U.S. Non-Paper regarding the September 2022 Revisions to the Draft EU Artificial Intelligence Act Proposed by the Czech Presidency

The United States and European Union both seek a rights-respecting, innovation-friendly, risk-based approach that maximizes the benefits of artificial intelligence (AI). We support the legitimate objectives of protecting consumers and their rights under EU law while ensuring quality, safety, security, and alignment of AI regulation with international human rights.

We commend the EU for developing a thoughtful architecture that addresses many of our shared AI objectives. Many of our comments are prompted by our growing cooperation in this area under the U.S.-EU Trade and Technology Council (TTC) and concerns over whether the proposed Act will support or restrict continued cooperation. We hope our comments serve as a basis for further constructive dialogue.

We note that these comments are not meant to be comprehensive and are without prejudice to other comments or concerns the U. S. Government may raise in response to the Act.

Intergovernmental Cooperation

- We recommend revising Article 2(4), which, as currently drafted, will impede cooperation with third country governments. The U.S. government has devised and continues to devise its own AI standards; these standards are robust but will not be identical to those under the AI Act. While the fact that Art. 2(4) has been included recognizes that cooperation with third States should continue even where there is such divergence, it is drafted too narrowly. First, 2(4) only applies to law enforcement. Since the Act categorizes law enforcement as separate from border management and other important regulatory uses of AI systems, the exception in 2(4) will be read not to apply to these other governmental functions, and third country partners using AI systems/outputs in cooperating with their EU member states' counterparts will either have to comply with the Act (including requirements to share sensitive information with EU regulators) or the cooperation will not be permitted. Particularly in areas considered to be "high risk" under the Act, many U.S. government agencies will likely stop sharing rather than risk that closely held methods will be disclosed more broadly than they have comfort with.

- Second, we believe reference to "agreements" in Art. 2(4) alone is too narrow, in that existing binding agreements are not well adapted to AI cooperation, and it would take years to conclude sufficient new ones; in the meantime, under the current drafting, even law enforcement cooperation would suffer. Furthermore, significant law enforcement collaboration takes place outside of formal, binding "agreements." Accordingly, we urge you to expand 2(4) to exclude from the scope of the Act a broader category of critical intergovernmental cooperative activities with third State democracies, and to broaden the "agreement" requirement.

- Also important, especially to the extent the proposed changes to Art. 2(4) are not attained:

a) In Art 5(1)(d)(ii), replace "specific and" with "credible and," so as to avoid adversely affecting cooperation with member states' authorities to ensure safety at major public events.[1]

b) In Art. 5(4) provide for an EU-wide rule, in order to avoid fragmentation and the consequent hampering of cooperation between some EU member states and third countries.

c) 6(3) states: "AI systems referred to in Annex III shall be considered high-risk if the output of the system is not purely accessory…", In contrast, Annex III states: "[i]n each of the areas listed under points 1-8, the AI systems specifically mentioned under each letter are considered to be high-risk AI systems pursuant to Article 6." This sentence should be modified to insert "*unless excluded* pursuant to Article 6," in order to make clearer that a system is not "high-risk" unless Article 6 considers the system to be high risk. Similarly, Art. 7(1) provides for amendment to Annex III if criteria set forth in 7(1)(a) and (b) are met and it should be clearer that these conditions apply to the AI systems in Annex III *ab initio*.

d) Art. 7(2) factors that may be considered will create challenges for implementation, e.g., the purpose factor in Art. 7(2)(a) will not necessarily reflect that an AI system's purpose may be very different from the AI system's results. We would propose that, with respect to intergovernmental cooperation with other democratic States, the alternative approach of individualized risk-assessment (such as the NIST standards under consideration in the United States, which might consider threat sources and events, vulnerabilities, the likelihood of occurrence of intended or unintended yet foreseeable impacts, and the magnitude of such impacts) also be considered compliant. We urge you to avoid mismatch between the very targeted criteria for the identification of high-risk AI applications as described in article 7(2) and annexes II and III. We welcome the addition of Art.7(2).i which takes into account the potential benefits of the AI system under consideration.

