CLIENT ALERT | March 20, 2026

What the Remote Access Security Act Means for Export Controls Compliance Programs

Key considerations and practical steps for data center companies, cloud services companies, and those operating on the cloud.

Key Points:

- **Closing the perceived "cloud loophole":** BIS has attempted over the last 15 years to clarify how export controls apply to modern cloud computing. Recent new controls on advanced computing items have highlighted what many perceive to be a gap in BIS's authorities, which helped spur the passage of RASA in the House.
- **Redefining remote access:** If enacted, RASA would expand BIS authority under US export controls to regulate remote access by foreign persons to items subject to the EAR through internet or cloud services.
- **Preparing for enactment:** Cloud providers and cloud users should understand how cloud computing rules currently apply to their company, how this could change if the bill is enacted, and how to minimize risk.

On January 12, 2026, the House of Representatives passed the Remote Access Security Act (RASA), which would grant the Commerce Department's Bureau of Industry and Security (BIS) authority to regulate remote access to items subject to the Export Administration Regulations (EAR) in the United States. This bill is intended to plug what some perceive as a gap in US export controls following BIS's attempts to clarify how export controls apply to the modern internet age from 2009 onward.

The bill now awaits Senate action in the Senate Banking, Housing, and Urban Affairs Committee. If enacted, the legislation could substantially expand the scope of the EAR and the export control compliance burden for companies operating on the cloud.

The Regulatory Framework

How BIS Has Approached Cloud Computing

The definition of "export" in the EAR predates the modern internet age and was designed for a world in which physical shipments and on-premise equipment was the norm — not one in which, for example, software and data reside in a data center in Germany and can be accessed instantaneously by an

engineer or a customer in Brazil. Over the past 15 years, BIS has attempted to clarify the definition of "export" to account for modern communication by issuing advisory opinions and regulatory amendments addressing the responsibilities of cloud providers and cloud users under the EAR.

BIS Advisory Opinions (2009-2014)

- The 2009 Advisory Opinion makes clear that the cloud provider is not the "exporter" of technology subject to the EAR when a cloud user leverages the provider's cloud computing resources to create and download that technology. The advisory opinion concludes that "the provider of the computational capacity would not be the 'exporter' under the EAR when the user exports data … resulting from use of the computational capacity."

- The 2011 Advisory Opinion concludes that because the cloud provider is not the exporter of technology that users access or download from its cloud network, the provider does not need deemed export licenses for foreign national IT staff who have access to export controlled data on that cloud network. A "deemed export" is defined in Section 734.13(b) as a release of technology or source code to a foreign national in the US. Under the deemed export rules, a license is required to provide source code or technology to a foreign national in the US if an export license would be required to export that same source code or technology to the foreign national's home country.[1]

- The 2014 Advisory Opinion clarifies that providing users access to what was then called a "cloud-based storefront" — but is now commonly understood to be a Software-as-a-Service (SaaS) — is not an export of software under the EAR, provided the users do not download the software. This advisory opinion states that "there is no export of software in the cloud-based storefront" where "users … utilize the software application … in the cloud, without downloading it." This opinion allowed the SaaS industry to grow rapidly without each customer interaction being treated as a potential export event.

These advisory opinions have several limitations: They are fact-specific, they are focused on the responsibilities of cloud providers (not cloud users), and they were never intended as a comprehensive set of rules that address all possible cloud computing situations.

The 2016 Encryption Carveout

After BIS published the three advisory opinions to address the responsibilities of cloud providers, it took steps to address the responsibilities of cloud users. In June 2016, BIS amended the EAR to introduce the so-called "end-to-end encryption rule" in Section 734.18 of the EAR. This regulation is intended to provide a safe harbor for exporters transmitting controlled technology and source code to the cloud, if the transaction meets certain conditions. Like the three advisory opinions, this rule was not intended to address all cloud computing situations but instead clarify how the rules apply to a particular set of facts.

The end-to-end encryption rule states that an EAR-regulated export does not take place when sending, taking, or storing technology or source code that is:

- unclassified;
- secured using end-to-end encryption;
- secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by "software" implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current US National Institute for Standards and Technology publications, or other equally or more effective cryptographic means; and
- not intentionally stored in a country listed in Country Group D:5 (*see* supplement no. 1 to part 740 of the EAR).

If an exporter transmits controlled technology or source code following this method, Section 734.19 of the EAR states that no export of that technology or source code occurs until the exporter provides access information to a person outside the US (or a foreign person in the US). The EAR defines "access information" to include the information needed to access the technology or source code, which could be a password, a decryption key, or even a file location.

