October 11, 2024

Sean Delehanty
Office of Strategic Industries and Economic Security
Bureau of Industry and Security
Department of Commerce

Subject: RIN 0694-AJ55, *Establishing Reporting Requirements for the Development of Advanced AI Models & Computing Clusters*

Dear Mr. Delehanty:

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to comment on the proposed rule, *Establishing Reporting Requirements for the Development of Advanced AI Models & Computing Clusters, issued* by the Bureau of Industry and Security (BIS) (the Proposed Rule). The Proposed Rule would amend the BIS Industrial Base Surveys Data Collections regulations by establishing reporting requirements for the development of advanced artificial intelligence (AI) models and computing clusters under the Executive Order (EO) 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

SIIA is the principal trade association for companies in the business of information. Our membership of nearly 400 companies reflects the broad and diverse landscape of digital content providers and users in academic publishing, education technology, financial information, software, platforms, data analytics, and information services. Our members include upstream and downstream AI designers, developers, and deployers of AI systems across various environments.

BIS has a critical role in safeguarding national security and U.S. interests through administration of the U.S. export controls regime, and we recognize this expertise is an important factor in its delegation of responsibilities under Section 4.2(a) of EO 14110 and the Defense Production Act. EO 14110 reflects a balancing of interests in advancing safe, secure, and trustworthy AI while promoting U.S. competitiveness and continued innovation in this still emerging field. initiatives SIIA supports this vision, and we believe the balancing of interests is critical in advancing the objectives of Section 4.2(a). In that spirit, we provide the following comments. These reflect our concerns that the Proposed Rule's quarterly reporting requirements would impose significant operational burdens on companies that are developing advanced AI models. Achieving a balance between security imperatives and practical industry capabilities will be essential for fostering innovation, maintaining sustainable oversight, and ensuring that U.S. innovation does not fall behind in a globally competitive environment. We also recommend that BIS provide further clarity on safeguarding collection and storage of sensitive data and ensure that the scope and quality of information sought is manageable both for companies and for BIS itself. Lastly, we recommend that BIS consider the international landscape and the importance of harmonizing requirements with those being developed in other jurisdictions that may exercise regulatory authority over U.S. companies.

Frequency and Burden of Reporting (Comments on Quarterly Notification Schedule)

SIIA is concerned about the quarterly reporting structure laid out in this proposal, as this frequency poses significant operational burdens for companies. The proposed rule estimates that the reporting requirements will result in a burden of 5,000 hours per year spread across all potential respondents. The proposed rule predicts there are up to 15 companies likely to fall within scope, which means BIS anticipates it will take ~333 hours for each respondent to complete all 4 quarterly reports. Our member companies' experience indicates that quarterly reporting at this level is considerably more time-intensive than estimated, given the complexity of the data required. We are also concerned that the proposed notification and reporting cadence may particularly place burdens on emerging start-ups and businesses eager to leverage AI, including within the context of delivering service to the national security community.

SIIA believes a semi-annual or annual cadence would more effectively balance the need for information with the practical realities companies face. A less frequent schedule would alleviate the strain on resources and allow companies to focus more on innovating and streamlining operational effectiveness. Additionally, we request that BIS provide more comprehensive guidance on the specific logistics of reporting, such as whether ongoing reports are required for models or computing clusters in continuous use. Clarity on these operational processes would enhance industry compliance and accuracy.

Data Confidentiality and Security Measures (Comments on Collection and Storage)

SIIA urges BIS to prioritize confidentiality for any information collected through this reporting process. We recommend that BIS clarify how it will safeguard this sensitive information, including whether it will be exempting it from FOIA requests. The agency should adopt robust security protocols to prevent misuse or unauthorized access, possibly modeled after CISA's secure software development attestation portals, to mitigate risks associated with data collection and storage, particularly given recent breaches affecting government-held information.[1] Regardless of approach, information should be kept in an isolated environment with careful access controls and measures to restrict exfiltration. For example, there are risks associated with using email, and we do not view this as the most appropriate method for delivery of sensitive information regarding AI models. The practice of encrypting email attachments and separately emailing the attachment password creates significant risks if an inbox client becomes accessible to a malicious actor.

