Council of the European Union

Brussels, 29 November 2022
(OR. en)

13928/1/22
REV 1

LIMITE

TTC 22
USA 33
POLCOM 182
TELECOM 478
COMPET 925
MI 847
COMER 142
CYBER 378
HYBRID 107
DISINFO 91
COTRA 37

NOTE

From:	European Commission
To:	Delegations
Subject:	Revised draft EU-U.S. Joint Statement of the Trade and Technology Council (5 December 2022, Washington, D.C.)

In accordance with the agreed inter-institutional procedure for non-binding instruments, Member States will find enclosed for the Council's endorsement the revised EU-US Joint Statement, accompanied with Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management (AI Roadmap), and the Joint Statement on protecting human rights defenders online that is intended to be issued at the EU-US Trade and Technology Council meeting on 5 December 2022 for the Council's endorsement. The circulated document reflects the latest state of play of exchanges with the US, with the text in brackets still subject to further discussion.

**U.S.-EU Joint Statement
of the Trade and Technology Council
December 5, 2022
[Washington, D.C.]**
Draft as of November 29, 2022

I. Introduction

The U.S.-EU Trade and Technology Council (TTC) met outside Washington, D.C., on December 5, 2022. The meeting was co-chaired by U.S. Secretary of State Antony Blinken, U.S. Secretary of Commerce Gina Raimondo, U.S. Trade Representative Katherine Tai, European Commission Executive Vice President Margrethe Vestager, and European Commission Executive Vice President Valdis Dombrovskis, joined by European Commissioner Thierry Breton, as well as U.S. Deputy Under Secretary of Labor Thea Lee, Jamaica Minister for Information Communication Technology Floyd Green, and Kenya Cabinet Secretary for Information, Communication and the Digital Economy Eliud Owalo.

The TTC is a key mechanism to support stronger transatlantic relations and to deliver concrete outcomes. We reaffirm that international rules-based approaches to trade, technology, and innovation that are founded on solid democratic principles and values can improve the lives of our citizens and generate greater prosperity for people around the world. Through the TTC's ten working groups, we are supporting sustainable, inclusive economic growth and development, promoting a human-centric approach to the digital transformation, and ensuring that international norms and the international trade rulebook are respected and reflect our shared values. We will continue to work together to modernize and reform the World Trade Organization (WTO) as set out in the WTO MC12 Outcome Document.

Geostrategic challenges, including Russia's full-scale invasion of Ukraine and increased assertiveness of autocratic regimes, have reinforced the importance of our shared democratic values, commitment to universal human rights, and leadership role in upholding an international rules-based order. The United States and the European Union reiterate our strong condemnation of Russia's illegal and unjustifiable war of aggression against Ukraine and reaffirm our unwavering commitment to stand firmly with Ukraine for as long as it takes to ensure Ukraine's sovereignty, independence, and territorial integrity. We condemn attacks by Russia on Ukraine's infrastructure and will continue supporting Ukraine in securing, maintaining, and rebuilding this infrastructure, including its telecommunications and internet infrastructure. We resolve to continue to impose severe and immediate costs on Russia and hold it accountable for its brutal war against Ukraine, including through unprecedented cooperation on sanctions related export restrictions, and countering Russian disinformation. We will also hold Belarus to account for its complicity in Russia's war. The TTC Working Groups on Export Controls and on Misuse of Technology have made critical contributions to this successful and ongoing collaboration. [The TTC Working Groups on Data Governance and Technology Platforms and on Misuse of Technology Threatening Security and Human Rights are coordinating to understand and address the spread of Russian information manipulation and interference in third countries, notably Africa and Latin-America.]

The impact on our supply chains of Russia's full-scale invasion of Ukraine has further underscored that we share an urgent need to identify and address supply chain vulnerabilities. The United States and the European Union recognize that the concentration of resources in key supply chains can expose our economies to challenging disruptions. We plan to explore coordinated actions to foster diversification and make key supply chains more resilient.

To support our shared desire of tackling climate change, the United States and the European Union intend to launch a new Transatlantic Initiative for Sustainable Trade to advance our shared objective of achieving a green and sustainable future. [Placeholder for preliminary results of task force and commitment to address EU concerns. We have also established a dedicated U.S.-EU Task Force on the Inflation Reduction Act. These initiatives will aim to ensure a coordinated approach to achieve a green transition underpinned by resilient transatlantic supply chains that benefit both sides.]

The United States and the European Union are establishing a Talent for Growth Task Force that will pursue our collective objective to recognize and develop the talent of our working-age populations.

II. Key Outcomes of the Third TTC Ministerial

A. Digital Infrastructure and Connectivity

Joint Initiatives with Jamaica and Kenya

The United States and the European Union are supporting secure and resilient digital connectivity and information and communication technology and services (ICTS) supply chains in third countries, provided by trusted suppliers. As a first step, we intend to support inclusive ICTS projects in Jamaica and Kenya based on our common overarching principles. This work reflects our commitments under our Global Gateway and Partnership for Global Infrastructure and Investment initiatives.

- **Cooperation on connectivity with Jamaica:** In cooperation with the government of Jamaica and other Jamaican stakeholders, we will connect over 1,000 public schools and children's homes around Jamaica to robust, inclusive, and secure internet service, strengthen the digital competencies of teachers, and support the use of digital technologies by micro-, small-, and medium-sized enterprises. Our efforts will also assist Jamaica's electric utility, Jamaica Public Service, to expand reliable and trustworthy public Wi-Fi infrastructure in the New Kingston neighborhood of Jamaica's capital, with the potential to expand the service across the country. We also intend to support secure and resilient rural broadband connectivity provided by trusted vendors in the country.

- **Cooperation on connectivity with Kenya:** In cooperation with the government of Kenya, we will support the implementation of Kenya's 2022-2032 National Digital Masterplan by expanding school connectivity in Kenya and bridging gaps in last-mile connectivity. First efforts will include a study on scalable solutions to expand school connectivity in Kenya, building fiber optic connections to schools in remote areas, a policy roadmap for affordable, secure, trustworthy and meaningful connectivity, and training options to develop the next generation of digital professionals. We also will provide technical assistance to help Kenya

update its Information and Communications Act and 5G Strategy in line with the principles set for high-quality global infrastructure projects at the TTC meeting in Paris-Saclay, France on May 16, 2022.

