October 11, 2024

The Honorable Thea D. Rozman Kendler
Assistant Secretary for Export Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: ITI Feedback to BIS Proposed Rule on Establishing Reporting Requirements for the Development of Advanced Artificial Intelligence Models and Computing Clusters (RIN 0694-AJ55)

Assistant Secretary Rozman Kendler,

The Information Technology Industry Council (ITI) welcomes the opportunity to provide feedback to the amendment of BIS Industrial Base Surveys – Data Collections regulations by establishing reporting requirements for the development of advanced artificial intelligence (AI) models and computing clusters under Section 4.2(a) of the Executive Order 14110 of October 30, 2023 (E.O 14110) (RIN 0694-AJ55).

ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, and other internet and technology-enabled companies that rely on ICT to evolve their businesses. Artificial Intelligence is a priority technology area for our member companies, who are both developing and using the technology to evolve their businesses.

ITI is committed to fostering the responsible development and deployment of AI. We have been actively engaged in shaping AI policy around the world. We have also been engaged with NIST on both AI and cybersecurity-related subjects throughout the last several years, including in the development of the Secure Software Development Framework (SSDF) and AI Risk Management Framework (AI RMF). We are also a member of the U.S. AI Safety Institute Consortium.

In 2021, we issued a set of *Global AI Policy Recommendations*, aimed at helping governments facilitate an environment that supports AI while simultaneously recognizing that there are challenges that need to be addressed as the uptake of AI grows around the world.[1] We also launched our AI Futures Initiative in 2023, an initiative comprised of technical and policy experts aimed at addressing challenging questions that are emerging in the global conversation on AI. We have published several policy papers via this Initiative, including our recently released *AI Accountability Framework,* as well

[1] Our complete *Global AI Policy Recommendations* are available here: https://www.itic.org/documents/artificial-intelligence/ITI_GlobalAIPrinciples_032321_v3.pdf

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

as papers on the *AI Value Chain and Foundation Models AI-Generated Content Authentication*.[2] It is with this background that we provide feedback on the rulemaking.

General Feedback

Below, we offer several high-level points, followed by specific responses.

BIS should:

Clarify the stated purpose for which information may be collected while making requests under the Defense Production Act (DPA) (50 U.S.C. 4501 *et seq*.)
We understand that BIS is collecting information pursuant to the authority granted to it under the Defense Production Act and that Section 4.2 (a)(i) of E.O 14110 provides guidance on the type of information that may be collected (such as ongoing or planned activity related to training and development of dual-use foundation models, results of red-teaming testing). It is important that BIS exercises its DPA authority in a careful and targeted way. This will build trust between the U.S. government and the entities that are required to report this information. By limiting the scope of its surveys to questions that directly promote secure and safe development and deployment of dual use foundation models, BIS can avoid setting a precedent that might unintentionally lead to broader or more intrusive data collection in the future.

As currently drafted, the rules do not indicate how the collection of the stated information – which may include confidential and commercially sensitive information – aids in "ensuring the supply of products and services to support national defense." We understand that "competitiveness" is a critical factor in supporting the overall defense industrial base, and that the DPA also authorizes the collection of this information to "perform industrial base studies assessing the capabilities of the U.S. industrial base." All of that being said, we encourage BIS to provide greater clarity around which rationale it is using to request this information, and to the extent possible, clarify how it intends to use the information. Is it merely for performing industrial base studies, or does BIS intend to use the information for something else? As stated earlier, articulating this information will help to foster a more collaborative process between those companies that are impacted by the reporting requirement and BIS, ultimately bolstering confidence and engendering trust.

We also suggest that as a part of the implementation of this reporting requirement, BIS establish a consultative mechanism that can serve as a forum for BIS and covered entities to discuss issues or otherwise field questions that may arise as a result of reporting requests. Such a mechanism can further build trust and facilitate the provision of the most accurate information in a timely manner.

