SIIA

June 2, 2025

The Honorable Darrell Issa
Chair, House Judiciary Subcommittee on Courts,
Intellectual Property, and the Internet
2138 Rayburn House Building
Washington, DC 20515

Re: "Protecting Our Edge: Trade Secrets and the Global AI Arms Race"

Dear Chair Issa:

Thank you for the opportunity to participate in the hearing on May 7, 2025, and to provide these answers to your questions following the hearing. Below are my answers as President of the Software and Information Industry Association.

1. Would industry support AI being identified as critical infrastructure? Are there resources that would be needed if such a designation were to be made?

Our members acknowledge the need for robust security and resilience measures for AI systems, especially those deployed in high-risk critical infrastructure sectors (like energy, healthcare, or transportation).

We believe some technology used in the AI space should be considered critical infrastructure depending on the specific systems in which AI is used and how those systems map onto critical infrastructure sectors as defined by Presidential Policy Directive 21 (PPD-21). AI systems *used in* critical infrastructure—such as in managing power grids, medical diagnostics, or transportation systems—fall within the scope. These applications warrant robust security and resilience measures. Also, AI infrastructure itself, such as the data centers, specialized computing equipment, and energy supply needed to train and operate large AI models should be considered critical infrastructure.

Treating all AI as falling within "critical infrastructure" would lead to overregulation of AI, ultimately harming the ability of U.S. companies to compete globally. In addition, designating AI as critical infrastructure, even in a targeted way, would trigger a massive undertaking requiring substantial investment in legal, technical, financial, and human resources to ensure the safety, security, and resilience of these increasingly vital systems.

There is a difference, however, between regulating AI as critical infrastructure for the purposes of national security (which must be a nuanced and carefully calibrated decision) and ensuring that AI technology is not acquired by adversarial nations. We recommend that Congress consider expanding the scope of CFIUS to cover a broader range of investment in order to protect against technology transfer to foreign nations of concern. This matters because only those potential transactions involving critical technologies that pose a risk to U.S. national security fall within the CFIUS process.

2. There has been an increasing push for oversight, disclosure, and regulation of AI systems in the United States and Europe. Is there a need to strike a balance between disclosure and encouraging innovation, and if so, how can we strike such a balance? In which areas would disclosure harm innovation, and in which areas would it not harm innovation?

There is a critical need to strike a balance between disclosure and encouraging innovation in AI systems. This is a central tension in the ongoing development of AI policy in the United States and abroad. In general, we believe the touchstone for determining appropriate disclosure, or transparency, must entail a risk-based approach that looks at the uses of AI systems as well as the sectors in which they are deployed and the intended users of the system.

Where the user is the U.S. government, for example, we support the balanced approach set out in OMB M-25-21 and M-25-22, issued earlier this year. (See SIIA's thoughts on these memos.) Consumer-oriented AI systems, such as generative AI tools with multiple potential uses, do not require the same degree of disclosure. For these, we believe the emergence of voluntary best practices in the United States, including model cards, identification of synthetic content, and other features, is providing users with an appropriate level of transparency into features of the AI models or systems they interact with.

Ultimately, disclosure or transparency measures should be designed to generate user trust, which is essential to advance adoption of AI and to support continued innovation. In the context of high-risk AI systems, these measures can help to mitigate harm and prevent a race to the bottom.

With respect to disclosure of training data, which is an issue of current importance in the IP community, we support a general description of the data used to train AI models, which may include summaries of sources and descriptions of datasets. We do not support detailed inventories of all data used for training. The reason is that detailed disclosure is likely to reveal trade secrets and other sensitive information that will have a negative impact on innovation. This would also give an advantage to developers outside the United States, including in countries of concern, and potentially drive developers to jurisdictions with less stringent disclosure requirements.

Beyond training data, we do not support disclosure of core algorithms, proprietary architectures, or training methodologies. Disclosure could reveal information that would put U.S. developers at a competitive disadvantage and chill innovation during early-stage research and development.

In addition to disclosure of general information about training data, we believe the goal of building user trust is furthered when developers disclose risk assessments and mitigation strategies, as well as information about how they engage in testing, evaluation, verification, and validation (TEVV), address adverse incidents, and authenticate content, among other areas.

In conclusion, the goal is not to choose between disclosure and innovation, but to find the sweet spot where transparency and accountability foster responsible innovation, building public trust and ensuring that AI benefits society as a whole. This often means tailoring disclosure requirements to the specific risks and impacts of the AI system in question.

3. Do the risks of trade secret leakage increase as the use of third party litigation funding in IP cases continues to expand, often without transparency requirements? Would you recommend reforms to address potentially inconsistent treatment of undisclosed proprietary information in court?