The United States and the European Union intend to expand our coordination on financing digital infrastructure projects in third countries, including through a Memorandum of Understanding between the U.S. Development Finance Corporation (DFC) and the European Investment Bank (EIB), which aims to enable increased collaboration on financing for secure connectivity in third countries.

Future Secure Connectivity Projects

The United States and the European Union recognize the importance of cooperating on trust and security in the ICT ecosystem. We welcome projects that strengthen the resilience of that ecosystem, including subsea cables. The TTC Working Group on ICTS security and competitiveness intends to discuss transatlantic subsea cables' connectivity and security, including alternative routes, such as the transatlantic route to connect Europe, North America and Asia. We also welcome supplier diversification efforts in ICTS supply chains and continue to discuss market trends towards open, interoperable approaches, alongside trusted, established architectures, in a technology neutral way.

B. Cooperation on New and Emerging Technologies

Artificial Intelligence (AI) Roadmap and Pilot Project on Privacy-Enhancing Technologies [and AI Research Collaboration]

To fulfill our commitment on developing and implementing trustworthy AI, the United States and the European Union have issued a first Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management (AI Roadmap) and collected perspectives from relevant stakeholders (*hyperlink to the Roadmap*). This roadmap will inform our approaches to AI risk management and trustworthy AI on both sides of the Atlantic, and advance collaborative approaches in international standards bodies related to AI. In conjunction with this effort, we aim to build a shared repository of metrics for measuring AI trustworthiness and risk management methods, which would support ongoing work in other settings such as the OECD and GPAI. Our cooperation will enable trustworthy AI systems that enhance innovation, lower barriers to trade, bolster market competition, operationalize common values, and protect the universal human rights and dignity of our citizens.

Recognizing the importance of privacy in advancing responsible AI development, the United States and the European Union have identified [privacy-enhancing technologies as a subject of interest and will pursue a feasibility project for privacy enhancing technologies and synthetic data in an area of joint interest such as healthcare, in line with applicable data protection rules].

A joint study [add hyperlink] on the impact of AI on the workforce was finalised, with US and EU case studies on hiring and logistics.

[Tech for the Public Good]

The United States and European Commission intend to bring together experts to explore collaboration on advanced digital research projects, [including by pooling digital resources such as artificial intelligence models and computing power] that can benefit other partner countries and the global scientific community. This cooperation will aim at jointly addressing challenges in key focus areas such as extreme weather and climate forecasting; health and medicine; electric grid optimization; agriculture optimization; and emergency response management. [Today, [x] signed an administrative arrangement to implement this collaboration.]

Collaboration on Quantum

The United States and the European Union plan to establish an expert task force to reduce barriers to research and development collaboration on quantum information science and technology, develop common frameworks for assessing technology readiness, discuss intellectual property, and export control-related issues as appropriate, and work together to advance international standards. This approach could serve as a basis for more enhanced cooperation in other emerging technology areas.

Electric Vehicle Charging

On 16 May 2022, at the TTC meeting in Paris-Saclay, the United States and the European Union decided to cooperate on **Megawatt Charging Systems (MCS) standard for heavy-duty vehicles.** We welcome the progress on the physical prototype developed by industry. We intend to continue working towards a common international standard to be adopted by 2024 at the latest to provide the highest level of interoperability, safety and security.

In parallel, we intend to develop in 2023 joint recommendations for government-funded implementation of **electro-mobility charging infrastructure** that aims to advance electric vehicle adoption in the United States and the European Union, as well as recommendations for future public demonstrations of **Vehicle to Grid Integration pilots**. As intermediate steps, the United States and the European Union organized a stakeholder conference, are publishing the results of the ongoing research work, and have prepared public information on vehicle-to-grid integration and smart charging interoperability [*hyperlink to digestible*].

Other Standards and Research Cooperation

We have launched workstreams to increase standards cooperation on **Additive Manufacturing, Recycling of Plastics, and Digital Identity**, with plans to launch new workstreams on **Post-**

Quantum Encryption [**and Internet of Things (IoT)**, including cybersecurity standards to be discussed by the EU-US Cyber Dialogue].

Following the signing of the Administrative Arrangement in May 2022, we rolled out the **Strategic Standards Information (SSI)** mechanism, which will enable the United States and European Union to voluntarily share information about international standardization activities and promptly react to common strategic issues. Thanks to this cooperation, the United States and the EU, in coordination with like-minded partners, supported successful campaigns for [the elections to the International Telecommunications Union (ITU) leadership] [positions in international standards bodies]. Looking to the next TTC ministerial, and in coordination with key stakeholders, the U.S. and EU intend to develop a common vision on research and development beyond 5G and 6G.

C. Building Resilient Semiconductor Supply Chains

Since the TTC ministerial meeting in Paris-Saclay, the United States passed the CHIPS and Science Act into law, and the European Chips Act has made steady progress in the co-legislative process. The United States and the European Union recognize the importance of cooperating on promoting resilient supply chains.

To achieve this, [x] signed today an administrative arrangement to implement an early warning mechanism to address and mitigate semiconductor supply chain disruptions in a cooperative way. The mechanism draws on the results of last summer's pilot in which the United States and the European Union explored and tested approaches to the exchange of information and cooperation in case of disruptive events.

Transparency is a key tool to avoid concerns over public support programs. Today, [x] signed an administrative arrangement memorializing a common mechanism for reciprocal sharing of information about public support provided to the semiconductor sector to support transparency. We intend to work with other likeminded countries to make similar commitments to transparency.

For our respective public support programs, we will also seek to exchange information and methodologies, share best practices, and develop a common understanding of market dynamics. This includes:

1. Working with industry to promote initiatives aimed at advancing the transparency of demand for semiconductors;

2. Improving our understanding of forecasted global semiconductor demand to inform our common policy objective of avoiding over capacity and bottlenecks. For this purpose, we expect to meet regularly and share information on demand forecast methodologies;

3. Exchanging information and best practices regarding investment approaches and terms and conditions for public support;

4. Exchanging areas of interest and exploring cooperative initiatives in research in semiconductors.

Building on this baseline of transparency, cooperation on potential disruptions, and a common understanding of global demand, we will work to avoid subsidy races and market distortions, and ensure a more resilient, sustainable and innovative semiconductors value chain.

