TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

October 11, 2024

Bureau of Industry and Security
Herbert C. Hoover Federal Building
1401 Constitution Avenue NW
Washington, DC 20230

Re: Establishment of Reporting Requirements for the Development of Advanced Artificial Intelligence Models and Computing Clusters

To Whom It May Concern:

TechNet appreciates the opportunity to comment on the Bureau of Industry and Security's (BIS) proposed rule on "Establishment of Reporting Requirements for the Development of Advanced Artificial Intelligence Models and Computing Clusters." Many of our nation's leading AI developers, deployers, distributors, researchers, and users are TechNet members.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. Our membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.5 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

Reporting Cadence

BIS's proposed rule states that "all covered U.S. persons with models or clusters exceeding the technical thresholds for reporting should notify BIS on a quarterly basis". We are concerned that this rate is too frequent for meaningful updates to be reported and will impose a heavy burden on companies. The NPRM estimates that the reporting requirements will impose a total burden of 5,000 hours per year across all potential respondents. According to the NPRM, up to 15 companies may be affected, meaning BIS anticipates it will take approximately 333 hours for each respondent to complete all four quarterly reports. However, we believe this significantly underestimates the actual burden of quarterly reporting. Based on our member companies' experience with similar reporting obligations, the burden is considerably higher. Furthermore, the complexity of the information being requested makes these quarterly reports extremely time-consuming and resource intensive.

TechNet advises that BIS instead look to require a 6-month or annual reporting period. We also recommend allowing for a sixty-day collection period for the survey, with 30 days for organizations to respond to any corrections and 14 days to respond to additional follow up questions. We believe this frequency strikes a balance by providing the government with timely updates on innovation while granting responders the flexibility needed to accommodate the workload required and potential personnel fluctuations.

Reporting Clarifications

We strongly encourage BIS to establish clear criteria for the reporting process. The current proposal allows BIS to request information on almost any aspect of the safety and security of frontier model development or research clusters. This raises concerns that BIS could mandate customized reporting for each cycle, further increasing the reporting burden. We recommend that BIS define specific criteria, potentially leveraging its experience in gathering information under the President's Executive Order on AI.[1]

In order to help achieve this goal, as a first step we recommend that the BIS question content listed under Section 2(b)(2) be amended as follows:

"(2) BIS will send questions to the covered U.S. person which must address the following topics:

(i) Physical and cybersecurity protections taken to assure the integrity of the foundational model training process against sophisticated threats;
(ii) Physical and cybersecurity measures taken to protect the ownership and possession of the model weights of any dual-use foundation models; and
(iii) The results of any developed dual-use foundation model's performance in relevant AI red-team testing or evaluations, redacting sensitive information as appropriate, 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."

Dual-Use Foundation Model Definition

TechNet advises BIS to revise subsection (i)(E) under the definition of "dual-use foundation model." We believe "catastrophic risks" is more widely understood across the industry than "serious risks" which could capture several risk levels. By focusing on catastrophic risks, BIS can better focus their reporting requirements on information essential for national security.

We recommend that subsection (i)(E) be amended as follows:

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

"(E) Exhibits high levels of performance at tasks that pose a catastrophic risk (Catastrophic risk refers to AI's potential to cause large-scale, acute harm with devastating societal or global consequences through: (1) Intentional misuse by malicious actors, (2) Autonomous actions contrary to their intended design, (3) Disruption of existing strategic balances due to new capabilities) to security, national economic security, national public health or safety, or any combination of those matters, such as by:

(1) Substantially lowering the barrier of entry for non-experts, as compared to existing technological systems or platforms, to design, synthesize, acquire or use chemical, biological, radiological, or nuclear (CBRN) weapons or;
(2) Operating autonomously through means of deception or obfuscation."

Securing Sensitive Information

We recommend that all industry responses be submitted either through a secure portal or delivered in hardcopy directly to DOC headquarters, with all submissions uploaded to a TS/SCI secure system and the original copies destroyed. This approach aligns with the existing practices from the initial reporting requirements from the President's Executive Order on AI. We strongly advise against accepting submissions via nonsecure email or consolidating all responses in a single centralized location. Furthermore, we request that these submissions be explicitly excluded from FOIA requests to protect sensitive information. Additionally, we suggest that any individual with access to these submissions be subject to a government-mandated cooling-off period before transitioning to employment in an AI or AI-related company.

Determining Advanced Models

The proposed rule requires that U.S. persons engaged in "conducting any AI model training run using more than 10^26 computational operations (e.g, integer or floating-point operations [FLOPs])" be required to submit a notification to BIS. AI models that surpass these high FLOPs thresholds are assumed to pose a higher risk. However, we encourage BIS to review this assumption and whether this is the appropriate threshold to require additional reporting.

The computational threshold is being questioned within scientific communities, as there is increasing evidence that more computational power during training does not always correlate with higher risks.[2] Risks from AI models are influenced by factors not reflected in compute metrics, such as the quality of the data, the context in which the models are deployed, and safety optimizations. There have also been technical uncertainties regarding how to consistently calculate FLOPs, and industry has worked to put forward best practices to advance a uniform standard.[3] We are concerned that over reliance on compute-based thresholds could lead to a greater focus on managing compute power instead of addressing immediate or near-term risks and disproportionately scrutinizing models that exceed the

[2] https://arxiv.org/pdf/2407.05694v1

[3] https://www.frontiermodelforum.org/updates/issue-brief-measuring-training-compute/

threshold even if they don't pose more immediate risks to security, national economic security, or national public health or safety. We encourage BIS to explore alternative or complementary to compute-threshold methods to determine which AI models would fall under the oversight of this proposed rule. We advise examining flexible rather than fixed compute-thresholds, and provide clarity on how FLOPs should be calculated and measured.

Data Centers

TechNet would appreciate greater clarity on Section 2(a)(ii) which outlines that a U.S. person who has access to advanced computing power be required to report to BIS. Section 2(a)(ii) states that a U.S. person who "… com[es] 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." We are concerned that the mention of mere "possession" could capture organizations that partner or rent space from cloud service providers, while these entities don't necessarily have the ability to report what BIS is looking for. We would recommend that possession be modified to "ownership" or "physical possession" in order to better target U.S. persons that are the focus of BIS' proposed rule. We also advise that this section further refine that this requirement is focused on U.S. persons who own computing clusters that are being used explicitly for covered AI training activities.

Conclusion

We look forward to working with you on AI policy and appreciate the opportunity to discuss this innovative technology. We stand ready to serve as a resource to you in your examination of this important issue. Thank you for your consideration of our perspective.

Sincerely,

Carl Holshouser
Executive Vice President