<u>Regulatory and legal clarity</u>

- The lack of definition of the terms "output" and "Used in the Union" allows for a broad definition that is applicable extraterritorially. We also recommend clarifying the relationships between the Act and other existing and proposed EU legislation, such as the General Data Protection Regulation (GDPR), the EU Medical Device Regulation, and others.

- We acknowledge that the Council text includes proposed revisions to improve the AI Board and strengthen its role vis-a- vis Member State oversight bodies. It also sets up a standing sub-group of stakeholders. Given that the Board is prescribed to have wide ranging duties, including issuing opinions on technical specifications, the use of harmonized standards, and the preparation of guidance documents (Article 58), we'd suggest that there be wording to specify the allowance for participation of like-minded international partners at least in the sub group, who can provide

[1] As a grammatical point, currently in Art. 5(1)(d)(ii), "critical infrastructure" modifies "of natural persons," meaning biometric ID systems could only be used it if strictly necessary for the prevention of a specific and substantial threat to the critical infrastructure of natural persons. It may better read: "the prevention of a substantial threat to critical infrastructure *or to the* life, health, or physical safety of natural persons".

valuable and relevant feedback and insight into key AI decisions, particularly when it comes to avoiding the creation of trade barriers.

- The United States Government would welcome the opportunity to provide input in meaningful way on the Artificial Intelligence Board. Collaboration in this space is particularly important to preventing barriers to transatlantic commerce, which is also in line with the goals of the U.S.-EU Trade and Technology Council.

Definition of "Artificial Intelligence"

- In the rapidly developing world of artificial intelligence, a cohesive, globally applicable definition of the term AI is critical to ensure that innovation, regulation, and development can be applied to the same technology. We welcome the characteristics in Recital 6 defining "artificial intelligence," but believe the text of Recital 6 might more appropriately be included in Article 3.

- The definition of "artificial intelligence system" still includes systems that are not sophisticated enough to merit special attention under AI-focused legislation, such as hand-crafted rules-based systems. To avoid over-inclusiveness, we recommend narrowing the scope further to systems to which the term "artificial intelligence" is widely applied. For example, the existing U.S. regulations on federal use of AI use a definition that captures the spirit of the OECD definition but in more specific terms: a "system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets; . . . [a] system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action; . . . [a] system designed to think or act like a human, including cognitive architectures and neural networks; a set of techniques, including machine learning, that is designed to approximate a cognitive task; or [a] system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting." We recommend using a definition that provides similar clarity on what is and is not included.

Definition of "high-risk"

- Reviewing the changes to Chapter 1 of the Council text regarding the definition of "high-risk", the United States continues to advocate for a more individualized risk-based assessment. During this risk-based assessment, each AI system would be evaluated for (1) threat sources and events; (2) vulnerabilities; (3) the likelihood of impacts' occurrence; and (4) the magnitude of impacts. Moreover, human rights impact assessments could be used to determine risk in particular contexts. The addition of an appeals process for companies that feel they were wrongly included in high-risk categories would be of use as well.

- We appreciate the improved language of Article 6, clarifying what constitutes High-Risk AI. We also welcome the changes the Czech Presidency's third compromise text has introduced in recital 32 to further clarify '*not purely accessory'* in article 6(3). We are however concerned that products that would be classified as High Risk as defined by the EU's AI Act may also be subject

to regulation under current sector-specific regulatory regimes such as the Medical Device Regulation. How can we ensure that potential conflicts and inconsistences are avoided?

General purpose AI

- We recommend distinguishing the responsibilities and related liability under the Act applicable to the original manufacturer of a general purpose AI from the responsibilities and related liability of the users of such general purpose AI who subsequently use it to develop, train and deploy High-Risk AI.

- The first part of the third compromise text by the Czech Presidency did not amend articles 4(a) and 4(b) on general purpose AI which would place on any provider of general purpose AI that may be used in High-Risk AI the obligation to comply with certain AI Act requirements for High-Risk AI without a risk-based justification that considers the specific provider's level of control over that use.