D. Promoting Our Values Online

Declaration for the Future of the Internet

The principles of the Declaration for the Future of the Internet (DFI) – protection of universal human rights and fundamental freedoms, a global internet, and inclusive and affordable access to the Internet– are global in scope and enjoy support from the United States and the European Union. The United States and the European Union again demonstrated their commitment to these principles on 2 November 2022, in Prague, where they engaged with the multi-stakeholder community, welcomed new countries that endorsed the Declaration, and reaffirmed their commitment to its vision and principles.

Protecting Human Rights Defenders Online

The United States and the European Union are deepening cooperation and mutual learning between U.S.- and EU-funded emergency mechanisms, in order to expand resources in support of human rights defenders worldwide. We promote an open, free, global, interoperable, reliable, and secure Internet, in line with universal human rights, and seek to eliminate the use of arbitrary and unlawful surveillance to target human rights defenders. To underline our shared commitments, the European Union and the United States have released a joint statement on protecting human rights defenders online (*add hyperlink to U.S.-EU TTC Joint Statement on Protecting HRDs Online*).

Addressing Internet Shutdowns

The United States and the European Union reiterate our alarm at the increasingly entrenched practice of government-imposed Internet shutdowns. To address this issue, we have facilitated the creation of a multi-stakeholder group of technical experts who will document Internet shutdowns and their effects on society as rapidly and comprehensively as possible. The group released its first report [add hyperlink] on recent Internet shutdowns. We look forward to drawing on the findings of this report and future ones in our diplomatic work.

E. Enhancing Transatlantic Trade

Increasing the Use of Digital Tools

Digital technology can make it easier for companies, particularly small- and medium-sized enterprises, to engage in trade. Prior to the next TTC co-chairs meeting, the United States and the European Union therefore plan to compile and exchange information on respective initiatives to use digital technology to simplify or reduce the cost of commercial actors' interactions with our governments in relation to trade-related policy, legal requirements, or regulatory requirements. The United States and the European Union intend to then build on this information exchange to develop joint best practices for the use of digital tools and to discuss how best to promote compatibility of such digital tools.

Mutual Recognition Agreements and Conformity Assessment-Related Initiatives

The United States and the European Union recognize the importance of mutual recognition agreements and conformity assessment-related initiatives for U.S. and EU stakeholders engaged in transatlantic trade in a range of sectors. Before the next TTC co-chairs meeting, the United States and the European Union plan to explore ways in which the increased use of digital technology, where permissible, may help U.S. and EU stakeholders better utilize existing mutual recognition agreements to facilitate increased transatlantic trade.

The United States and the European Union will also explore the feasibility of extending the scope of the existing U.S.-EU Marine Equipment Mutual Recognition Agreement to include certain radio equipment.

The United States and the European Union also support regulators' work on considering the necessary steps to extend the scope of the EU-U.S. Mutual Recognition Agreement annex for Pharmaceutical Good Manufacturing Practices to include vaccines and plasma-derived pharmaceuticals for human use, as discussed by the Joint Sectoral Committee.

The United States and the European Union will [take steps to facilitate conformity assessment in sectors such as machinery and] continue to work on identifying other potential sectors in which strengthened cooperation on conformity assessment could enhance transatlantic trade.

F. Trade, Security and Economic Prosperity

Cooperation on Export Controls

Regarding cooperation on export control, we are looking at how to simplify transatlantic trade with regard to exports and re-exports of dual-use items and technologies while ensuring appropriate protection against misuse through pilot exchange of information on the disposition of U.S. exports to Europe and vice versa. We are facilitating trade between the United States and the European Union by more coordinated adoption and publication of multilateral control list revisions. We continue to consult on new regulatory actions. We are also planning to conduct coordinated export control outreach with partners. We are taking additional steps to enhance enforcement collaboration between the United States and the European Union, including through the exchange of best practices as appropriate and with a view to promoting the consistent application of sanction related export restrictions targeting Russia and Belarus through regular information exchange, including regarding authorization and denial decisions. Lastly, the United States and the European Union will cooperate on the export controls of sensitive and emerging technologies, while ensuring appropriate protection against misuse with a view to facilitate legitimate transatlantic trade and research interests.

Investment Screening

We have deepened our cooperation on investment screening through technical exchanges, including an in-person tabletop exercise in Brussels. We also continue to discuss security risks related to specific sensitive technologies, including those related to critical infrastructure, and to holistically assess the policy tools available to address these risks. The United States and the European Union underscore the importance of comprehensive, robust foreign investment screening mechanisms on both sides of the Atlantic in order to address risks to national security and, within the European Union, for public order, while remaining open for investment. The United States and the European Union will continue to support the development and implementation of these mechanisms. The working group will be hosting a public stakeholder outreach event on the work of the Investment Screening Working Group in mid-December.

Addressing Non-Market Economic Policies and Practices [and Economic Coercion]

The United States and the European Union have shared concerns about the threat posed by a range of non-market policies and practices, such as those used in the medical devices sector and those involving government-owned or government-controlled investment funds. Following input received from stakeholders, the United States and the European Union have started exchanging information on the market situation of U.S. and EU medical devices companies in China, in order to better understand the impact of non-market policies and practices on U.S. and EU companies. The United States and the European Union are also deepening their exchanges to identify shared concerns relating to increasing use of the aforementioned investment funds. The two sides plan to work together on exploring which policy tools could address non-market policies and practices, including those affecting our medical devices companies. To that end, we will continue building a shared

understanding of the impact of economic and industrial government directives and other non-market policies and practices on our workers and companies.

Addressing Economic Coercion

The United States and the European Union are increasingly concerned with the use of economic coercion that [is inconsistent with the international legal order and] that seeks to undermine our legitimate choices and those of our partners at all levels of development, as well as global security and stability. We resolve to identify and address economic coercion and explore potential coordinated or joint efforts, bilaterally and with other likeminded partners, to improve our assessment, preparedness, resilience, deterrence, and responses to economic coercion. [To that end, we will continue building a shared understanding of the PRC's economic and industrial directives and other non-market policies and practices, and develop coordinated action to foster supply chain diversification, build resilience to economic coercion, and reduce dependences.]

