WINSTON & STRAWN LLP

BLOG

Commerce Prepares for an AI Warfare Future with Quarterly Reports of AI Modeling and Computer Cluster Plans

SEPTEMBER 12, 2024

On September 11, 2024, the U.S. Department of Commerce's (Commerce) Bureau of Industry and Security (BIS) published a proposed rule in the Federal Register that would require quarterly reporting by organizations, companies, and corporations organized in the U.S. (including branches outside the U.S.) if they plan to either engage in artificial intelligence (AI) model training or acquire, develop, or otherwise possess a high-performance computing cluster for AI training (the Proposed Rule). The quarterly reports would give the U.S. government advance notice of activities that it may want to restrict from export, reexport, or transfer to the People's Republic of China (China), as well as insights into safety and other concerns relating to the use of AI in and for modern warfare.

BACKGROUND:

On October 30, 2023, President Biden signed Executive Order 14110 titled "Safe, Secure, and Trustworthy Artificial Intelligence." Section 4.2(a)(i)-(ii) of E.O. 14110 directs Commerce to collect information about "dual-use foundational models" (i.e., AI models that can be used for both civilian and military purposes) and large-scale computer clusters pursuant to the Defense Production Act (50 U.S.C. 4501 *et seq.*) (DPA). Commerce assigned the information collection task to BIS. The background section in the Proposed Rule cites examples of AI already making its way into the control of maneuverability, accuracy, and efficiency by defense articles, the performance of signals intelligence devices, and the speed at which cybersecurity software responds to attacks.

BIS is best known for its administration of the Export Administration Regulations (EAR), which regulate the export, reexport, and in-country transfer of goods, software, and technology (collectively, "Items") "subject to the EAR," as well as regulate some U.S. person activities pertaining to Items "not subject to the EAR." Through the EAR and international coordination with a variety of international partners, BIS has aggressively sought over the past two (2) years to prevent China from acquiring the advanced semiconductors, semiconductor manufacturing equipment, and related technologies and parts needed to advance its own domestic industry, including its ability to conduct AI model training for military purposes. BIS' latest edit to those AI-related export controls includes a September 6, 2024 Interim Final Rule imposing worldwide licensing requirements on quantum computing Items, gate-all-around field-effect transistor (GAAFET) semiconductor manufacturing equipment and technologies, and additive manufacturing equipment. The U.S. House of Representatives would like to see further edits to U.S. law to counter perceived threats emanating from China, including twelve (12) bills passed on September 9, 2024.

Less well-known are BIS' Industrial Base Surveys – Data Collection regulations (IBSR), which authorize BIS to conduct surveys of the defense industrial base pursuant to the DPA. The IBSR do not currently have any automatic reporting requirements – i.e., a survey must be issued by BIS before anyone is required to respond. BIS now proposes to implement automatic quarterly reporting through an entirely new section in the IBSR.

The following questions and answers detail the changes to the IBSR as proposed.

1. **When is the first report due?**

As this is merely a proposed rule, there is no final requirement to begin reporting.

However, the Proposed Rule requests comments on the quarterly notification schedule, storage of data collection (given the extreme sensitivity), and whether the thresholds for reportable "applicable activities" are appropriate. **Comments are due October 11, 2024.**

2. **The Proposed Rule will apply to "covered U.S. persons," but what does that mean?**

The Proposed Rule would apply to U.S. organizations, companies, and corporations (including non-profits such as academic institutions and research centers) established under the laws of the U.S. or any jurisdiction in the U.S., including their foreign branches, wherever located. Interestingly, the Proposed Rule makes no mention of subsidiaries of U.S. persons. The Proposed Rule would also cover all individual U.S. citizens, lawful permanent residents (green card holders), and any other person (including entities) located in the U.S.

3. **What is the reporting threshold?**

Covered U.S. persons must file a quarterly report if they engage in or plan to engage within six (6) months in an "applicable activity." There are two types:

- Section 702.7(a)(1) (the AI Model Training Activity): Conducting any AI model training run using more than 10^26 computational operations (e.g., integer or floating-point operations).
- Section 702.7(a)(2) (the Computer Cluster Activity): 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 (e.g., integer or floating-point operations) per second (OP/s) for AI training, without sparsity.

Representative of the government-wide effort regarding AI, the computational operations threshold for the AI Model Training Activity trigger matches the highest performance threshold under consideration for the U.S. Department of the Treasury's Outbound Investment Security Program.

Further, if a covered U.S. person makes just one quarterly report, they are on the hook for filing seven (7) consecutive quarterly affirmations of no "applicable activities."

4. **What is the proposed reporting schedule and what must be reported?**

"Notifications" describing planned "applicable activities" to BIS will be due on the following dates: April 15; July 15; October 15; and January 15. Planned "applicable activities" six (6) months in advance of the reporting date (e.g., through October 15 when reporting on April 15) will be reportable.

BIS anticipates asking questions following receipt of notifications, and a list of topics of potential interest are available in the Proposed Rule at paragraph (b)(1) for covered U.S. persons who would like to begin preparing responses:

- *Any ongoing or planned activities related to training, developing, or producing dual-use foundation models, including the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats;*

- *The ownership and possession of the model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights;*
- *The results of any developed dual-use foundation model's performance in relevant AI redteam testing, including a description of any associated measures the company has taken to meet safety objectives, such as mitigations to improve performance on these red-team tests and strengthen overall model security; and*
- *Other information pertaining to the safety and reliability of dual-use foundation models, or activities or risks that present concerns to U.S. national security.*

5. **What is the penalty for a failure to provide a timely and full notification?**

It is unclear whether the Proposed Rule will have significant bite. The IBSR contain authority arising from the DPA for BIS to issue and enforce a subpoena relating to a survey, and willful failures to comply with required responses to surveys carry a maximum penalty of $10,000, one year's imprisonment, or both.

The Proposed Rule does not, however, provide an independent regulatory authority for penalties. Given the Proposed Rule's ominous inclusion of the EAR "knowledge" standard (which goes beyond positive knowledge and includes an awareness of a high probability that a circumstance is substantially certain to occur), covered U.S. persons may end up having a high burden to alert the government in advance of their plans to engage in any "applicable activities" when the final reporting rules are released, likely in 2025.

* * * * *

Please reach out to the authors or your Winston relationship attorney if you would like assistance with preparing for the reporting obligations or submitting comments.
5 Min Read

Authors

Cari Stinebower

Tony Busch

Related Topics

Artificial Intelligence (AI) | China | Bureau of Industry and Security | U.S. Department of Commerce | Commerce Department

Related Capabilities

Artificial Intelligence (AI) | Technology, Media & Telecommunications

Related Professionals

Cari Stinebower

Tony Busch

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.