Charter of Trust Response to the EU – US Trade and Technology Council Working Group 3

Introduction

We, the members of the Charter of Trust, welcome the opportunity to provide input to the EU – US Trade and Technology Council. Digitalization has transformed nearly every aspect of modern life. Today, billions of devices are connected through the Internet of Things. While this created great opportunities, it also harbors great risks. To make the digital world more secure, we have joined forces as the Charter of Trust - a unique initiative by leading global companies - with a cooperation that has reached significant milestones toward improving cybersecurity and has ambitious goals for the future. The Charter of Trust's focus is on three important objectives: To protect the data of individuals and companies; to prevent damage to people, companies and infrastructures; and to create a reliable foundation on which confidence in a networked, digital world can take root and grow.

Working Group 3 - Secure Supply Chains

Technological progress in the field of semiconductors plays a major role in the modern world. Semiconductors are essential for industry-wide advancement and innovation. Today, no individual state can have full autonomy over the semiconductor supply chain, and there is a very high level of interdependence between countries and regions. These interdependencies make the supply chain highly complex and vulnerable to disruptions, including supply chain shortages or increasing geopolitical tensions.

To build a robust supply chain, it is essential to ensure the availability of materials, skilled labor, R&D equipment and facilities, manufacturing capacity, and technological know-how. Solid government support will be required to address these factors, and improve the competitiveness and resilience of the semiconductor supply chain in North America and Europe. To this end, the **TTC provides a unique forum to collaboratively take on these global challenges and a unique opportunity for the US and the EU to work together on a transatlantic initiative** to build a deeper understanding of semiconductor supply chains, agree on topics for research cooperation, pinpoint shortages in the value chain and take aim at a more balanced, steady and secure supply on a global scale. Against the backdrop of current and comprehensive efforts to expand manufacturing capacities on both sides of the Atlantic, U.S and EU governmental investments should always take into consideration the respective domestic market-demand of their own user industries, in order to achieve complementarity and create mutual synergies, and avoid a subsidy race.

Specific areas of collaboration could include: regularly sharing information, best practices and intelligence on mitigating upcoming shortages; effective early warning mechanisms, to strengthen preparedness in moments of crisis; exchange of information on long-term investment strategies; international standardization activities; workforce development; and best practices to reduce the environmental impacts of production.

In addition, both U.S. and European stakeholders should be guaranteed equal market access and competitive conditions. The coordination of export control measures is also crucial to mitigate any unfavorable impact on European or U.S. companies along the semiconductor supply chain. Unilaterally controlling regulations for foreign goods that do not represent a safety risk should be eliminated and export controls should be multilaterally and strategically targeted to address specific security issues. In addition, a transparent and consistent authorization procedure should be established for the United States as well as the European Union to create a level playing field for both regions.

The digitalization of industry (further accelerated by the COVID-19 pandemic) has enhanced change in the supply chain, which is now comprised of large and growing volumes of third-party partners, suppliers, service providers, contractors etc. who need access to data and assurances they can control who sees that data.

Yet, supply chain digitalization also brings new cyber risks. Data breaches, ransomware attacks and malicious activities from insiders or attackers can occur at any point in the supply chain. A localized security incident with a single supplier can still significantly disrupt a fully integrated supply chain process. Ensuring effective cybersecurity in the supply chain will be key to protecting the integrity (and quality) and availability of products and services, and the associated data, processes and systems involved.

Protection of Intellectual Property as well as of Personal Identifiable Data needs a common understanding and close cooperation of the respective rule setting entities on both sides of the Atlantic.

In this context, **the Charter of Trust calls on the EU and the US to collaborate on ways to better identify common vulnerabilities or dependencies and address policy gaps to improve supply chain security and resilience**. This approach could include a **common certification mechanism** based on international standards and certification schemes, as well as **wider holistic baselines for cybersecurity**, drawing on industry-led cybersecurity recommendations such as the Charter of Trust's baseline security requirements in the digital supply chain.

This shall be complementary to discussions taking place within Working Group 4 on ICT security and competitiveness.