
edavis@kslaw.com

Alan R. Dial
Washington, DC
+1 202 661 7977
adial@kslaw.com

Dan Donovan
Washington, DC
+1 202 626 7815
ddonovan@kslaw.com

Robert L. Ehrlich, Jr.
Washington, DC
+1 202 626 9710
rehrlch@kslaw.com

David Farber
Washington, DC
+1 202 626 2941
dfarber@kslaw.com

Zachary Fardon
Chicago
+1 312 764 6960
zfardon@kslaw.com

Emily Gordy
Washington, DC
+1 202 626 8974
egordy@kslaw.com

Leah B. Grossi
Washington, DC
+1 202 626 5511
lgrossi@kslaw.com

Ehren Halse
San Francisco
+1 415 318 1216
ehalse@kslaw.com

Zachary J. Harmon
Washington, DC
+1 202 626 5594
zharmon@kslaw.com

Ted Hester
Washington, DC
+1 202 626 2901
thester@kslaw.com

Max Hill, K.C.
London
+44 20 7551 2130
mhill@kslaw.com

Amy Schuller Hitchcock
Sacramento/San Francisco
+1 916 321 4819
ahitchcock@kslaw.com

John A. Horn
Atlanta
+1 404 572 2816
jhorn@kslaw.com

Andrew C. Hruska
New York
+1 212 556 2278
ahruska@kslaw.com

Rob Hur
Washington, DC
+1 202 383 8969
rhur@kslaw.com



Mark A. Jensen
Washington, DC
+1 202 626 5526
mjensen@kslaw.com

Dixie L. Johnson
Washington, DC
+1 202 626 8984
djohnson@kslaw.com

William Johnson
New York
+1 212 556 2125
wjohnson@kslaw.com

Barry Kamar
Miami
+1 305 462 6044
bkamar@kslaw.com

Allison F. Kassir
Washington, DC
+1 202 626 5600
akassir@kslaw.com

M. Alexander (Alec) Koch
Washington, DC
+1 202 626 8982
akoch@kslaw.com

Yelena Kotlarsky
New York
+1 212 556 2207
ykotlarsky@kslaw.com

Steve Kupka
Washington, DC
+1 202 626 5518
skupka@kslaw.com

Jade R. Lambert
Chicago
+1 312 764 6902
jlambert@kslaw.com

Jamie Allyson Lang
Los Angeles
+1 213 443 4325
jlang@kslaw.com

Raphael Larson
Washington, DC
+1 202 626 5440
rlarson@kslaw.com

Carmen Lawrence
New York
+1 212 556 2193
clawrence@kslaw.com

Brandt Leibe
Houston
+1 713 751 3235
bleibe@kslaw.com

Aaron W. Lipson
Atlanta
+1 404 572 2447
alipson@kslaw.com

Daniel E. Lungren
Washington, DC
+1 202 626 9120
dlungren@kslaw.com

William S. McClintock
Washington, DC
+1 202 626 2922
wmclintock@kslaw.com

Amelia Medina
Atlanta
+1 404 572 2747
amedina@kslaw.com

Kendrick B. Meek
Washington, DC
+212 626 5613
kmeek@kslaw.com

Andrew Michaelson
New York
+212 790 5358
amichaelson@kslaw.com

Jim C. Miller III
Washington, DC
+1 202 626 5580
jmiller@kslaw.com

Patrick Montgomery
Washington, DC
+1 202 626 5444
pmontgomery@kslaw.com

Paul B. Murphy
Atlanta/Washington, DC
+1 404 572 4730
pbmurphy@kslaw.com

Grant W. Nichols
Austin/Washington, DC
+1 512 457 2006
gnichols@kslaw.com

Alicia O'Brien
Washington, DC
+1 202 626 5548
aobrien@kslaw.com

Patrick Otlewski
Chicago
+1 312 764 6908
potlewski@kslaw.com

Michael R. Pauzé
Washington, DC
+1 202 626 3732
mpauze@kslaw.com

Michael A. Plotnick
Washington, DC
+1 202 626 3736
mplotnick@kslaw.com

Olivia Radin
New York
+1 212 556 2138
oradin@kslaw.com

John C. Richter
Washington, DC
+1 202 626 5617
jrichter@kslaw.com

Rod J. Rosenstein
Washington, DC
+1 202 626 9220
rosenstein@kslaw.com



Daniel C. Sale
Washington, DC
+1 202 626 2900
dsale@kslaw.com

Greg Scott
Sacramento/San Francisco
+1 916 321 4818
mscott@kslaw.com

Richard Sharpe
Singapore
+65 6303 6079
rsharpe@kslaw.com

Kyle Sheahen
New York
+1 212 556 2234
ksheahen@kslaw.com

Michael Shepard
San Francisco
+1 415 318 1221
mshepard@kslaw.com

Thomas Spulak
Miami
+1 305 462 6023
tspulak@kslaw.com

Aaron Stephens
London
+44 20 7551 2179
astephens@kslaw.com

Cliff Stricklin
Denver
+1 720 535 2327
cstricklin@kslaw.com

Jean Tamalet
Paris
+33 1 7300 3987
jtamalet@kslaw.com

Courtney D. Trombly
Washington, DC
+1 202 626 2935
ctrombly@kslaw.com

Rick Vacura
Northern Virginia
+1 703 245 1018
rvacura@kslaw.com

Anthony A. Williams
Washington, DC
+1 202 626 3730
awilliams@kslaw.com

David K. Willingham
Los Angeles
+1 213 218 4005
dwillingham@kslaw.com

David Wulfert
Washington, DC
+1 202 626 5570
dwulfert@kslaw.com

Sally Q. Yates
Atlanta/Washington, DC
+1 404 572 2723
syates@kslaw.com



ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,300 lawyers in 24 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered “Attorney Advertising.” View our [Privacy Notice](#).

ABU DHABI	CHARLOTTE	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY
ATLANTA	CHICAGO	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
AUSTIN	DALLAS	GENEVA	MIAMI	RIYADH	TOKYO
BRUSSELS	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.

ⁱ Items not described on the CCL are designated as “EAR99.”

ⁱⁱ The VEU does not allow for the export or reexport to eligible data centers of 600 series items. 600 series items are items that were formerly on the U.S. Munitions List or those covered by the Wassenaar Arrangement Munitions List (WAML)—the Wassenaar Arrangement is a multilateral export control regime that the United States and 41 other nations participate in.

ⁱⁱⁱ Country Group D:1 countries are those subject to national security controls and Country Group D:4 countries are those subject to missile technology controls. Country Group D:5 countries are those subject to arms embargoes as designated by the U.S. State Department. Data centers in these countries cannot participate in the Data Center VEU Authorization program. As of October 2024, Country Group D:5 includes Afghanistan, Belarus, Burma, Cambodia, Central African Republic, China, Democratic Republic of Congo, Cuba, Eritrea, Haiti, Iran, Iraq, North Korea, Lebanon, Libya, Nicaragua, Russia, Somalia, South Sudan, Sudan, Syria, Venezuela, and Zimbabwe.