SIIA

21 December 2022

SIIA input to the AI Act Parliament’s compromise amendments

1. **Which of the four AI definitions do you find best and why? Which elements/words are important and must be included? And what should not be included? FYI: both the EP as well as the Council will very likely delete the whole ANNEX I.**

The definition of AI used in the AI Act will have significant consequences for businesses and consumers in the EU and globally. SIIA recommends that the EP adopt a definition that is both clear and designed to further global alignment on AI regulation. Either the Voss/Clune/Maydell proposal or the NIST definition would achieve these goals.

Both definitions are based on language agreed to within the OECD and as such have been subject to substantial deliberation involving experts from the larger AI community. Both definitions include focus on the unique characteristics of machine-based systems that are designed to generate outputs consistent with defined objectives and operate with varying levels of autonomy. SIIA has concern that the two other definitions could be interpreted broadly to include various analytical or data-based systems that execute defined operations in an automatic manner.

2. **What do you think about the Council‘s Art 6? Is paragraph 3 a good & narrow way to make sure that only really risky AI systems are listed in ANNEX III?**

SIIA supports an approach to high-risk AI systems that distinguishes within each category to focus EU resources on the systems anticipated to create the highest risk. SIIA appreciates the Council’s attempt to provide more nuance to differences among AI systems in the Annex III categories by proposing a carve out, in Article 6(3), for systems with output that is “purely accessory in respect of the relevant action or decision to be taken.” SIIA believes that this recommendation is moving closer to a workable approach for classifying AI systems and determining which systems should be subject to pre-market approval and other requirements in the AI Act.

SIIA recommends, however, that the EP provide further clarity on what may constitute “purely accessory” output. We are concerned that this phrase may prove challenging in the implementation; concrete guidance would improve predictability for consumers, developers, businesses, and government agencies. We recommend providing clarity around this term.

In addition, SIIA recommends revisions to classification of high-risk systems that reflects the state of industry practice with respect to AI systems within each category. For example, many systems used in the educational context already adhere to pre-market assessment practices to ensure accuracy, safety, and reliability. Those systems present lesser risk than systems that are not subject to rigorous pre-market assessment and should be treated different with respect to the need for official EU pre-market certification. Incorporating a revision along these lines would greatly reduce the regulatory burden that the AI Act will have on the EU and will help to foster a greater climate for innovation of responsible AI systems.

SIIA also cautions the co-rapporteurs not to treat any system developed using personal data as prima facie high risk. In addition to creating an extraordinary burden on EU infrastructure, this approach will have a chilling effect on innovation in the EU and greatly limit the availability of services and products to consumers in the EU.

3. **What do you think of the current version of Article 8, which is an umbrella article that applies to all high-risk obligations in Art 9-15? Is it enough to make sure that different contexts/sectors/applications are handled differently?**

SIIA believes that Article 8 as proposed requires additional clarity to avoid confusion in terms of obligations that extend during the lifetime of an AI system. We recommend that Article 8 reflect that AI systems are constantly evolving and improving. In addition, we recommend that the requirement for pre-market certification be refined to treat different contexts, sectors, and applications differently based on a risk assessment and recognition of existing policies and procedures that developers and companies undertake to ensure the reliability and trustworthiness of the AI systems.

4. **What do you think about the current version of Art 2? Is this approach in line with EU law and trade agreements? Can the EU regulate in a way that is described in (c), (ca) and (cba)?**

SIIA recommends taking a more nuanced approach to Article 2 to ensure that the AI Act is not limiting the ability of EU individuals to take advantage of AI innovation developed outside of the EU. There is a risk that certain requirements of the AI Act may lead organizations not to offer certain AI-based products and services within the EU even if the underlying systems adhere to rigorous standards for responsible and trustworthy AI. In particular, the phrase "has effects or affects natural persons" can be subject to a range of interpretations and, without further clarity, will increase the risk to companies that develop, deploy, or make available output from AI systems.

5. **GDPR and DSA follow the „country of origin" principle but the co-rapporteurs want to change it to „place of harm" as it is often the case with consumer protection legislation (Brussels1). What do you think about Article 59a paragraph 2? Is this shift away from „country of origin" (Brussels1a) a problem?**

SIIA recommends that the EP not adopt this proposal because it is likely to lead to compliance challenges and confusion given its departure from the GDPR and DSA framework. We recommend adhering to the approach established in the GDPR rather than adopting an approach that aligns more closely with product liability regulations given the breadth of the AI Act and its focus on advancing innovation and deployment of trustworthy and responsible AI systems.

6. **Is the addition in Art 61 technical feasible for the provider, in particular in IoT ecosystems?**

SIIA does not believe that the proposed addition to Article 61 will be feasible because of the complex interplay of any given AI system with an array of other systems. We believe this will foster confusion with respect to post-market monitoring and likely impede EU innovation and AI investment in the EU.

7. **Is this improved version of Art 64(2) now OK or still too far-reaching? Is access to the source code even useful for the regulator?**

SIIA supports the proposed amendment to Article 64(2) as an improvement on the earlier version because it provides for alternative means to verify conformity and clarifies alignment with current legislation, such as the trade secrets directive. SIIA recommends, however, that the EP consider the value in granting the national supervisory authority with access to source code. We believe assessment of conformity can be undertaken more effectively by a focus on the potential effects of such systems and question whether the national supervisory authorities will have the expertise necessary to assess source code in an effective and timely manner. In addition, we recommend the EP add language to ensure the confidentiality of any and all information shared with national supervisory authorities and prevent the use of such information in other contexts.

8. What do you think about this new enforcement article (Article 66a) that was added in order to better address certain GDPR-like problems on the Digital Single Market?

No position.

9. What do you think about article 67? Is it really a typical NLF norm or is it something new?

SIIA questions the need to include Article 67 as by its language it concerns those AI systems that are otherwise in compliance with the terms of the AI Act. We recommend striking Article 67 in its entirety.

If Article 67 remains, we recommend that the text specify the grounds by which a compliant AI system may be deemed to present an unreasonable and serious risk. While we appreciate the proposed revisions to Article 67 to identify the relevant authorities responsible for making this determination, we have concern that without further guidance Article 67 will create significant risk for companies developing and deploying AI systems that will impede innovation in the EU and lead non-EU companies to limit AI-based services – especially those with uses that benefit society at large or respond to consumer demands– provided to EU organizations and individuals.