October 11, 2024

Department of Commerce
Bureau of Industry and Security
14th St NW & Constitution Ave. NW
Washington, DC 20230

On behalf of the Center for Data Innovation, we are pleased to submit this response to the Bureau of Industry and Security's (BIS) proposed rule to establish reporting requirements for the development of advanced artificial intelligence (AI) models and computing clusters.[1]

The Center for Data Innovation studies the intersection of data, technology, and public policy. Its mission is to formulate and promote pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, AI, and the Internet of Things. The Center is part of the Information Technology and Innovation Foundation (ITIF), a nonprofit, nonpartisan think tank.

EXECUTIVE SUMMARY

The proposed rule would require companies developing or planning to develop large, dual-use AI models to report detailed information to the U.S. government, including activities related to AI model development, ownership and possession of model weights, and the cybersecurity measures in place to protect these models. The rule also mandates reporting for companies with large-scale computing clusters capable of running these models.

Knowledge is power, and collecting data about the status of the U.S. AI industry would help the federal government understand U.S. industrial capabilities in AI as well as potential vulnerabilities. However, the proposed requirements are closely tied to computing thresholds rather than performance thresholds. Computing thresholds are a poor standard for determining risk levels and could overlook high-performing AI models that use less compute. In addition, these reporting requirements could disproportionately burden open-source AI projects, which do not easily conform to traditional models of ownership and possession, and curtail open-source AI innovation.

[1] Federal Register. "Establishment of Reporting Requirements for the Development of Advanced Artificial Intelligence," https://www.federalregister.gov/documents/2024/09/11/2024-20529/establishment-of-reporting-requirements-for-the-development-of-advanced-artificial-intelligence.

Shift from Compute-Based Reporting to Performance-Based Reporting

The proposed rule focuses on computing power as a trigger for reporting, but that is a poor measure of AI model risk.[2] Some high-compute models could pose minimal threats, while lower-compute models with superior performance could present far greater risks. A shift to performance-based thresholds would provide a more accurate assessment of capability and risks, better identifying the most advanced AI models. These thresholds should be dynamic, evolving as AI capabilities and risks change, rather than relying on static compute-based measures.

Shifting from compute-based reporting to performance-based reporting would better align BIS's threshold with other departments within Commerce that are already tiering models. The AI Safety Institute (AISI) under the National Institute for Standards and Technology (NIST) published draft guidelines, *Managing Misuse Risk for Dual-Use Foundation Models (NIST AI 800-1)*, in July 2024.[3] These guidelines recommend assessing risks by evaluating capabilities rather than compute power. While the guidelines rightly recognize the relationship between a model's capability and its potential risk of harm can be unclear, its approach is still a far more effective starting point than relying on compute power alone.[4] By aligning the proposed rule with AISI's capabilities-based approach, BIS can ensure consistency across departments, improving the accuracy of AI model assessments and enabling better understanding of those that could pose national security concerns.

Adapt Requirements to Balance Approach for Open-Source and Closed Foundation Models

The proposed rule requires reporting on the "ownership and possession" of model weights and the cybersecurity protections in place. However, open-source models— sometimes developed collaboratively and without clear ownership—don't align with these requirements as easily as closed-source models do.

In open-source projects, it's often unclear who "owns" or "possesses" the model, making compliance difficult. Requiring developers to track and report ownership and security measures may create administrative and legal burdens that open-source contributors are not equipped to handle. These projects thrive on flexibility, with many contributors working informally or across borders. Imposing

[2] Sara Hooker, "On the Limitations of Compute Thresholds as a Governance Strategy," Cohere website, July 2024, https://cohere.com/research/papers/on-the-limitations-of-compute-thresholds-as-a-governance-strategy-2024.
[3] U.S. AI Safety Institute, "Managing Misuse Risk for Dual-Use Foundation Models," Initial Public Draft, July 9, 2024, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.800-1.ipd.pdf.
[4] Hodan Omaar, "Comments to AISI on Managing Misuse Risk for Dual-Use Foundation Models," (Center for Data Innovation, September 2024), https://datainnovation.org/2024/09/comments-to-aisi-on-managing-misuse-risk-for-dual-use-foundation-models.

centralized reporting requirements could discourage participation, slow development, and limit the sharing of improvements and ideas that drive innovation in open-source AI.

To avoid disadvantaging and stifling open-source AI, BIS should consider adjustments of reporting for open-source models, allowing for the continued growth of innovation while ensuring the necessary security oversight.

Yours sincerely,

Hodan Omaar
Senior Policy Manager
ITIF's Center for Data Innovation
homaar@datainnovation.org