We urge the Department to act with caution in determining the type and quantity of data that it requires to be collected from applicable companies, and suggest adopting strict data minimization standards to ensure that responding organizations collate and return only those records that are narrowly tailored to the "national defense" concerns as outlined in the proposed rule.

[1] https://www.cisa.gov/resources-tools/resources/secure-software-development-attestation-form

Revisiting the Scope and Quality of Information Collection (Comments on Collection Thresholds)

We are concerned that the breadth of the proposed information collection requirements may result in an overwhelming volume of data that could diminish the value of the information for BIS and its delegated responsibilities under Section 4.2(a) of EO 14110. SIIA suggests that BIS streamline the survey content, focusing only on data points critical to achieving national security objectives, which will not only reduce undue burdens on industry, but also provide a manageable amount of information for BIS to process and evaluate.

BIS should approach its thresholds for reporting in such a way as to drive consistency

across respondents. For example, there are various methodologies for calculating compute usage, such as those based on counting arithmetic operations, and different approaches may present advantages and tradeoffs. For compute-based threshold proposals to fulfill their objectives, there should be a baseline degree of consistency in how model developers can measure and report training compute. Since BIS issued its initial survey, companies that are members of the Frontier Model Forum have aligned on a set of proposed methodology principles for calculating the compute cost of models.[2] We recommend that BIS mirror these principles in its approach to determining which models are in scope for reporting.

Additionally, we believe that BIS should allow covered organizations to respond to certain survey questions with nuance by offering more open-ended, explanatory responses in order to reflect the evolving nature of AI safety practices. There are some particular circumstances where we see value in this:

- The reporting may be focused on dual-use foundation models, as mandated by the US Executive Order on AI, but to be most useful, the questionnaire should allow respondents to reflect that many mitigations will be appropriately implemented at a combination of the model and application level.
- Reporting should reflect more nuance in how companies' frontier safety frameworks (for those who have adopted them) are evolving: it will frequently be more appropriate to consider whether the right safety mitigations have been implemented, rather than focusing on the concept of a "pause" in development or deployment.
- BIS's questions should reflect the scope of the role that external evaluators actually play in companies' governance practices. While they are highly valuable inputs for risk assessment and management, they are not typically in a position to make general determinations as to the suitability (or lack thereof) of an AI model for deployment.

Harmonization and Collaboration on Refinements as Technology Evolves

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

We encourage BIS to advance an agile approach to reporting requirements to facilitate alignment with international and foreign reporting requirements that are still in the formative stage. This includes, for example, ongoing work to develop a Code of Practice for general purpose AI under the EU AI Act, and efforts underway among the International Network of AI Safety Institutes., This approach will assist in the development and deployment of safe AI and reduce duplication for companies operating in multiple jurisdictions by ensuring consistent, coordinated information collection.

Additionally, we recommend that BIS consult with industry stakeholders on future survey revisions to reflect evolving technologies and AI safety practices more accurately. There are certain domains in the survey that will likely need to be refined over time given the evolving nature of the technology. One example is the set of benchmarks collected to assess general performance for dual-use foundation models. Currently, the field is gravitating toward certain benchmarks, but these are imperfect proxies, have some risk of gaming, and are likely to shift over time. Another example involves questions related to model evaluations: given the early state of the science of conducting dangerous capability evaluations, BIS should refine the questions over time to make sure they specify the right unwanted model behaviors, grounded in threat models.

Conclusion

In conclusion, SIIA recommends that BIS consider adopting a semi-annual or annual reporting frequency, revisit the scope of data collected, and implement stringent data security measures. We urge BIS to continue engaging with industry to create a manageable and effective framework that enhances national security without imposing unnecessary burdens on companies.

Thank you for considering our views. We look forward to working with BIS on these important issues.

Sincerely,

Paul Lekas
Senior Vice President, Head of Global Public Policy & Government Affairs
Software & Information Industry Association

Bethany Abbate
Manger, Artificial Intelligence Policy
Software & Information Industry Association