G. Trade-Related Environment and Labor Initiatives

Transatlantic Initiative on Sustainable Trade

The United States and the European Union have already taken, and will continue to take, important policy steps to reduce carbon emissions and promote the accelerated deployment and uptake of environmental technologies. Today we launch a transatlantic initiative on sustainable trade.

This initiative will enhance work across the TTC that strives to support the transition to low-carbon economies by identifying actions in key areas of trade and environmental sustainability that support our shared twin goals of a green and sustainable future and to increase transatlantic trade and investment. We intend to explore areas of cooperation to support these twin goals, including where there is opportunity to measurably decarbonize our energy intensive industries, and facilitate the deployment of goods and services essential to the transition to more circular, and net-zero, economies.

Trade and Labor Dialogue

The first principal level session of Trade and Labor Dialogue (TALD) offered an opportunity to exchange views with senior representatives from labor, business, and government on both sides of the Atlantic. During today's meeting, we built on the technical meeting of September 20 and discussed the critical importance of eradicating forced labor in global trade and supply chains. We explored how we can translate shared transatlantic values concerning combatting forced labor into concrete actions that promote internationally recognized labor rights, and promote resilient and sustainable trade and supply chains.

Health Data for Research

[The EU and the US share a common interest in working together in the appropriate existing fora with a view to facilitating the exchange of health information, in line with applicable data protection rules, to support research, innovation and advancements in public health.]

H. Developing Talent for the Digital Transition and Economic Growth

The United States and the European Union are launching a Talent for Growth Task Force that will bring together government and private sector leaders from business, labor, and organizations that provide training, building on existing initiatives on both sides of the Atlantic. The goal of the task force is to exchange best practices, and to serve as a catalyst for innovative skills policies.

We have a collective objective to develop systems of training for our working-age populations and means of recognizing the talent of all our people. The Talent for Growth Task Force will advise the TTC on the actions needed to achieve this. It will work with and encourage our respective communities to learn from each other, promote common taxonomies and tools, and inspire innovation on training programs; engage the public on the rewarding careers in technology sectors, including a focus on underrepresented communities; exchange on training programs that meet the changing demands of the market; build a skilled workforce that fosters growth and uninterrupted supply chains; facilitate small- and medium-sized businesses access to relevant skilled professionals to foster competition; and help generate middle-income jobs to create a more resilient and equitable middle class.

III. Conclusion

These outcomes represent tangible progress across all workstreams established under the TTC. We are committed to advancing these projects and developing new ones as we deepen and grow the transatlantic economic relationship, based on our shared values and principles. The co-chairs intend to meet again in mid-2023 in Europe to review our joint work and discuss new ways to expand our partnership.

TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management

Draft for EU-US Discussion - Revised as of 25 Nov 22

1. Background

The global leadership of the United States and the European Union can provide scalable, research-based methods to advance trustworthy approaches to AI that serve all people in responsible, equitable, and beneficial ways. Effective risk management and assessment can help earn and increase trust in the development, deployment, and use of AI systems. Recognizing the power of AI to address the world's challenges, we also acknowledge AI systems entail risk. By minimizing the negative impacts of AI systems on individuals, culture, economy, societies, and the planet, we can maximize the positive impacts and benefits of AI systems that support the shared values underpinning like-minded democracies. Towards that goal, the U.S.-EU Joint Statement of the Trade and Technology Council (May 2022) expressed an intention to develop a joint roadmap ("Joint Roadmap") on evaluation and measurement tools for trustworthy AI and risk management.

This Joint Roadmap aims to guide the development of tools, methodologies, and approaches to AI risk management and trustworthy AI by the EU and the United States and to advance our shared interest in both supporting international standardization efforts and promoting trustworthy AI on the basis of a shared dedication to democratic values and human rights. It takes practical steps to advance trustworthy AI and uphold our shared commitment to the Organisation for Economic Co-operation and Development ("OECD") Recommendation on AI.

2. Risk-Based Approaches: Bringing EU and U.S. approaches closer

The United States and EU acknowledge that a risk-based approach and a focus on trustworthy AI systems can provide people with confidence in AI-based solutions, while inspiring enterprises to develop them. This approach supports common values, protects the rights and dignity of people, and sustains the planet, and encourages market innovation. Both parties share this commitment to trustworthy AI supported by a shared respect for democratic values and human rights. Both parties are pursuing risk-based approaches that operationalize these values.

Both sides apply risk-based and socio-technical perspectives to advance trustworthy AI. Examples of the EU's risk-based approach to AI are represented in the proposed EU AI Act and the work of the High-Level Expert Group (HLEG) on AI. Examples of the U.S. approach can be seen in the National Institute of Standards and Technology (NIST) draft AI Risk Management Framework as well as the White House Office of Science and Technology Policy (OSTP) Blueprint for an AI Bill of Rights. While the EU and United States may have different views on regulatory approaches,

including allocation of the responsibility for risk assessment, possible legal responsibility for the establishment of a risk management system, and the balance between regulatory and voluntary measures, the EU and US risk-based approaches recognize that shared values can guide the advancement of emerging technologies.

This Joint Roadmap underscores the importance of the U.S. and EU approaches being supported by science, international standards, shared terminology, and validated metrics and methodologies, and it suggests activities which are intended to be compatible with the respective regulatory, policy, and legislative initiatives of the two parties. Stakeholder engagement and the active engagement and participation of the whole AI community (including industry, academia, and civil society) is key to fulfilling the objectives of this roadmap. In this respect, all planned activities are intended to be conducted with engagement and support by stakeholder and expert consultation plans, including expert workshops.

Suggestions for concrete activities aimed at aligning EU and U.S. risk-based approaches are advancing: 1) Shared Terminologies and Taxonomies; 2) Leadership and Cooperation in International Technical Standards and Tools for Trustworthy AI and Risk Management; and 3) Monitoring and Measuring Existing and Emerging AI Risks.

3.   Roadmap activities

3.1 Advance Shared Terminologies and Taxonomies

Shared terminologies and taxonomies are an essential step for operationalizing trustworthy AI and risk management in an interoperable fashion. The activities in this section support the United States' and EU's work on interoperable definitions of key terms such as trustworthy, risk, harm, and risk threshold, and socio-technical characteristics such as bias, robustness, safety, interpretability, and security. The objective is to develop a shared understanding of basic terms in order to use an interoperable taxonomy when developing standards and identifying responsibilities, practices, and policies.

