October 8, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the next page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

US AI Industry Reporting for Duty: BIS Rule Would Require Quarterly Filings for 'Dual-Use' AI Models and Computing Clusters

On September 11, 2024, the Department of Commerce's Bureau of Industry and Security (BIS) published a proposed rule that would require U.S. persons to report certain activities related to the development or acquisition of "dual-use" artificial intelligence (AI) models and computing clusters (Proposed Rule).

The Proposed Rule, which would be issued pursuant to the Defense Production Act of 1950 (DPA), implements one of the several mandates in the October 2023 Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," and is intended to inform the government about state of the U.S. defense industrial base's AI capabilities.

BIS has the authority under the DPA to conduct industry surveys, and the Proposed Rule would amend BIS's existing industry survey regulations by mandating ongoing periodic reporting related to relevant AI models and clusters.

Reporting Requirements

The Proposed Rule will require U.S. companies and other covered U.S. persons to submit quarterly reports and respond to questions from BIS if they engage in, or plan to engage in, "applicable activities," including:

- Conducting any AI model training run using more than 10^26 computational operations (*i.e.*, a "large-scale computing cluster").
- Acquiring, developing, or coming into possession of a computing cluster that has a set of machines transitively connected by data center networking of greater than 300/Gbit/s and having a theoretical maximum greater than 10^20 computational operations per second for AI training, without sparsity.

Required information would be both backward- and forward-looking — capturing the nature of the applicable activity undertaken in the past quarter and any planned applicable activities for the next two quarters, as well as the location of such activities. BIS also plans to follow up on such notices with question sets, to which the company will have 30 calendar days to respond, with responses to any follow-up questions due seven days from receipt. These questions will include, but may not be limited to, the following topics:

- Ongoing or planned training, development or production of dual-use foundation models.
- Ownership and possession of the "model weights" of dual-use foundation models, and the security measures in place to protect them.

- Results of a dual-use foundation model's performance in structured testing efforts to find flaws and vulnerabilities (*i.e.*, red-team testing).
- Information pertaining to the safety and reliability of dual-use foundation models or other national security concerns.

The Proposed Rule focuses on "dual-use foundation models" which are defined as AI models that: (a) are trained on broad data; (b) generally use self-supervision; (c) contain at least tens of billions of parameters; (d) are applicable across a wide range of contexts; and (e) exhibit, or could easily be modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination thereof that otherwise meet certain technical parameters set by BIS.

The Proposed Rule gives several examples, including "substantially lowering the barrier of entry for non-experts" to develop weapons of mass destruction, as well as automated cyber vulnerability detection and exploitation, but does not otherwise further define what is a serious risk to security, health, or safety. This definition also includes models that meet these criteria, even if they include technical safeguards intended to prevent users from utilizing the relevant unsafe capabilities of the model.

Any information submitted to BIS under the Proposed Rule will be treated as confidential and protected against public disclosure.

Next Steps

The Proposed Rule does not establish a timeline for implementation but, given the broad interest in the requested information, we expect BIS to move quickly to implement it. BIS is currently soliciting comments on the Proposed Rule, which are due October 11, 2024.

While the requirements of the Proposed Rule may be limited, information gathered by BIS through the Proposed Rule could inform future export controls or other restrictions on foreign access — particularly from countries of concern — to "dual-use" AI models which are not currently subject to strict export control restrictions. Such an expansion would complement existing export controls focused on AI-related hardware. See our October 25, 2023, client alert "BIS Updates October 2022 Semiconductor Export Control Rules."

While the Proposed Rule appears to reflect the U.S. government's overall caution against over-regulating a technology anticipated to be crucial to future defense capabilities, the Proposed Rule joins a number of other recent regulations that circle around the edges.

Contacts

Brian J. Egan
Partner / Washington, D.C.
202.371.7270
brian.egan@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Tatiana O. Sullivan
Counsel / Washington, D.C.
202.371.7063
tatiana.sullivan@skadden.com

Sammuel Kim
Associate / Washington, D.C.
202.371.7301
sammuel.kim@skadden.com

Patrick Stewart
Associate / Washington, D.C.
202.371.7348
patrick.stewart@skadden.com