[2] ITI's *Guide to AI Content Authentication* available here: https://www.itic.org/policy/ITI_AIContentAuthorizationPolicy_122123.pdf and ITI's *Understanding Foundation Models & the AI Value Chain* paper available here: https://www.itic.org/documents/artificial-intelligence/ITI_AIPolicyPrinciples_080323.pdf

Limit access to the requested information and clarify that requested information will be restricted in its use. We underscore that the information that may be reported is highly sensitive and should be protected appropriately. While the NPRM states that all information submitted to BIS will be treated as confidential, we request BIS clarify that all information submitted under the proposed rule be subject to relevant restrictions in its use, including exempting such information from requests under the Freedom of Information Act, 5, U.S.C. § 552. (FOIA) and ensuring that the information collected will be stored in BIS' most secure systems. BIS should also restrict access to this highly sensitive information to those employees/staff with the appropriate clearances and on a strictly need-to-know basis. Existing authorities such as the Trade Secrets Act, 18, U.S.C. § 1905 and confidentiality procedures built into the CFIUS regulations (31 CFR 800.802(e)) can serve as models for listing additional protections against the unauthorized access/distribution of sensitive material.

BIS should also articulate the specific measures it intends to take to preclude the divulgence of sensitive information by staff that have access to the information. Laying out these measures will help to foster trust and confidence with covered entities to ensure that sensitive information will be protected and not unnecessarily exposed to the public and unauthorized third parties.

Provide timely updates on technical parameters. We understand that the proposed rule relies on the collection thresholds for dual-use foundation models based on the technical specifications provided in E.O. 14110 (10^26 computational operations). Furthermore, E.O. 14110 also empowers the Commerce Department to update these collection thresholds – in this case, the proposed rule defines a new set of limits for large scale-computing clusters. As the technology evolves, BIS may be required to further revise the collection thresholds. Relatedly, the diverse methodologies experts have put forward[3] in calculating the threshold parameters for compute could result in different interpretations across the industry and divergences in reporting.

Therefore, we ask BIS to work with industry to ensure technical parameters affecting collection thresholds are defined using the latest technology, and are updated at a predictable cadence. It would also be helpful if BIS could provide additional guidance or a specific formula for calculating computational operations for purposes of the rule.

Specific Feedback

1. *Quarterly Notification Schedule*

The NPRM proposes a quarterly reporting regime for all covered persons or clusters. We believe that quarterly notification is too frequent, and will be overly burdensome for covered entities. BIS estimates in the NPRM that it will have an estimated burden of 5000 hours per year aggregated across all new respondents and has assessed that there are up to 15 companies that meet the proposed reporting thresholds for models and computing clusters.[4] It is possible that more

[3] *See Issue Brief: Measuring Training Compute*, Frontier Model Forum (May 2, 2024), https://www.frontiermodelforum.org/updates/issue-brief-measuring-training-compute.
[4] https://public-inspection.federalregister.gov/2024-20529.pdf

companies may be covered by the rule as the technology progresses and that the estimated burden may be more than 5000 hours per year. It would be helpful for BIS to clarify how it estimated the number of companies and man-hours as this information would better inform industry stakeholders on reporting thresholds.

Given the complexity of the information that may be requested, we believe that a quarterly report will be incredibly time and resource intensive. The vast scope of issues contemplated by the reporting requirement will necessitate coordination across a wide range of teams and a significant investment of time from subject matter experts within each firm's legal, infrastructure engineering, security, AI development, and AI evaluation and red teaming, and business development teams. As such, the quarterly reporting timeline will not only be a burden for the covered entities, but could also wind up being onerous for BIS to collect, process, and update stored information.

We understand that the quarterly reporting schedule has been proposed based on the development lifecycle of dual use foundation models. With the inclusion of reporting requirements around new computing clusters, covered entities will need additional time to ensure they are providing accurate information. This is because some entities may satisfy the collection thresholds for both dual use foundation models and large-scale computing clusters. Information for each technical parameter may, at times, require coordination with diverse teams – as explained earlier – within an organization and therefore, take extra time.

As such, we suggest modifying the reporting schedule to *a 6-month reporting period, with a 60-day collection period for the survey, with 30 days to respond to any corrections and 14 days to respond to additional follow up questions*.