This work will focus on leveraging the global work already done and ongoing (such as within the International Organization on Standardization [ISO], OECD, and Institute of Electrical and Electronics Engineers [IEEE]), and consider related work of the United States (such as the NIST AI risk management framework and the Blueprint for an AI Bill of Rights) and the EU (such as the EU AI Act, HLEG and European Standardisation Organisations. Both the United States and EU affirm the importance of a shared understanding and consistent application of concepts and terminology that include, but are not limited to: risk, risk management, risk tolerances, risk perception, and the socio-technical characteristics of trustworthy AI.

This work could be informed by:

- Alignment with international standards development organizations.
- Ongoing efforts within OECD Working Party on AI Governance (AIGO) and OECD Network of AI Experts (ONE.AI).
- NIST's efforts in developing an AI risk management framework and its related guides and tools.

- The National AI Initiative Act and Blueprint for an AI Bill of Rights
- The EU AI Act
- Work developed by the European standards organizations.
- The deliverables of the EU High-Level Expert Group, such as the ALTAI Assessment List for Trustworthy AI

3.2 EU-U.S. Leadership & Cooperation on International Technical Standards and Tools for Trustworthy AI and Risk Management

The United States and EU affirm that AI technologies should be shaped by our shared democratic values and commitment to protecting and respecting human rights. Leadership in standards for AI and emerging technologies should promote safety, security, fairness, non-discrimination, interoperability, innovation, transparency, diverse markets, compatibility and inclusiveness. Both sides are committed to supporting multi-stakeholder approaches to standards development, and recognize the importance of procedures that advance transparency, openness, due process, impartiality, and inclusiveness.

3.2.1. International Technical Standards

Standards shape the design, development and use of technologies that underpin our economies, cultures and societies. It is important to understand the opportunities technologies have for positive impact as well as the risks and vulnerabilities that can cause cascading negative consequences without proper safeguards.

AI standards that articulate requirements, specifications, test methodologies, guidelines, or trustworthy characteristics can help ensure that AI technologies and systems meet critical objectives (e.g., functionality, interoperability, and trustworthiness) and performance characteristics (e.g., accuracy, reliability, and safety). In contrast, standards that are not fit for purpose, not yet available, not broadly accessible (notably to start-ups and small and medium-sized enterprises (SMEs)), or not designed around valid technological solutions, may hamper innovation and the timely development and deployment of trustworthy AI technologies.

Global leadership, participation, and cooperation on international AI standards will be critical for consistent "rules of the road" that enable market competition, preclude barriers to trade, and allow innovation to flourish. This may enable governments to align with an international approach when developing internal policy while safeguarding and advancing respect for human rights and democratic values.

As like-minded partners, the EU and United States seek to support and provide leadership in international standardization efforts. This can be achieved by contributing and cooperating on technical AI standards development, currently underway in international standards organizations, which will impact the design, operation, and evaluation and measurement of trustworthy AI and risk management.

Without prejudice to the specificities and needs of their respective legal systems [US wants to add: in relation to standardisation], both the United States and EU aim to support and use international standards, as appropriate, as the basis for technical regulations, conformity assessments and regional standards, adhering to the WTO TBT principles, and role model this commitment to 3rd countries. At the same time, both the United States and EU, working with our respective stakeholders and mechanisms, aim to identify critical gaps in existing international AI standards development activities. The EU and the United States can cooperate on AI pre-standardization research and development (R&D) to advance the technical and scientific foundation for development of international standards development.

The EU and United States intend to actively promote the participation of a wide range of stakeholders – including their standards experts, impacted communities, domain-experts, and other cross-disciplinary experts – in ongoing standards development work. Both sides plan to promote continual expert-level information sharing to improve understanding of the respective approaches and possible uptake of common technical solutions. The United States and EU governments can play a convening role with their respective stakeholders to promote appropriate representation at critically important standards-setting bodies and organizations. Furthermore, both sides intend to promote the development and voluntary use of international standards that are developed in an open and transparent manner, that are technically sound, performance based, and suitable for the purposes of public and private sector use. Both sides also plan to support the consideration of SMEs and start-up communities in standards development activities.

In the short term, this activity will engage with stakeholders to identify standards that are of mutual interest, starting with AI trustworthiness, bias, and risk management.

3.2.2.   Tools for Trustworthy AI and Risk Management

Regardless of respective policy landscapes technical tools are needed to map, measure, manage, and govern AI risks. Tools – defined by OECD as instruments and structured methods (of either a technical, procedural or educational nature) that can be leveraged by relevant stakeholders to make their AI applications trustworthy – should be built upon strong scientific foundations and aligned with standards development activities. Objectives of the EU-U.S. joint work on tools for trustworthy AI and risk management are as follows:

● Shared Hub/Repository of Metrics and Methodologies

The EU and United States intend to work together to build a common knowledge base of metrics and methodologies for measuring AI trustworthiness, risk management methods, and related tools. The latter could for instance include the measurement of AI's environmental implications, which should include its negative and positive impacts. Building on the common work related to terminology, this effort involves the development of selection criteria for inclusion of metrics in the shared hub/repository. The knowledge base would be openly and publicly accessible online, and could augment the ongoing OECD efforts in the area. The selection and inclusion of metrics and tools supports a useful repository for the two parties but does not constrain or prejudge the [EU wants to add: regulatory] activities of the two parties.

- Analysis of Tools for Trustworthy AI

The United States and EU expect to support studies to characterize the landscape of existing sector- or application-agnostic and sector- or application-specific standards and tools for trustworthy AI developed by standard developing organizations, industry including start-ups and SMEs, open-source developers, academia, civil society organizations, governments and other stakeholders. Learnings from these studies could inform and support AI standards development efforts, and to identify commonalities in approaches that operationalize shared values and frameworks as well as gaps in existing methodologies as they relate to EU-US shared values – ultimately supporting interoperable risk management strategies, evaluation and measurement tools. As trustworthy AI tools begin to be deployed more widely to align with AI standards, the learnings from this activity may not only inform standards development, but shape AI standards themselves.

