Center for AI Policy

Response to RFC on provisions for US investment into certain national security technologies

Executive Summary

The Center for AI Policy (CAIP) broadly supports the proposed rule as a means to implement Executive Order 14105. The proposed rule seeks to create visibility over and, in some cases, limit US investment into cutting-edge technologies that threaten national security. It clearly defines which US investments require notification and which are prohibited activities, with only one minor clarification required. Furthermore, the definitions of which entities are 'covered persons', either directly or indirectly, are comprehensive and clear.

CAIP offers four suggestions to ensure the successful implementation of the Executive Order. First, dedicated technical staff are necessary to remain responsive to changes in the sectors of semiconductors and microelectronics, quantum information technologies, and artificial intelligence. Second, the Department should share notifications analysis with the relevant security and intelligence agencies to proactively identify national security threats. Third, additional detail on the definition and timing of 'reasonable and diligent inquiry' would clarify the knowledge standard. Fourth, it is worth clarifying the definition of which AI systems are 'designed to be used for any government intelligence or mass surveillance end-use' and therefore are notifiable transactions.

Finally, CAIP would like to highlight that other adversarial states and non-state actors can also pose a national security threat. Thus, these provisions only address one aspect of the threat augmented by advanced technologies. If focused on a broader mitigation of national security risk, the Department may consider expanding the notifiable transactions to include other countries. Going forward, the investment guidelines for a 'reasonable and diligent inquiry' may also provide a foundation for 'Know Your Customer' guidelines regarding AI users.

1. Intent of the rule

This proposed rule sets forth regulations that would implement Executive Order 14105 of August 9, 2023, "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern". This Executive Order identified China, The Special Administrative Region of Hong Kong, and The Special Administrative Region of Macau as 'countries of concern'. It highlighted the threat of these countries having access to advanced technologies to advance their military and intelligence objectives. The Executive Order requests

categorization of semiconductors and microelectronics, quantum information technologies, and artificial intelligence into ‘notifiable’ and ‘prohibited’ transactions.

2. Strengths of the proposed rule

The proposed rule will likely achieve the goals of the Executive Order with minimal unintended consequences and limited loopholes. CAIP would like to highlight the clear definitions of ‘notifiable’ and ‘prohibited’ transactions, and to express support for the Department’s use of computing power to identify ‘covered activity’ until more effective, nuanced benchmarks become available. The definition of covered person, including more complex entity structures, is comprehensive and clear.

3. Suggestions for the proposed rule

3a. Resources to remain responsive to changes in sectors

The Department estimates that a maximum of $2 million annually will be spent on personnel costs related to analyzing notifications and promoting compliance (see excerpt below). CAIP supports the Department’s commitment to ensuring it is appropriately staffed and suggests that technical staff will be critical to remaining responsive to changes in these advanced technology sectors.

> **Excerpt on resourcing from proposed rule**[1]
>
> *“The Department of the Treasury and other relevant agencies, including the Department of Commerce, may incur additional costs… This includes other responsibilities related to the implementation of the proposed rule such as analyzing notifications submitted as well as complying with the reporting requirements under the Outbound Order… Furthermore, costs may be associated with efforts to promote compliance with the notification requirement and prohibition requirements, potentially including education on the requirements, development of guidance and frequently asked questions, and conducting stakeholder outreach. The Department of the Treasury does not currently have specific estimates for these costs but estimates that there would be personnel costs of less than $2 million associated with the proposed regulation in Fiscal Year 2024 with additional costs for ongoing outreach and enforcement thereafter. The Department of the Treasury and other government agencies may also incur costs in enforcing compliance with the regulation.”*

To ensure that regulations are keeping pace with technological development, the Department will need technical staff who can monitor and analyze ongoing changes in the AI marketplace. For example, any improvements in algorithmic efficiency will reduce the computing power required for a given capability and thus indirectly increase the capability threshold permitted by the proposed rule. Without technical staff to analyze such effects, the Department’s proposed rule may quickly lose its intended efficacy.

