**Comment on Reporting Requirements for the Development of Advanced Artificial Intelligence Models and Computing Clusters**

On behalf of a concerned and interested citizen, thank you for the opportunity to comment. Artificial Intelligence and how it impacts national defense and security is an important issue. It is good that the government is addressing it in some concrete ways, and doing so early, due to the potential that such technology could have.

The definition of “dual-use foundation model” is overly broad., and should be narrowed to cover national defense as defined in the DPA, and public health. The definition includes “high levels of performance at tasks that pose a serious risk to security, national economic security, national public health safety, or any combinations of these matters.” This definition includes a variety of vague potential threats without much of clear definition as to what they actually cover. For example, does economic security refer to just materials for making weapons (steel). Does it include resources for surveillance technology (silicon in chips). Or does it even include resources that are needed to make the general economy function (oil). There is no clarity based upon the vague definition used above. With such a broad definition it easy to see how such a regulation could affect a wide range of industries that potentially have no real security threat, but now have to suffer the extra cost of reporting.

The department claims that it will apply the reporting requirement to dual-use foundation that meet technical conditions issued by the department. Such technical conditions have yet to be released, and there is no indication as to what they could be, or how they might affect the scope of the regulation. When looking at section 4.2(b) of E.O. 14110 it seems that the government is worried about the ownership and possession of the models. Presumably that such models would fall into the possession or ownership of adversaries. While this makes some sense, it does not contend with the overall issues surrounding the breadth of the reporting requirement. Without clear terms as to what the technical conditions are, or whether they affect the scope of the reporting, it fails to serve as much of a mitigating tool on the breadth of the reporting requirement.

The DPA’s term of national defense includes “programs for military and energy production or construction, military or critical infrastructure assistance to any foreign nation, homeland security, stockpiling, space, and directly related activity.” The focus on military and energy production is substantially narrower than the definition used previously and allows for a much clearer focus as to what the act means to regulate. As such, this definition is preferable to the one used above.

Given the experience of the pandemic, public health seems to be an issue of substantial enough security importance as to be covered under the meaning of the act.

An additional issue with the act comes with the inclusion of signal intelligence devices. The use of AI surveillance technology, of which cameras are a part of, is a worrying trend within our country and globally. As Beraja, Kao, Yang, and Yuchtman’s article “AI-tocracy” in the Quarterly Journal of Economics noted autocratic regimes, such as China, benefit from AI technology especially facial recognition when it comes to crushing democracy and dissent. Beraja, Kao, Yang, and Yuchtman, *AI-tocracy*, Quartey Journal of Economics, Vol. 138, Issue 3, August 2023. Having reporting requirements to keep tabs on such technology, is not in itself a bad thing, however, there is a deeper question as to whether such powerful surveillance tools should be developed and used at all. Many other countries are investing in this kind of technology, and the United States already uses it, but that does not mean that we should. Perhaps such a reevaluation is beyond the scope of this rule, but the more that it is used in this rule, and in future rules, the more legitimized it becomes. In the interests of democracy, we should consider reversing this.