3.3 Monitoring and Measuring Existing and Emerging AI Risks

With the shared understanding that advances in AI can lead to both positive and negative impacts on people, markets, innovation and societies, and with the goal of keeping up with the rapid progress of AI, the United States and EU intend to develop knowledge-sharing mechanisms on cutting-edge scientific research in AI and related risks, which have the potential to significantly impact EU and US trade and technology.

The United States and EU intend to take actionable steps towards:

- Tracker of risks and risk categories based on context, use cases, and empirical data on AI incidents, impacts, and harms. A values-based understanding of existing risks serves as a baseline for detecting and analyzing both existing and emergent risks. This activity seeks to provide a common ground for both parties to better define the origin of risks and their impact, and to better organize risk metrics and methodologies for risk avoidance or mitigation. The tracker would be continually extended or updated to include new risks emerging from the dynamics of development and usage, improvements in understanding of the potential harms to shared values, compound risks due to the interaction of several systems, or unknown but predictable risks that could arise from new AI methods and/or contexts of use.

- Interoperable tests and evaluations of AI risks: Evaluations strengthen research communities, establish research methodology, support the development of standards, and facilitate technology transfer. Evaluations inform consumer choice and facilitate innovation through transparency of system functionality and trustworthiness and can be used for compliance tests. A significant challenge in the evaluation of trustworthy AI systems is that context of deployment matters; for example, accuracy measures alone do not provide enough information to determine if a system is acceptable to deploy. The accuracy measures must be evaluated based on the context within which the AI system operates and the associated harms and benefits that could occur. Other challenges include quickly

moving state of the art, the diversity of architectures of AI systems, and the complex behavior and emergent capabilities of large deep learning systems. New joint efforts in AI tests and evaluations are expected to focus on trustworthiness characteristics of system performance in addition to metrics such as accuracy.

4. Implementation plan

Advancing shared terminology and taxonomy provides an interoperable lexicon to communicate about risk and appropriate risk treatment, which in turn promotes interoperable measurements and evaluations of AI risks and impact. Jointly developing tools such as a shared repository of metrics likewise fosters transparency, interoperability, or uniformity of risk measurements. Collectively, such efforts improve effectiveness, transparency, and interoperability of risk assessment and risk management.

The objectives described in this joint roadmap can be achieved through several mechanisms including:

Short-term Objectives:

- Establish inclusive cooperation channels:
  - Establish three (3) expert working groups on 1) AI terminology and taxonomy;2) AI standards and tools for trustworthy AI and risk management; and 3) monitoring and measuring existing and emerging AI risks.
  - Develop work plans for each of the three expert groups mentioned above.
  - Establish stakeholder and expert consultation plans, including expert workshops.

- Advancing shared terminologies and taxonomies:
  - Conduct a mapping of terminology and taxonomy in key EU and U.S. documents and international standards that include, but are not limited to: risk, risk management, risk tolerances, risk perception, and the socio-technical characteristics of trustworthy AI.

- AI Standards:
  - Conduct a landscape analysis of international standards of interest to the EU or United States, and evaluate the level of participation in and contribution to international standards development.
  - Identify international standards of interest for mutual cooperation.
  - Promote participation of experts and relevant stakeholders in respective international standardization bodies.

- Development of Tools:
  - Establish a process for tool selection, inclusion and revision.
  - Establish the criteria to evaluate tools for trustworthy AI.

- Monitoring and Measuring Existing and Emerging AI Risks:

- Establish the objectives and methodology for tracking existing AI risks based on use cases and incidents reporting, which may be based on pilot attempts at categorization.
- Identify the research methodology for tests and evaluations of emerging AI risks.

Long term Objectives:

- Establish inclusive cooperation channels to inform input to and leadership in international standards:
  - Conduct expert workshops.
  - Review and assess progress made and update the roadmap if needed.
  - Identify opportunities to cooperate and share roadmap outputs and learnings.

- Advancing shared terminologies and taxonomies:
  - Develop or revise shared understanding of terminology and taxonomy.

- AI Standards:
  - Organize possible cooperation in international standardization fora with respect to certain identified items.
  - Work with and support experts in the development or deployment of standards of mutual interest.

- Development of Tools:
  - Identify metrics and methodologies to add to the shared hub/repository.
  - Update and maintain the shared hub/repository.

- Monitoring and Measuring Existing and Emerging AI Risks:
  - Create benchmarks and evaluations of AI risks that could be informed by empirical studies of AI incidents.
  - Theoretically-informed and analytical forecasting of emerging and future risks.

APPENDIX :: EU and U.S. approaches to AI risk management

Examples of the US's risk-based approach to AI.

NIST's draft AI Risk Management Framework (AI RMF)

The AI RMF is intended to address challenges unique to AI systems and encourage and equip different AI stakeholders to manage AI risks proactively and purposefully. The Framework describes a process for managing AI risks across a wide spectrum of types, applications, and maturity – regardless of sector, size, or level of familiarity with a specific type of technology. Cultivating trust by understanding and managing the risks of AI systems helps preserve civil liberties and rights and enhances safety while creating opportunities for innovation and realizing the full potential of this technology.

The AI RMF is a voluntary framework seeking to provide a flexible, structured, and measurable process to address AI risks prospectively and continuously throughout the AI lifecycle. It is intended to help organizations manage both enterprise and societal risks related to the design, development, deployment, evaluation, and use of AI systems through improved understanding, detection, and preemption. Using the AI RMF can assist organizations, industries, and society to understand and determine their acceptable levels of risk.

The AI RMF is not a compliance mechanism, nor is it a checklist intended to be used in isolation. It is law- and regulation-agnostic, as AI policy discussions are live and evolving. While risk management practices should incorporate and align to applicable laws and regulations, the NIST AI RMF is not intended to supersede existing regulations, laws, or other mandates; it should support organizations' abilities to operate under applicable domestic and international legal or regulatory regimes. Engagement with the broad AI community during development of the AI RMF informs AI research, development, and evaluation by NIST and others. The AI RMF is currently in its second draft and is expected to be released in early 2023.

NIST AI RMF employs the following definitions:

Note: additional considerations are underway to further align with international AI standards (including ISO/IEC 22989, ISO/IEC 23894 etc.)

