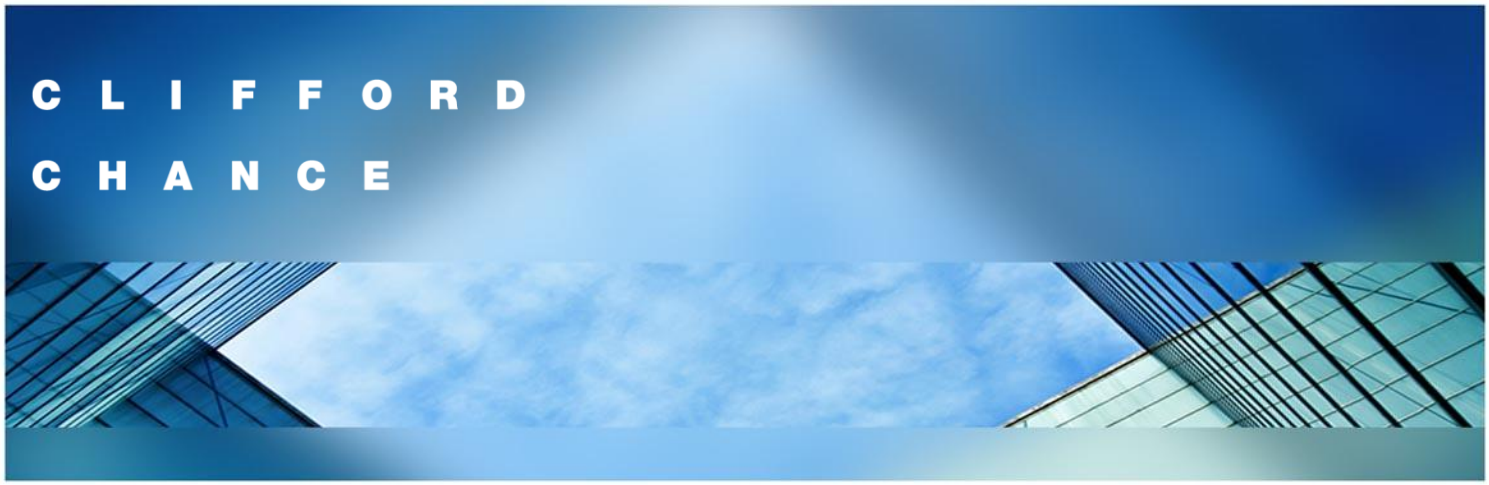

FRAMEWORK FOR ARTIFICIAL INTELLIGENCE DIFFUSION: A STEP FORWARD FOR US SECURITY AND ECONOMIC STRENGTH IN THE AGE OF AI

During its final weeks in office, the Biden Administration issued various regulations to strengthen American leadership in artificial intelligence (**AI**). These actions included an Executive Order directing federal agencies to lease sites for the development of frontier AI infrastructure and an Executive Order requiring government vendors and cloud providers to apply specific cybersecurity safeguards, while launching a new AI cyber defense pilot program. Key among these developments is the long-awaited interim final rule, Framework for Artificial Intelligence Diffusion, issued on January 13, 2025 by the U.S. Department of Commerce's Bureau of Industry and Security (**BIS**)(**Framework**).

While President Trump has already rescinded many of his predecessor's orders and actions, the above initiatives remain in force. It is unclear how Trump will address the Framework. He has indicated support for building data centers in the United States and his advisers include China skeptics. The Framework itself appears to have bipartisan support, and the Biden Administration has indicated that it consulted with the incoming administration on these rules.

FRAMEWORK FOR ARTIFICIAL INTELLIGENCE DIFFUSION: KEY FEATURES

The Framework aims to formulate a comprehensive strategy for managing AI using the power of export controls. According to the former Commerce Secretary Gina Raimondo, it is "*designed to safeguard the most advanced AI technology and ensure that it stays out of the hands of our foreign adversaries but also*

enabling the broad diffusion and sharing of the benefits with partner countries." The Framework builds on the existing export controls on advanced AI chips that the Biden Administration has put in place, by, among other developments, raising AI security standards, closing loopholes to ensure that advanced semiconductors sold abroad are not used by countries of concern to train advanced AI systems and restricting the transfer to non-trusted actors of model weights for advanced closed-weight models.

Key features of the Framework include:

- **Tiered Approach**. The Framework categorizes countries into three tiers, each with different access rights and security requirements for importing advanced AI chips and certain AI model weights:
    - **Tier 1** comprises the United States and 18 key allies and partners, who face no import or chip sale restrictions. This flexibility allows jurisdictions with robust technology protection regimes and aligned national security interests to benefit from seamless large-scale purchases. The Tier 1 countries include Australia, Canada, Japan, Taiwan, South Korea, New Zealand, Norway, the United Kingdom, and 10 of the 27 EU member states: Belgium, Denmark, Finland, France, Germany, Ireland, Italy, the Netherlands, Spain, and Sweden.
    - **Tier 2**, comprising most of the world, consists of 120 nations with significant trade and security relationships with the United States, such as Israel, Singapore, Saudi Arabia, the United Arab Emirates, Romania, Morocco, Turkey, Luxembourg, Czech Republic, Saudi Arabia, Brazil, Singapore, and Poland. These countries can receive exports only through companies that have joined the data center authorization program or obtained individual licenses.
    - **Tier 3** includes countries such as China and Russia, which face continued restrictions designed to prevent advanced AI chips from reaching arms-embargoed countries, stop the theft and unauthorized use of AI model weights, and slow the development of cutting-edge AI capabilities by US competitors.
- **Control Mechanisms**. The Framework imposes relative shares and absolute caps on the number of AI chips that companies can deploy in each country, serving as the primary mechanism for controlling AI diffusion globally. Additional mechanisms update Data Center Validated End User Authorization and provide exemptions for certain orders and shipments. The major control mechanisms are:
    - **Changes to Data Center Validated End-User Authorization**: BIS split the Data Center Validated End User authorization into Universal and National Validated End-User authorizations.
        - **Universal Validated End User (UVEU) Status**: Entities with high security and trust standards and headquartered in Tier 1 countries can obtain UVEU

status. This status allows entities to deploy up to 7% of their global AI processing capacity in various countries.

- **National Validated End User (NVEU) Status**: Entities with high security and trust standards and headquartered in Tier 2 countries can obtain NVEU status. This status enables entities to purchase processing capacity equivalent or to up to 320,000 advanced Graphics Processing Units (**GPUs**) over the next two years.

- **Cap for non-Validated End User (VEU) entities**: Non-VEU entities located in Tier 3 countries can purchase up to 50,000 advanced GPUs per country.
- **Government-to-government arrangements**: Government agreements aligning export controls, clean energy, and cybersecurity efforts with the US can double their chip caps to 100,000 advanced GPUs.
- **Exemption for certain orders**: Orders of up to 1,700 advanced GPUs do not require a license and do not count against national chip caps. Most chip orders are in this category and their streamlined processing is considered an important step forward.
- **Exemption for certain manufacturing/supply chain shipments**: To minimize supply chain disruptions, a license exception allows the export, reexport, and in-country transfer of Advanced AI Chip Items to a "private sector end user" located outside of, not headquartered in, and without an ultimate parent company in the Tier 3 group, for specific development, production, or storage activities.

- **Safeguards for VEUs**: Entities operating in Tier 2 countries are required to implement comprehensive safeguards to protect AI chips, secure model weights, and prevent misuse. These safeguards include cybersecurity standards, physical security protocols, personnel vetting, secure model weight storage requirements, and independence from Tier 3 countries for both supply chains and operations.
- **New Controls on AI Model Weights**: The Framework's new controls target advanced AI models by applying export restrictions to model weights that exceed a specific computational threshold. These model weights, which encode an AI system's learned capabilities, are crucial for the performance of sophisticated AI models. By imposing these controls, the Framework seeks to limit the proliferation of highly advanced AI technologies to unauthorized entities, thereby enhancing security and reducing the risk of misuse. Because publicly available model weights are exempt from these restrictions.

INDUSTRY RESPONSE

Proponents of the Framework believe that that the United States needs to act quickly to preserve its potentially dwindling AI advantage over competitors,

including China. The Chinese company DeepSeek made news recently when it released an open-source AI model that outperformed any American open-source language model, despite a global embargo on the sale of advanced AI chips to China. Proponents also highlight that the Framework does not hinder AI-driven data center expansion plans of cloud computing providers such as Amazon, Google and Microsoft. Data centers are an important source of economic activity and jobs, e.g., as consumers of electricity and steel, and US officials are encouraging companies to build data centers in the United States, rather than other regions.

Critics of the Framework worry that it could put US companies at a disadvantage and impede innovation, including by introducing costly compliance requirements. It could limit access to chips used for video games and consumer hardware and limit which companies could build data centers abroad. Some worry that the Framework would motivate buyers in the Middle East, Southeast Asia and other countries to buy their technologies from China. Others lament that the policy was "rushed out the door" before President Trump took office.

COMPLIANCE TIMELINE AND NEXT STEPS

While the Framework is effective as of January 13, 2025, the compliance date for the new licensing requirements is May 13, 2025, at which point the notice and comment period will also close.

Companies affected by the Framework are advised to familiarize themselves with its requirements and to map potential compliance gaps. We are available to discuss specific guidance and next steps.

CLIFFORD CHANCE

CONTACTS

Renée Latour
Partner

T +1 202 912 5509
E renee.latour
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Devika Kornbacher
Partner

T +1 713 821 2818
E devika.kornbacher
@cliffordchance.com

Michelle Williams
Partner

T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Inna Jackson
Tech Knowledge & Innovation Attorney – Americas

T +1 212 878 3292
E inna.jackson
@cliffordchance.com

Nicolas Friedlich
Associate

T +1 202 912 5197
E nicolas.friedlich
@cliffordchance.com

Curtis Sails III
Associate

T +1 202 912 5193
E curtis.sailsiii
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 2001 K Street NW, Washington, DC 20006-1001, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh* • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.