Furthermore, we request BIS provide guidance on how the reporting regime will be operationalized. For example, will covered entities be required to report on model or cluster activity during each subsequent reporting period after the first report? Will entities be required to provide information on model and cluster activity that it decides to shut down? Providing additional guidance to covered organizations will ensure that they can easily comply with the rulemaking.

2. *Collection and Storage*

As we discuss earlier in our submission, we request that BIS clarify that collected information under the proposed rule will be exempt from FOIA requests and that it articulates the specific measures it will adopt to protect the submitted information. BIS should maintain the collection practices it has instituted under the current reporting requirement, ensuring that all industry responses are either submitted via a secure portal or delivered in hardcopy to the Department of Commerce headquarters and subsequently uploaded to a TS/SCI secure system, with the original copies destroyed. We advise against using nonsecure email for submissions or centralizing all submissions in a single location. Furthermore, we suggest that any individuals with access to the submissions be subject to a government-imposed cooling-off period before joining any companies that are actively developing dual-use foundation models. These measures will foster greater trust

and confidence among covered entities, ensuring that sensitive information remains protected from public and unauthorized third-party disclosure.

3. *Collection Thresholds*

Collection thresholds should be crafted based on industry standards to ensure the highest level of precision and consistency in reporting among companies. By adhering to these benchmarks, organizations can uniformly assess and communicate their data, thereby facilitating a more cohesive and reliable evaluation of dual-use foundation models. BIS should also work with industry and other stakeholders in the event the collection thresholds need to be modified.

While we understand that BIS may solicit information from covered entities on a variety of issues regarding activities on development, deployment, and ownership of dual-use foundation models as well as the results of any AI red team testing (based on guidance provided under Section 4.2(a) of E.O. 14110), given the sensitive nature of the information, we request that BIS revise the content listed under Section 2(b)(2). This will ensure a more targeted and precise application of its DPA authority. We request this section to be amended as follows:

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

- *Physical and cybersecurity protections taken to assure the integrity of the foundation model training process against sophisticated threats;*
- *Physical and cybersecurity measures taken to protect the ownership and possession of the model weights of any dual-use foundation models; and*
- *The results of any developed dual-use foundation model's performance in relevant AI red-team testing, 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."*

4. *Definitions*

a. *Dual-use foundation model*

We understand that BIS is relying on the definition of "Dual-use foundation model" as provided in E.O 14110. However, to ensure that submissions are sufficiently focused, we request that the definition of "Dual-use foundation model" be clarified as follows:

Under subsection (i)(E) of the definition for "Dual-use foundation model," change the existing language to:
"*Exhibits high levels of performance at tasks that pose a catastrophic risk, where catastrophic risk refers to AI's potential to cause large-scale, acute harm with devastating societal or global consequences through:*

- *Intentional misuse by malicious actors,*
- *Autonomous actions contrary to their intended design,*

- *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:*
- *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*
- *Operating autonomously through means of deception or obfuscation.*"

b. *Training or training run*

To ensure the rules are appropriately targeted and scoped, it is important to have a precise definition of "training or training run." The proposed definition may inadvertently include processes that are employed to improve already trained AI models. We understand that the intent of the draft rules is to cover training of models based on techniques such as unsupervised learning and reinforcement learning. As such, the definition should be clarified as follows:

"*Training or training run refers to any process by which an AI models learns from data using computing power. Training includes but is not limited to techniques employed during pre-training like unsupervised learning and employed during fine tuning like reinforcement from human feedback, but excludes techniques employed to optimize trained AI models.*"

c. *Large-scale computing clusters*

The proposed rules define large scale computing clusters to mean "*a set of machines transitively connected by a network of over 300 Gbit/s.....*" The term "transitively connected" is not an industry standard and by itself does not permit capability comparison between systems. For accurate and consistent reporting, we recommend a clarification to the definition of large-scale computing clusters.

Conclusion

In conclusion, we would like to thank BIS for the opportunity to provide comments on this important matter. Should you have any questions or require further clarification on any of the points raised, please do not hesitate to reach out. We are ready to assist in any way possible.

Thank you once again for considering our input.

***