- **Risk**: In the context of the AI RMF, 'risk' refers to the composite measure of an event's probability of occurring and the magnitude (or degree) of the consequences of the corresponding events. The impacts, or consequences, of AI systems can be positive, negative, or both and can result in opportunities or threats (Adapted from ISO 31000:2018).
- **Risk management**: Risk management refers to coordinated activities to direct and control an organization with regard to risk (Source: ISO 31000:2018).

- **Risk tolerance:** Refers to the organization's or stakeholder's readiness or appetite to bear risks in order to achieve its objectives. Risk tolerance can be influenced by legal or regulatory requirements (Adapted from: ISO Guide 73).
- **Socio-technical characteristics of AI trustworthiness**: A system is considered trustworthy if it is valid and reliable, safe, fair and with managed bias, secure and resilient, accountable and transparent, explainable and interpretable, and privacy-enhanced.

The Blueprint for an AI Bill of Rights

The Blueprint for an AI Bill of Rights is a set of five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence. Developed through extensive consultation with the public, these principles are a blueprint for building and deploying automated systems that are aligned with human rights and democratic values. The Blueprint for an AI Bill of Rights gives concrete steps that can be taken by many kinds of organizations—from governments at all levels to companies of all sizes—to uphold these values.

The Blueprint for an AI Bill of Rights lays out five core protections to which everyone should be entitled:

- **Safe and Effective Systems**: You should be protected from unsafe or ineffective systems.
- **Algorithmic Discrimination Protections**: You should not face discrimination by algorithms and systems should be used and designed in an equitable way.
- **Data Privacy**: You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used.
- **Notice and Explanation**: You should know that an automated system is being used and understand how and why it contributes to outcomes that impact you.
- **Human Alternatives, Consideration, and Fallback**: You should be able to opt out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter.

To protect the civil rights of Americans, and ensure technology is working for the American people, and to move these principles into practice, the Blueprint for an AI Bill of Rights also includes concrete steps which governments, companies, communities, and others can take in order to build these key protections into policy, practice, or technological design to ensure automated systems work in ways that protect human rights and democratic values.

The Blueprint for an AI Bill of Rights is focused on protecting human rights and democratic values, so the systems defined as in scope are based on *impact* as opposed to the underlying technical choices made in any system, since such choices can and do change with the speed of technological innovation. Specifically, the Blueprint should be applied with respect to all automated systems that have the potential to meaningfully impact individuals' or communities' rights, opportunities, or access, defined as below:

- **Rights, opportunities, or access**: The set of: civil rights, civil liberties, and privacy, including freedom of speech, voting, and protections from discrimination, excessive punishment, unlawful surveillance, and violations of privacy and other freedoms in both public and private sector contexts; equal opportunities, including equitable access to education, housing, credit, employment, and other programs; or, access to critical resources or services, such as healthcare, financial services, safety, social services, non-deceptive information about goods and services, and government benefits.

The EU risk-based approach to AI

The EU approach to AI is **human-centric**, aiming to foster the trust of and uptake by citizens while offering the conditions for companies and researchers to develop and deploy trustworthy AI in Europe. A **balanced** approach to AI is needed in order to reap the benefits of this technology while addressing potential risks its use can pose to safety and fundamental rights.

Promoting the development of **trustworthy AI** is a key aspect of the European strategy on AI, and it plays a crucial role in the promotion of a values-based European digital economy and society. The EU supports basic and applied research, testing and experimentation (including regulatory sandboxes), and deployment.

Trust is also needed for uptake and adoption, and thus a **precondition for the benefits of AI** to materialize in the EU digital market. The EU's human-centric approach to AI involves balancing and assessing on an ongoing basis the progress and benefits of AI against their potential risks to individuals and society. Values guiding socio-technical governance efforts are derived from the Treaties of the European Union and its Charter of Fundamental Rights that prescribes a series of fundamental rights that EU member states and EU institutions are legally obliged to respect when implementing EU law.

Coordinated Plan on AI

The Coordinated Plan on AI (2001) puts forward EU measures on supporting innovation and enabling conditions, such as access to data and computing infrastructure, promoting the development and deployment of trustworthy AI solutions, training and skills development, as well as promoting the EU's value-based approach to AI on the global stage.

To develop a European **ecosystem of excellence**, the EU is setting up AI Networks of Excellence to foster cooperation among Europe's AI research teams to tackle major scientific and technological challenges in AI hampering deployment of AI-based solutions, including the development of ethical and trustworthy AI. Furthermore, it set up a European public-private partnership on AI, data and robotics.

To bridge the gap between AI research and deployment. AI Testing and Experimentation Facilities are being set up. They will allow companies to test their AI-based technologies in real-world environments. This will be complemented by the development of a European marketplace for trustworthy AI solutions, connecting resources and services to support innovators in developing and deploying trustworthy AI solutions.

The EU AI Act

Certain specific features of AI technologies (e.g. opacity) can make the application and enforcement of existing legislation more challenging and generate high risks for which a tailored regulatory response is needed. Therefore, the EU AI Act introduces a set of rules applicable to the design, development and use of certain high-risk AI systems, as well as restrictions on certain uses of remote biometric identification systems.

By earning people's trust, the envisaged risk-based legislation should also foster the uptake of AI across Europe. To be future-proof and innovation-friendly, the proposed legal framework is designed to intervene only where this is strictly needed and in a way that minimises the burden for economic operators, with a light governance structure.

The proposed AI regulation puts forward rules to enhance transparency and to minimise risks to safety and fundamental rights before AI systems can be used in the European Union. It is a proportionate and risk-based approach.

The proposal focuses on high-risk AI use cases. Whether an AI system is classified as high-risk depends on its intended purpose and on the severity of the possible harm and the probability of its occurrence.

AI systems identified as high-risk would include AI technology used in: safety components of regulated products; critical infrastructures; educational and vocational training; employment, workers management and access to self-employment; essential private and public services; law enforcement that may interfere with people's fundamental rights; migration, asylum and border control management; and administration of justice and democratic processes.

High-risk AI systems are to comply with specific requirements, which include the setting up of a sound risk management system, the use of high-quality datasets, appropriate documentation to enhance traceability, the sharing of adequate information with the user, the design and implementation of appropriate human oversight measures, and the achievement of the highest standards of robustness, safety, cybersecurity and accuracy.

