CONTRIBUTED CONTENT & PRESENTATIONS

Export Controls Evolving for Infosec Threats to Cloud, SaaS, IaaS, AI Platforms

MARCH 21, 2024

Authors: Jonathan R. Todd, Kristopher J. Chandler, Megan K. MacCallum

The growth of cloud services, Software-as-a-Service ("SaaS") and Infrastructure-as-a-Service ("IaaS") arrangements, Artificial Intelligence ("AI") models, and increased reliance on the use of outsourced technology service providers in recent years has been no less than exponential. Many enterprises rely upon these services, as do many consumers, without awareness of the technology supporting these platforms or the risks. Regulators with jurisdiction over aspects of these information technology products and their use are beginning to adapt to this environment.

We are tracking new guidance and rules across a number of regulatory agencies addressing threats to United States domestic industry and national security that continue to evolve. Action out of the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") is a perfect example of the changing information security terrain. BIS has shown an increasing focus on regulating the export, transfer and release of software and technology. This action takes the form of clarifying existing regulations in their applicability to emerging use of technology, and also issuing new rules that address perceived threats.

On Sept. 18, 2023, BIS made a technical change to regulatory provisions in an effort to clarify an ambiguity in the Export Administration Regulations (the "EAR") by identifying when a transfer of access information is akin to the release of software[i] and technology[ii] and would accordingly require a comparable authorization. Earlier this year, BIS also issued a Notice of Proposed Rulemaking for the implementation of Executive Orders governing IaaS providers (89 FR 5698) and certain requirements to combat an increasing threat of malicious cyber-enabled activity in the United States.

BIS Clarifications on Transfer of Access Information and Release

In a recent Final Rule[iii], BIS enacted a technical correction that "serves to clarify provisions of the EAR pertaining to the release of 'software'" and to "[clarify] an ambiguity in the EAR by adding a cross-reference addressing access information[iv] in the section on releases of 'technology' and 'software'". BIS stated that the new changes reflect the interpretation of terms BIS always intended, and the changes now make its intent crystal clear (the "Final Rule").

As originally enacted on June 3, 2016, and pursuant to 15 CFR § 734.15 (Release), a release of software and technology occurred either through: (1) Visual or other inspection by a foreign person of items that reveals "technology" or source code subject to the EAR to a foreign person; or (2) Oral or written exchanges with a foreign person of "technology" or source code in the United States or abroad.

The Final Rule clarifies through a cross reference to 15 CFR § 734.19 (Transfer of Access Information) that a "release" of software and technology also occurs, and a comparable authorization from BIS is required, when there is a transfer of access information with knowledge that such transfer would result in the release of such technology or software without a required authorization.

The Final Rule also expands on transfer of access information, making it clear that with respect to such transfer, "software" includes both source code and object code, and not just source code. This eliminates potential uncertainly that the definition of release under 15 CFR § 734.15 (Release) limits 15 CFR § 734.19 (Transfer of Access Information) might only control transfers of access information that release source code.

All regulated parties will now need to ensure they carefully consider whether the transfer of access information is akin to a software/technology release under the regulations that would require appropriate authorization to avoid potential pitfalls and federal enforcement actions.

BIS Proposed Rules on IaaS Provider Compliance

IaaS Providers will need to pay special attention to updates on the transfer of access information as well as to release of software and technology. Providers will also face the new obligation to conduct diligence, collect and report information, and change relationships with foreign resellers when IaaS products may enable malicious cyber activities.

BIS's Notice of Proposed Rulemaking issued on Jan. 29, 2024 (the "Notice") solicited comment on proposed regulations to implement two Executive Orders (89 FR 5698). EO 13984, published three years ago in 2021, directs the Department of Commerce to propose regulations to require U.S. providers IaaS products ("IaaS Providers") to verify the identity of foreign customers and to expand BIS oversight authority to implement measures to defer malicious foreign cyber actors from the use of U.S. IaaS products. EO 14110, published more recently in 2023, directs the adoption of regulations requiring IaaS Providers to submit certain AI training reports report to Commerce if there may be malicious cyber-enabled activity implications.

Acknowledging increased malicious cyber activities utilizing IaaS products, these Executive Orders and the proposed rulemaking are designed to address bad actors' leverage of new and evolving IaaS products to commit intellectual property and sensitive data theft, engage in covert espionage activities and threaten national security by targeting U.S. critical infrastructure.