This framework has enabled companies to store their data on cloud infrastructure globally, without necessarily needing to obtain export licensing to send that data outside the US. For example, a company seeking to back up unclassified emails to a non-US server may be able to rely on this rule without obtaining a license to export the controlled technology in those emails (or even examining whether the emails contain export-controlled technology in the first place). An "export" of export-controlled technology in the emails would take place in this case only if the company actually provides someone outside the US (or a foreign person in the US) with the means to access those emails.

Emerging Concern

Advanced Computing and the Perceived "Cloud Loophole"

Since 2016, as computing power has increased exponentially, and applications such as artificial intelligence (AI) have emerged as strategic national security priorities, concerns about potential gaps in the export control regime have grown. Starting in 2022, BIS issued a series of rules to control certain high-end graphical processing units (GPUs) destined to countries of concern such as China. However, even though countries of concern were prevented from being eligible to receive physical shipments of the chips, they were generally not prevented from remotely accessing GPUs in the US or other countries that were not subject to an EAR export license requirement. This apparent gap in US export controls came to the attention of lawmakers and helped spur the passage of RASA in the House.

RASA

Legislative History, Key Provisions, and Interpretive Questions

RASA traveled a winding path through Congress before reaching its current status. The House of Representatives first passed an earlier version of the bill (H.R. 8152) in September 2024, but the legislation stalled in the Senate. Representative Mike Lawler (R-N.Y.) reintroduced the bill as H.R. 2683 in April 2025, and the House Foreign Affairs Committee approved it unanimously (51-0) the same month. The full House passed the bill in January 2026 by a vote of 369-22.

On the Senate side, Senators Dave McCormick (R-Pa.) and Ron Wyden (D-Ore.), along with cosponsors Tom Cotton (R-Ark.) and Chris Coons (D-Del.), introduced a companion measure (S. 3519) in December 2025. The bill has been referred to the Senate Banking, Housing, and Urban Affairs Committee, where it currently awaits action.

Key Statutory Language: "Items Subject to the EAR"

RASA would amend the Export Control Reform Act (ECRA) of 2018, which gives BIS permanent authority to regulate exports. It would amend ECRA by adding a new definition of remote access, defining the term as: "access on a purposeful, knowing, reckless, or negligent basis to an item subject to the jurisdiction of the United States under this Act by a foreign person through a network connection, including the internet or a cloud computing service, from a location other than where the item is physically located if the Secretary determines that the use of the item could pose a serious risk to the national security or foreign policy of the United States."

The phrase "subject to the jurisdiction of the United States" is generally understood by BIS to be equivalent to "items subject to the EAR," which is defined in Section 734.3 of the EAR to include all items in the US, all US-origin items wherever located, certain foreign-made items with sufficient US content (de minimis), and certain foreign-produced direct products of US technology or software, unless specifically excluded in Section 734.3(b) of the EAR.

Sponsors of RASA have made it clear that the purpose of the legislation is to provide BIS with authority to restrict remote access to computing resources for AI. As Chairman of the House Select Committee on China John Moolenaar stated: "The CCP's [Chinese Communist Party] AI ambitions are being fueled by its access to American chips housed in data centers located outside of China. This bill brings our laws into the digital age and makes it clear that cloud compute is subject to U.S. export control law, just like physical chips." Senator McCormick similarly explained: "Under current law, bad actors can train AI models by accessing advanced chips under the jurisdiction of the US, and the Bureau of Industry and Security has no authority to require a license. This legislation closes this existing security gap by extending export controls to include remote access scenarios."

Although the amendments that RASA makes to ECRA provide BIS with authority to regulate remote access, these amendments do not describe the exact controls that should apply. For example, RASA

amends Section 4812 of ECRA — which gives the President authority to control exports, reexports, in-country transfers, and certain activities of US persons — to include "the remote access of items subject to the jurisdiction of the United States by a foreign person." Similarly, RASA amends Section 4815 of ECRA — which gives the President authority to establish a procedure to license exports, reexports, and in-country transfers — to include the authority to license remote access.

ECRA does not describe the exact controls that should apply to remote access. Therefore, if RASA clears Congress and is signed into law, BIS will have to issue regulations specifying what items will be subject to remote access restrictions, what license requirements will apply, and what the license review policies will be. Although remote access to GPUs was a major impetus for RASA, the authority that the bill would grant is broad enough to encompass a wide range of items subject to the EAR, and BIS's regulations could therefore apply to a much broader range of technologies, or conversely, only require licenses for remote access to certain items or for certain end users or end uses.