- When modifying these articles in the second part of the third compromise text, we strongly urge you re-consider the allocation of responsibilities under articles 4(a) and 4(b). Requiring all general purpose AI providers to comply with the risk-management obligations of the AI Act would be very burdensome, technically difficult and in some cases impossible. General purpose AI suppliers may have limited visibility on the subsequent use of their general purpose AI system, the context in which the system is deployed and other information necessary to ensure compliance with the iterative risk management obligations required for High-Risk AI systems under the EU AI Act.

- To the extent that Art.4b.5 and 4c require providers of general purpose AI systems to disclose to other providers or permit their use of "intellectual property rights, and confidential business information or trade secrets," we recommend that Art.4b.5 and 4c be removed from the Act. If that is not the intent of the current language, we recommend that it be clarified. We also recommend that any disclosure or permission for use be compensated and compliant with international obligations.

Disclosure of source code (Article 63.9)

- We recommend that the Act define "necessary" and specify which entity makes that determination. This will help avoid subjective and inconsistent decisions. We also suggest the inclusion of an objection or appeal process.

- Regarding whether the "cumulative conditions" of a) and b) have been met, we suggest that consistent and transparent criteria be determined and applied.

- We recommend that the Act include a provision to include the source code owner in the deliberations on whether the "cumulative conditions" have been met. This would allow productive discussions on how the regulator might assess conformity through means not involving access to the source code.

- We consider it critical that the requirements are uniform across the EU, rather than each Member State having its own regime.

Confidentiality (Article 70.1)

- When "intellectual property rights, and confidential business information or trade secrets of a natural or legal person, including source code" is in the hands of the parties listed in Art.70.1, we recommend the Act require the application of strong, consistent, and transparent protection schemes. We also recommend the addition of provisions on the return or destruction of the disclosed materials when no longer needed for legitimate purposes. If return or destruction is not practicable, then we recommend including a provision that confidentiality obligations do not expire.

Transparency obligations for certain AI systems [deep fakes] (Article 52.3)

- We recommend that this provision should be clarified to ensure that it does not limit freedom of expression or the right to freedom of the arts and sciences under the EU Charter of Fundamental Rights. For example, it should be clear that it is not necessary to include captions identifying deep fakes in the body of a movie; a disclosure in the credits should be adequate.

Standards

- We have an opportunity to prevent the creation of future standards barriers in a critical technology. Some concrete suggestions to help achieve this goal include:

    - The revisions of Article 40 in the Council text are generally welcome but highlight that a goal of standardization requests would be to "strengthen the Union's digital sovereignty." Art.40(2)(a). We suggest either deleting or more clearly defining the term "digital sovereignty" to ensure that standards are not developed in a manner that unnecessarily excludes non-European products or services.

    - Additionally, Art. 40(2)(c) urges multi-stakeholder governance in the development of AI standards by "relevant European stakeholders." Bilateral cooperation between the U.S. and EU on the development of AI standards necessarily depends on the inclusion of European stakeholders in U.S.-based standard developing organizations (SDOs), and the inclusion of U.S. stakeholders or SDOs in the development of European standards. We would therefore like to see the AI Act encourage the involvement of non-EU standardization bodies who might have state of the art AI standards expertise.

    - Given the emerging and highly technical nature of standards development in the AI field, we would urge you to consider permitting joint development of standards or making explicit the ability of EU SDOs to reference existing standards, including standards developed by U.S. based SDOs, in whole or in part, to ensure that EU standards are the best possible "fit for purpose" and to maximize the opportunity for regulatory alignment.

    - Similarly, when the Commission undertakes to draft Common Specifications under Article 41, we would like the Commission to have the flexibility to work with international stakeholders, and for the Act to reference non-European standards, in whole or in part, in order to ensure the best possible standards, and to maximize regulatory alignment.

Conformity Assessment

- Conformity assessment procedures should avoid disproportionate and / or negative impacts on transatlantic trade, especially for small- and medium-sized businesses.

- As international standards, test methods and scope requirements for accreditation are still under development in the field of AI, we would like to ensure there is enough time available for the organizations that will conduct and enforce the conformity assessment procedures to be accredited and available to manufacturers to conduct the required conformity assessment procedures, where applicable.

- If the Act goes into force without enough time for notified bodies to certify products for high-risk applications where third-party certification is required in Annex II or III, goods and services will be hindered or delayed from entering the EU marketplace.