SheppardMullin
AI Law and Policy
Legal Considerations Involving Artificial Intelligence

Commerce Takes on AI: Recent Developments from BIS on AI

By Townsend Bourne, Lisa Mays & Jordan Mallory on October 30, 2024

Listen to this post

In two recent rules, the Department of Commerce, Bureau of Industry and Security (BIS) has begun to take significant steps to monitor, and potentially control access to, U.S. artificial intelligence (AI) technology. AI continues to pose a unique challenge for regulators due to its rapid expansion as a consumer product and potential defense applications.

Both rules stem from the October 2023 **AI Executive Order** (Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"). These rules also reach semiconductors that are necessary for building AI foundation models. Together, the two rules advance U.S. government efforts to regulate AI.

Proposed Rule Requiring Reporting on Dual-Use AI Capabilities

The **first rule proposes to establish reporting requirements for the development of dual-use AI models and computing clusters**. The rule implements the definition of dual-use foundation model under the AI Executive Order.**[1]**

1. **Reporting Requirements.** The rule proposes to require U.S. companies to submit quarterly reports to BIS when engaging in defined activities where AI development surpass certain technological thresholds as follows:
    - Training runs using more the 10^26 computational operations (e.g., integer or floating-point operations); or
    - Computing clusters with machines connected by data center networking of greater than 300Gbit/s and having a theoretical maximum greater than 10^20 computational operations (e.g., integer or floating-point operations) per second (OP/s) for AI training, without sparsity.
2. **Follow-up BIS Questions.** Following submission of a report, BIS will send the U.S. business follow-up questions. BIS will only allow 30 days to respond. The questions may cover any of the following topics:
    - Ongoing or Planned AI Activities: Any ongoing or merely planned activities within the next six months, including the development phase and hardware used for developing dual-use foundation models;
    - Ownership information: Any ownership and possession of the model weights of any dual-use foundation model; and
    - AI Red-Team Testing: Results of any developed dual-use foundation model's performance in relevant AI red-team testing, highlighting the model's safety, reliability, and cybersecurity measures taken to protect the equipment and model testing.
3. **Implications for U.S. Industry.** The imposition of these reporting requirements will mean greater oversight of AI development within the private sector. While this rule is still in the proposed stage, companies engaged in AI development should prepare for compliance with the reporting requirements. Regulators are expected to use this data to better understand the current capabilities of the U.S. AI industry and identify potential vulnerabilities related to national security concerns.

Final Rule Expanding Validated End-User (VEU) Program

The **second rule expands BIS's VEU Program** to include data centers in specified destinations. BIS is expanding the VEU Program to "recognize the advancement and benefits" of AI. This change provides a simpler path for companies to quickly export advanced semiconductors and electronic assemblies necessary for AI data centers to preapproved, trusted Validated End-Users.

1. **Expansion of the VEU Program to Additional Countries.** Previously, the VEU Program was limited to the export of certain items to preapproved end users in India and China. Now, the VEU Program has expanded to include data centers in countries where a license would be required to export advanced semiconductors and equipment (i.e., ECCNs 3A090 and 4A090, and .z items in Categories 3, 4, and 5) except to Country Group D:5 countries.
2. **VEU List.** Once approved, end user data centers will be identified in Supplement No. 7 to Part 748 of the Export Administration Regulations (EAR). Data centers listed on the VEU List will be authorized to receive an export without a license of any item on the Commerce Control List (CCL) necessary for a data center, except for 600-series items.
3. **Restrictions on End Use.** Additionally, these items must be consumed at the end user's own facility, and additional authorization is required to reexport the items. There are also further restrictions on end uses specific to China and India (largely restricting use of these items for any activities described in Part 744 of the EAR (e.g., developing chemical or biological weapons)).
4. **Enhanced Compliance Requirements.** In addition, data center end users will be subject to enhanced compliance obligations. Prospective data center VEU applicants must navigate an application process that details their cybersecurity, technology control, and personnel security plans, customer base, and other compliance procedures. Applicants should be prepared to address relationships with any entities on various U.S. export control and sanctions lists and demonstrate a robust export control program with training. Both reexporters and data center VEUs will be required to report on such activities semiannually.

This expansion of the VEU Program is a significant effort by BIS to balance the promotion of technological innovation with protecting national security interests.

FOOTNOTES

[1] The E.O. defined such models as those trained on broad data, generally uses self-supervision, contains at least tens of billions of parameters, is applicable across a wide range of contexts, and is capable of high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters.