Other versions of the bill may hold clues as to some of the controls that BIS may impose. The version of the bill that is currently in the Senate states that remote access includes remote access to items subject to the EAR for purposes of training AI models that can help design, acquire, or use weapons of mass destruction, or that are capable of conducting offensive cyber operations or surveillance that would undermine human rights. The 2024 version of the bill also included remote access to quantum computers.

Practical Guidance

Preparing for Potential Enactment

Although passage of the bill in its current form is not certain, RASA has bipartisan support and is addressing what many consider to be a longstanding gap in US export controls, suggesting there is a fair chance it will eventually become law. Additionally, the authorization provided to BIS in the current version of the bill is broad enough to capture a range of cloud computing environments. Companies providing cloud services or using the cloud could therefore be impacted.

Both cloud providers and cloud users should understand how cloud computing rules currently apply to their company and how this could change if the bill is enacted, and take steps to minimize risk in this uncertain environment. Practical steps that companies can take now to prepare include:

- **Understand the current rules and how they may change:** Companies should make sure they understand how export controls apply to their situation today and how that may change if RASA is enacted. Companies should consider contingency plans in case remote access is cut off or they lose access to cloud resources temporarily while a license application is in process.
- **Review existing cloud access contracts:** Cloud providers and cloud users should understand the terms of their contracts and how they may be impacted if the legislation becomes law. For

new contracts or amendments to existing contracts, companies should consider adding protections to their contracts to mitigate the risk of potential remote access restrictions.

- **Reduce risks stemming from end users and end use:** Companies that provide remote access to entities in countries of concern (including Country Group D:5 entities) and entities of concern (such as military end users) are more likely to face restrictions if the legislation passes. Companies should consider screening customers and suppliers to understand their current customer base and implement new processes, procedures, and contractual terms to address potentially problematic end users and end uses going forward. Companies may also consider implementing enhanced monitoring mechanisms such as geo- and IP-based screening, identity and access management, and audit logging to more closely track who is using cloud resources.

We are following these developments closely and remain ready to assist with questions regarding RASA and the application of US export controls and US sanctions to data center companies, cloud services companies, and other parties that could be impacted by these potentially significant controls on the horizon.

Contacts

James H. Barker
james.barker@lw.com
+1.202.637.2200
Washington, D.C.

Les P. Carnegie
les.carnegie@lw.com
+1.202.637.1096
Washington, D.C.

Damara L. Chambers
damara.chambers@lw.com
+1.202.637.2300
Washington, D.C.

Andrew P. Galdes
andrew.galdes@lw.com
+1.202.637.2155
Washington, D.C.

Paul M. Rosen
paul.rosen@lw.com
+1.202.637.3354
Washington, D.C.

Aaron Amundson
aaron.amundson@lw.com
+1.202.521.5984
Washington, D.C.

Zachary N. Eddington
zachary.eddington@lw.com
+1.202.637.2105
Washington, D.C.

Ruchi G. Gill
ruchi.gill@lw.com
+1.202.654.7126
Washington, D.C.

Asia Y. Cadet
asia.cadet@lw.com
+1.202.637.2251
Washington, D.C.

Monica Calce
monica.calce@lw.com
+1.212.906.4850
New York

Matthew J. Crawford
matthew.crawford@lw.com
+1.617.880.4588
Boston

Dillon Riley Curtis
dillon.curtis@lw.com
+1.332.240.2484
New York

Joelle Hageboutros
joelle.hageboutros@lw.com
+1.332.420.2143
New York

Christine Kalpin
christine.kalpin@lw.com
+1.617.880.4713
Boston

Alexander Perkowski
alexander.perkowski@lw.com
+1.202.637.2200
Washington, D.C.

Ankita Satpathy
ankita.satpathy@lw.com
+1.202.521.5945
Washington, D.C.

Maria Stosz*
maria.stosz@lw.com
+1.415.395.8256
San Francisco

Amulya Vadapalli
amulya.vadapalli@lw.com
+44.20.7710.1865
London

*Not admitted to practice in California. Admitted to practice in Washington, D.C.

Endnotes

[1] Section 734.13(b) of the EAR defines the foreign national's home country as their most recent country of citizenship or permanent residence. BIS has issued additional FAQs on determining nationality or last country of permanent residence for deemed export purposes.