The risks of trade secret leakage increase as the use of third-party litigation funding (TPLF) in IP cases continues to expand, especially without robust transparency requirements. This can occur primarily in two patent litigation contexts. First, TPLF enables the funders to leverage and hold large numbers of poor-quality patents in a non-practicing entity. Those patents are then used to sue both our members and main-street businesses. In many of these cases, plaintiffs will seek information about how the alleged infringement is occurring, which often involves the introduction of sensitive proprietary information, including trade secrets, into discovery. Second, funders, who are not parties to the lawsuit, have an interest (and likely an obligation) to make sure that they are investing in litigations that are likely to produce value. As part of that monitoring, they will gain access to confidential, proprietary, and sensitive information throughout the litigation. This includes detailed information about case merits, the defendant's business, and potentially the trade secrets at issue. Importantly, the funder typically does not have a fiduciary duty to the plaintiff, meaning their primary motivation is financial return. If they learn information from a lawsuit that helps their investors, they are generally free to use it.

While there are clear business concerns from the potential disclosure or leakage of trade secrets in TPLF cases, these cases also raise significant national security risk. Many TPLF backers in IP cases involving U.S. companies have the backing of foreign governments. Increasingly, these suits are seen as a means to gain access to trade secrets and proprietary information in critical technology sectors through the discovery process.

SIIA has endorsed HR 1109 – *The Litigation Transparency Act of 2025*. This legislation would require disclosure of investors receiving payment based on the outcome of a case and also disclosure of the financing agreement between investors and parties to civil actions. We believe that requiring disclosure of these facts will enable courts to more carefully determine what proprietary and sensitive information should be included in discovery and to craft appropriate protective orders for trade secrets and proprietary information in the course of litigation.

4. Are there solutions to mitigate risk of disclosure of trade secrets in litigation where even the owner may not entirely understand the bounds of the protected technology?

There are solutions to mitigate risk of disclosure even when the bounds of the protected technology are not fully understood. The first and most critical item is limiting disclosure of information unnecessary for the litigation. A district court judge has enormous discretion in deciding what information is subject to discovery and in crafting a protective order, but the judge needs a full set of facts to be able to do so judiciously. In many instances, the parties will vigorously litigate whether to disclose trade secret information at all, and if so under what conditions. A district court judge that knows that a plaintiff is funded by the Chinese Communist Party, for example, might not allow access to trade secret information at all in a patent suit brought by a non-practicing entity. This is the first line of defense against theft of trade secrets—preventing disclosure of information that is irrelevant to the case and sensitive. When district court judges are aware that foreign governments are behind invasive requests for sensitive information, the judge is more likely to limit the disclosure to only the sensitive information that is truly critical to the case. Thus, even when the party with protected or sensitive information is uncertain about the breadth of the sensitivity—such as what qualifies as a trade secret—enabling the judge to limit disclosure to only that information that is strictly necessary to the litigation minimizes the disclosure of other sensitive information.

And for the information that must be disclosed to the foreign-funded party, the judge can more effectively craft protective orders to limit disclosures. The trial judge might, for example, designate sensitive information as “attorney eyes only,” limiting access to only outside counsel or inside counsel (and experts) with a demonstrated need to know and who are uninvolved in competitive decision making. In addition, the court could require physical security, restriction of copying and printing (as well as logging), prohibitions on any use of sensitive materials for competitive activity, and affidavits of non-involvement. In addition to conducting in camera review, the court could also appoint a special master, who not only could assist the judge in evaluating the technology, but could also review proprietary information in a clean room environment. And these examples are not exhaustive of the solutions the district court judge can implement. The key is empowering the judge with information about who is behind the litigation, good-faith litigant or foreign government seeking technology secrets. The more the district court judge knows about the funders, the more it can tailor its orders to both competitive and national security risks.

Beyond limiting disclosure and thoughtfully shaping protective orders, there are a number of additional solutions that help prevent theft of sensitive technology even when the owner is not fully aware of the scope of the sensitive technology. Some of the solutions are educational self help, aimed at increasing the understanding of the owner of the sensitive technology, but others are steps that the court can take. Proposed solutions include the following: (1) owners should hire experts or consultants to evaluate and define the scope of sensitive information and technology, (2) owners should create active internal processes to track and document sensitive information and technology, (3) courts should appoint special masters or technical experts to evaluate the scope of sensitive information, (4) courts should require vetted, independent experts and phased disclosure in expert discovery, (5) courts should allow redactions and summarization of sensitive information and data where appropriate, and (6) courts should perform in camera review to evaluate the sensitivity and necessity of requested information and technology.

Respectfully submitted,

Christopher A. Mohr
President