Such requirements will be supported by harmonised technical standards to be developed by the European Standardisation Organisations (ESOs) on the basis of a mandate from the European Commission. Appropriate agreements in place between the ESOs and international standardisation organisations ensure that fit-for-purpose international standards can be taken over by ESOs and proposed as European harmonised standards in response to a standardisation request.

High-risk AI systems must be assessed for conformity with these requirements before being placed on the market or put into service. Depending on the type of high-risk AI system, the conformity

assessment procedure may be based on internal control or rely on the involvement of a third-party certification body.

The proposed regulation will also encourage the use of regulatory sandboxes establishing a controlled environment to test innovative technologies for a limited time.

Draft Joint Statement on protecting human rights defenders online

Begin Text:

The U.S.-EU partnership is a cornerstone of our shared strength, prosperity, and commitment to advancing freedom, democracy, and respect for human rights around the world. In the framework of the U.S.-EU Trade and Technology Council, we address the misuse of technology threatening security and human rights and have committed to strengthen our cooperation on protecting human rights defenders online; promoting the open, free, global, interoperable, secure, and reliable Internet as stated in the Declaration for the Future of the Internet; combatting online harassment and abuse; eliminating arbitrary and unlawful surveillance; combatting government-imposed Internet shutdowns; and countering disinformation and foreign information manipulation and interference

Digital technologies are a vital resource for human rights defenders and civic actors around the world, including in the context of documenting human rights violations and abuses, and international humanitarian law violations. However, these technologies can also be misused to target human rights defenders and undermine civic space. The United States and the European Union (EU) are deeply concerned by the rapid growth of online threats against human rights defenders and the ongoing contraction of civic space around the world. Human rights defenders continue to face threats and attacks, including arbitrary or unlawful online surveillance, censorship, harassment, smear campaigns, disinformation to include gendered disinformation, targeted Internet shutdowns, and doxing. Online attacks often pave the way for physical human rights violations and abuses, including beatings, killings, enforced disappearances, and arbitrary detention.

Women human rights defenders are disproportionately impacted by threats and attacks, which are more often gendered and sexualized than threats against their male counterparts and increasingly take place online. Many women human rights defenders face multiple and intersecting forms of discrimination and sexual and gender-based violence, including on the basis of other characteristics, including race, religion, ethnicity, disability, sexual orientation, socioeconomic status, or gender identity. Acts of gender-based online harassment and abuse have a chilling effect, leading to self-censorship and disengagement of women from public life and discouraging the political and civic ambitions of adolescent girls.

Given these trends, and in line with our respective policies, (the EU Action Plan for Human Rights and Democracy 2020-2024 and the EU Guidelines on Human Rights Defenders and the Guidelines for U.S. Diplomatic Mission Support to Civil Society and Human Rights Defenders, we reaffirm our joint commitment to protecting human rights defenders from threats and attacks and promoting freedom of expression, association, and peaceful assembly, both online and offline.

The United States and EU firmly condemn the misuse of technology by both state and non-state actors to target human rights defenders. We reaffirm that all human rights and fundamental freedoms apply both online and offline. We recall, that according to the UN Declaration on Human Rights Defenders, adopted by consensus by UN member States, States "*shall take all necessary measures to ensure the protection by the competent authorities of everyone, individually and in association with others, against any violence, threats, retaliation, de facto or de jure adverse discrimination, pressure or any other arbitrary action as a consequence of his or her legitimate exercise of the rights referred to in the present Declaration*". States should work to prevent attacks against human rights defenders and bring perpetrators of attacks to justice.

We also emphasize the responsibility of the private sector, in particular technology companies and digital platforms across the digital ecosystem, to respect human rights in line with the UN Guiding Principles on Business and Human Rights. We urge companies to prevent the misuse of their products and platforms, conduct due diligence, take effective action to address all forms of online violence and unlawful or arbitrary surveillance against human rights defenders, support victims and survivors in their search for remedy and accountability for violations and abuses, and provide a safe space for human rights defenders to carry out their work. We encourage companies to establish a grievance mechanism for internal and external reporting of misuse. We also support stronger accountability for technology platforms and recognize the role of government to enhance online safety, security and privacy.

We will continue leveraging our joint expertise to identify and mitigate threats faced by human rights defenders online. The United States and EU will work to develop effective policies to mitigate threats to democracy and human rights online, and to promote appropriate oversight and safeguards for the use of surveillance technologies. We will take a multistakeholder approach, including through working with partner governments, private sector, academia, civil society including human rights NGOs and human rights defenders, survivors of online harassment and abuse, multi-stakeholder organisations, and international organisations. We commit to counter the proliferation of foreign commercial spyware and hacking tools by actors that misuse them to target human rights defenders and others, and to promote accountability for companies that are complicit in enabling human rights abuses.

We will continue to give human rights defenders a platform to highlight the online threats they face, including through public events, as we did in the framework of the 49th Session of the Human Rights Council. We recognise the important role that the UN Office of the High Commissioner for Human Rights (OHCHR) and UN Special Procedures have in identifying innovative solutions for the online protection of human rights defenders. We are committed to working closely to elevate these issues within the UN system, including with the UN Special Rapporteur on the situation of Human Rights Defenders and the UN Tech Envoy. We call on likeminded countries to join in the effort and to publicly amplify their support for human rights defenders. The EU and the United States are committed to ensure access and meaningful participation of civil society in all conversations around human rights in the multilateral fora.

The United States and EU will continue to support mechanisms, including the Digital Defenders Partnership, the Lifeline Embattled CSO Assistance Fund, and ProtectDefenders.EU that provide resources for at-risk HRDs and civil society organizations, including for preventing digital attacks and for supporting digital security needs. In the framework of the Trade and Technology Council, we commit to expanding cooperation and mutual learning between U.S.- and EU-funded emergency mechanisms and the broader community of practice, with the goal of expanding the beneficial impact of these resources for human rights defenders worldwide.

The United States and EU are also committed to fostering cooperation through our missions around the globe. U.S. Embassies and EU Delegations play an instrumental role in monitoring developments and conducting joint outreach on issues surrounding human rights defenders' protection. The United States and the EU stand ready to engage with government partners to strengthen and support their national efforts, including capacities and institutions, to prevent and address threats against human rights defenders.

_____