

# Commerce Department Proposes Reporting Requirements for Certain Artificial Intelligence Models and Computing Clusters

by Lawrence Ward, Justin T. Huff, Dave Townsend, and T. Augustine Lo

In a notice published on September 9, 2024, announcing a proposed rule and request for comment (“Proposed Rule”), the U.S. Department of Commerce called for new reporting requirements for the development of certain advanced artificial intelligence (“AI”) dual-use foundation models and computing clusters used to train such AI models. The Proposed Rule would apply broadly to companies involved with advanced dual-use foundation models and require them to report to the Bureau of Industry and Security (“BIS”) about their activities in the development of AI models or their use of computer clusters for them. The Proposed Rule does not by itself restrict these activities, but it would collect information that could lead to further regulation of cross-border AI-related activities. Comments on the Proposed Rule are due to BIS by October 11, 2024.

## Background About the Proposed Rule

On October 30, 2023, President Biden signed Executive Order 14110 (“EO 14110”), titled the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, to direct a U.S. Government-wide approach to AI issues, including mitigation of potential threats associated with the development of advanced AI models. Among the directives in EO 14110, President Biden instructed the Secretary of Commerce to require companies developing or demonstrating an intent to develop so-called AI “dual-use foundation models” or large-scale computing clusters to report certain data to the U.S. Government. Authority for the reporting requirements is established under the Defense Production Act to ensure that the U.S. industrial base is prepared to supply products and services to support U.S. defense. EO 14110 also relies on the International Emergency Economic Powers Act, among other legal authorities.

The Proposed Rule cites a number of situations that justify the new reporting requirements. In particular, the Proposed Rule states that “AI models are quickly becoming integral to numerous U.S. industries that are essential to the national defense,” including military equipment, signals intelligence, and cybersecurity software. The Proposed Rule states that AI enables broader and more efficient application of such

## Related People

- Lawrence Ward
- Justin T. Huff
- Dave Townsend
- T. Augustine Lo

## Related Capabilities

- National Security Law
- Artificial Intelligence

items and can increase the speed with which they respond to potential threats. The Proposed Rule thus concludes that “the U.S. Government must be ready to take actions that ensure dual-use foundation models produced by U.S. companies are available to the defense industrial base.”

In addition, the Proposed Rule claims that the required data will help the U.S. Government assess how the AI models operate, and whether they are suitable and ready for use in sensitive national security or defense applications. Finally, the Proposed Rule cites cybersecurity concerns as justifying the need for government visibility into certain private industry information about the training of AI models and use of cluster computers.

The Proposed Rule complements a [BIS proposal](#) from earlier this year that would impose know-your-customer (“KYC”) requirements on internet-as-a-service providers whose products assist with AI model development. BIS also issued that previous proposal under the authority of EO 14110.

### **Scope of New Proposed Reporting Requirements**

Under the Proposed Rule, companies involved with the two types of AI development activities must report to BIS: (1) certain training runs for dual-use foundation models and (2) their acquiring, developing, or coming into possession of certain computer clusters. U.S. companies<sup>[1]</sup> that engage in or plan to engage<sup>[2]</sup> in developing dual-use foundation models or that acquire, develop, or come into possession of computer clusters must report to BIS on a quarterly basis (see below as to the proposed data elements to be reported).

EO 14110 defines a dual-use foundation model as one that is “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 that exhibits, or could be easily 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 of those matters.”<sup>[3]</sup>

The Proposed Rule establishes technical standards that would trigger the reporting requirements related to training of a dual-use foundation model. In particular, the Proposed Rule requires reporting on the training of a dual-use foundation model if the training involves “more than  $10^{26}$  computational operations (e.g., integer or floating-point operations).”<sup>[4]</sup>

Separately, a large-scale computing cluster is defined as a set of computing items that are “transitively connected by networking of over 300 Gbit/s and having a theoretical maximum performance greater than  $10^{20}$  computational operations (e.g., integer or floating-point operations) per second (OP/s) for AI training, without sparsity.”

### **Data to Be Reported**

For companies and persons whose activities trigger reporting (see above), the Proposed Rule would require quarterly reports to BIS. The company or person would notify BIS that they are or intend to undertake reportable activities, which could then trigger the issuance of BIS questions as to those activities. The Proposed Rule provides, as examples, the following topics that BIS envisions asking about:

1. Activities related to training, developing, or producing dual-use foundation models, including physical and cybersecurity protections to assure the integrity of the training process;
2. Ownership and possession of model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect the model weights;
3. The results of any developed dual-use foundation model's performance in AI testing, including any safety objectives or mitigative measures taken to improve performance on tests and strengthen overall model security;
4. Other information pertaining to the safety and reliability of dual-use foundation model activities or risks they present to U.S. national security.

The Proposed Rule gives a reporting person or entity 30 days to answer such BIS questions and then allows further BIS follow-up questions that must also be answered. The Proposed Rule also imposes requirements as to the accuracy of the reported answers and when any such answers will need to be amended or changed by the reporting person or entity.

### **Implications for Industry**

The Proposed Rule is scant on details of how onerous these reporting requirements and BIS questionnaires will be. One possibility is that BIS may keep its questionnaires straightforward and uniform among companies and persons required to report, but it is also possible that BIS could use the questionnaires to collect detailed, company-specific, and wide-ranging information and data. In particular, since the reporting requirements are intended to help assess whether dual-use foundation models are suitable to use in national security or defense applications or if such models may be vulnerable to threats, BIS may have a strong incentive to pose more and more detailed questions to reporting persons or entities.

Of particular interest to multinational companies is the extent to which BIS will probe the development or use of foundation AI models by non-U.S. persons. For example, if a U.S. company permits a non-U.S. person to use a computer cluster for the development of a dual-use foundation model, this may involve significant questioning from BIS as to the non-U.S. person and its use of the computing cluster, which may or may not be in the possession of the U.S. company. Such "non-U.S. person" compliance issues under the Proposed Rule also might involve questions about non-U.S.-national personnel of a U.S. company who are employed by U.S. business units.

Companies may turn to contractual terms or clauses to ensure they have access to or could access data if needed for such BIS reporting. Under BIS's data collection regulations, which would incorporate the new reporting requirements under the Proposed Rule, BIS could impose civil penalties for failure to report the required data. The U.S.

Government also could criminally prosecute persons who willfully refuse to comply with these reporting requirements.

## **Conclusion**

Dorsey's attorneys in the international trade and national security practice can assist companies in assessing the Proposed Rule and preparing comments for Commerce's consideration. The attorneys profiled below would be happy to answer questions about this eUpdate.

[1] The reporting requirements apply to any covered U.S. person involved with advanced foundation AI models or certain activities related to acquiring computer clusters. The Proposed Rule defines a U.S. person as follows: "any individual U.S. citizen, lawful permanent resident of the United States as defined by the Immigration and Nationality Act, entity—including organizations, companies, and corporations—organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person (individual) located in the United States."

[2] The Proposed Rule would require reporting for companies and persons who intend to engage in reportable activities within the six-month period following the deadline for a report. For example, if a report is due on April 15, the reporting person or entity's report would have to cover its reportable activities intended to be undertaken through October 15.

[3] EO 14110, Section 3(k).

[4] According to the Proposed Rule, models trained on primarily biological sequence data and at the lower threshold of  $10^{23}$  computational operations will be addressed in a separate BIS reporting requirement.