Specifically, the Notice first draws upon authority from EO 13984 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities) to require that IaaS Providers utilize a Know-Your-Customer ("KYC") program or Customer Identification Program ("CIP") for verification of users that sign up for, or maintain accounts that access or use, U.S. IaaS providers' products or services. BIS will establish certain minimum standards for IaaS providers to verify these identities and will also describe the documentation and procedures required to verify the identities of any foreign persons acting as lessee or sub-lessee of IaaS products or services. BIS will additionally outline the records that IaaS providers must maintain and methods for limiting third-party access to the information collected.

Under EO 13984, BIS may also prohibit or impose conditions on a foreign person, or a person acting on behalf of a foreign person, from opening or maintaining certain IaaS accounts when the foreign person offers, engages in a pattern of offering, or is otherwise known to obtain U.S. IaaS products for a malicious cyber-enabled activity. BIS may do this if the foreign person is located in a foreign jurisdiction with a significant number of foreign persons offering U.S. IaaS products that are used for malicious cyber-enabled activities or if the account is on behalf of such a foreign person.

The Notice then draws upon authority from EO 14110 (Safe, Secure, and Trustworthy Development and use of Artificial Intelligence) to propose regulations for certain IaaS providers to report when a foreign person contracts with that IaaS provider or reseller to train a large AI model with malicious potential capability for malicious cyber-activity. The report must minimally include the identity of the foreign person involved and the existence of a training run that meets certain established criteria. BIS must also determine the set of technical conditions that a large AI model must possess in order to have the potential capabilities that could be used in malicious cyber-enabled activity, and to make updates as required.

Finally, under EO 14110, BIS requires that IaaS providers prohibit any foreign reseller of U.S. IaaS products from providing those products unless the foreign reseller submits a report to the IaaS provider, which the IaaS provider must then provide to Commerce, detailing each instance in which the foreign person transacts with foreign resellers to use the products to train a large AI model with potential capabilities that could be used in malicious, cyber-enabled activity. The IaaS provider must also ensure that foreign resellers verify the identity of any foreign person that obtains an IaaS account through their sales. BIS will establish minimum identity verification standards for IaaS providers to require from foreign resellers.

These new rules proposed by BIS provide expansive compliance obligations on entities leveraging new technologies and certainly will impact business operations. Those interested in providing comments to BIS regarding these proposed new rules must do so by April 29, 2024.

Risk Assessments, Focused Compliance and Operational Awareness Key

Our clients are facing a dynamic threat environment as geopolitics and emerging technologies collide. These technologies, particularly the potential for AI, make it increasingly critical for enterprises implementing new and evolving tools for everyday business operations to remain vigilant. These changes out of BIS are just one example of things to come. With new regulation comes new compliance burdens to protect essential connectivity, data, infrastructure and even national security. Additional legislative, agency rulemaking and enforcement actions are expected for 2024 and beyond as these tools continue to transform our workplaces.

A cross-functional team effort is required within and outside our clients. Benesch stands ready to assist with our resource set as your teams confront these risks and compliance obligations. Collaboration between our Intellectual Property, Artificial Intelligence and Transportation & Logistics teams provide that multi-dimensional clarity of vision. Our attorneys are experienced in developing sophisticated and business-friendly practices and procedures for all manner of safety and security threat or regulatory compliance.

Jonathan Todd is a partner in Benesch's Transportation & Logistics Practice that provides supply chain, export controls, economic sanctions, and import compliance counsel across a wide range of industries. You may reach him at (216) 363-4658 or jtodd@beneschlaw.com.

Kris Chandler is an associate in the firm's Intellectual Property and Transportation & Logistics Practices and is the leader of Benesch's AI Commission. He may be reached at (614) 620-2207 or kchandler@beneschlaw.com.

Megan K. MacCallum is an associate in the Transportation & Logistics Practice Group and may be reached at (216) 363-4185 and mmaccallum@beneschlaw.com.

---

[i] Software means: A collection of one or more 'programs' or 'microprograms' fixed in any tangible medium of express. 15 C.F.R. § 772.1.

[ii] Technology means: Information necessary for the "development," "production," "use," operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control "technology") of an item. 15 C.F.R. § 772.1.

[iii] Federal Register Vol. 88, No. 179, **Export Administration Regulations (EAR): Transfer of Access Information and Release of Software (Source Code and Object Code,** 09/18/2023.

[iv] Access Information means: Information that allows access to encrypted technology or encrypted software in an unencrypted form. Examples include decryption keys, network access codes, and passwords. 15 C.F.R. § 772.1.