---

[1] Excerpt “Costs to the U.S. Government”, Page 93-94

These do not necessarily need to be full-time roles. While we recommend that these roles are within the Department for ease of communication, such monitoring could potentially be achieved through leveraging talent in another agency. Regardless of the specific staffing decision, there need to be several roles within government that have such technical monitoring as an explicit responsibility.

3b. Reporting for threat analysis

Regarding the analysis of notifications, CAIP recommends that the Department compile a monthly report on the distribution of investments into advanced technologies by geography, industry and type of owner, as well as the primary purposes of technologies, and any pattern in the flow and stockpiles of hardware. Given the scope of the Executive Order is limited to three 'countries of concern', this view will be inherently restricted, but still valuable. This analysis of notifications should be shared with the relevant security or intelligence agency to proactively identify major security risks.

3c. Clarification of the knowledge standard

CAIP supports the Department's indicators of a 'reasonable and diligent inquiry' as listed in § *850.104* – Knowledge standard on page 117-119. To further clarify the knowledge standard and ensure the efficacy of the proposed rule, CAIP suggests the Department add that "an inquiry will be deemed reasonable and diligent, if and only if, based on these factors, it will typically be adequate to correctly identify persons of concern".

CAIP also recommends that such an inquiry should be conducted whenever investments include covered activities, as defined in *§ 850.224—Prohibited transaction* and *§ 850.217—Notifiable transaction*, even if they initially seem not to involve a person of a country of concern. By requiring a reasonable and diligent inquiry each time covered activities are involved, companies are more likely to identify when a transaction may involve a person of concern and/or when these technologies will be used in a manner to threaten US national security.

3d. Clarification of 'government intelligence use' definition

There is potential ambiguity, and thus a potential loophole, regarding the description of AI systems 'designed to be used for any government intelligence or mass surveillance end-use' on page 4 in § 850.217. Currently, it is not clear whether the Department is suggesting that any AI system that is capable of image recognition or text mining could be used for government intelligence and, therefore, is a notifiable transaction. An alternative interpretation of the text would be that there needs to be evidence or an indication that capabilities such as image recognition or text mining would be used for government intelligence. The former interpretation will lead to far more notifications and thus is a stricter rule, while the latter raises the threshold for an investment to be a notifiable transaction. The Department should clarify which interpretation it means to prevent a potential loophole.

4. Beyond Executive Order 14105: A more expansive approach to AI and national security

As mentioned above, the proposed rule is a broadly effective implementation of Executive Order 14105. CAIP would like to highlight that advanced technologies pose additional national security risks beyond the narrow scope of Executive Order 14105. For example, there may be other adversarial state actors or non-state actors who could be using these technologies against the US. By limiting notifiable and prohibited transactions to those that involve three 'countries of concern', this proposed rule inherently limits risk mitigation.

For future iterations of the rule, CAIP suggests that notifiable transactions may be expanded to include those not involving persons of countries of concern. This visibility of investments would be highly valuable to proactively identifying a broader range of national security risks. In such an iteration, the Department may wish to raise the threshold for what is 'covered activity' not involving 'countries of concern' to ease the regulatory burden.

Finally, CAIP also would like to note that the proposed rule's requirements for 'reasonable and diligent inquiry' could forge the foundation of 'Know Your Customer' guidelines around the use of cutting-edge AI systems. Such guidelines would further reinforce the US approach to mitigating national security risks from AI.

Conclusion

Thank you for working to address the potentially uncontrolled investment into potentially dangerous technologies and thank you for the opportunity to comment on your proposed rule. Overall, the Center for AI Policy (CAIP) supports this proposed rule and sees it as a useful and worthwhile step toward reducing the national security risks from advanced AI. We appreciate your efforts to improve national security, and we hope to remain involved throughout this rulemaking process.