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

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 4 - ICT security and competitiveness

As our dependency on technology continues to grow so will the scale and sophistication of cybersecurity threats. While some attacks are costly and inconvenient, others can be severely damaging. With cybersecurity quickly becoming a new battleground for state competition, businesses and government share a collective responsibility to collaborate on preventing cyberattacks that could have a devastating impact or prompt national or global crises. Coordinated efforts to curb rising cybercrime are urgently needed in Europe and the United States. In 2011, global annual damage caused by cybercrime was at around $3 trillion, and in 2021 that number rose to $6 trillion. By 2025 that number is projected to go up to $10.5 trillion. We must join forces now to shore up the security of the critical infrastructure that keeps our society functioning.

Addressing **the magnitude of the cybersecurity challenge we face calls for global rather than local solutions, which can be specifically enabled by transatlantic leadership:** EU-US joint action should focus on **aligning and/or mutually recognizing risk-based approaches to cybersecurity policy** and regulation that rely on consensus-based international standards and risk management industry best practices to strengthen cybersecurity capabilities. Such common approaches should:

- **facilitate cross-sectoral industry collaboration to embed a cybersafe culture across every organization**: the Charter of Trust recently developed key recommendations for industry and governments, which are also commitments taken by the Charter of Trust's partners:
    - For example, security by default should apply to national education curricula and continuous professional development. Employees from every level in industry and the public sector should be cyber aware in their jobs and their daily lives.

- **support the uptake and development of cybersecurity solutions powered by advanced technologies,** from artificial intelligence to cloud, data analytics and threat visualization, as well as the **latest encryption techniques**:

- For example, cloud-based platforms can allow organizations to share and act on threat intelligence, enabling them to rapidly research the latest global security threats, aggregate actionable intelligence, consult with experts and collaborate with peers.
- As organizations increasingly rely on hybrid multi-cloud environments, where some can be owned and managed by third-party providers, innovative encryption solutions such as Confidential Computing capabilities to protect 'data-in-use'; or "Homomorphic Encryption" which allows manipulation of data by permissioned parties while it remains encrypted, can allow organizations to mitigate the security and privacy risks.
- While quantum computers will help solve new categories of problems that are beyond the reach of even today's most powerful traditional computers, they will also make our current encryption methods obsolete. As we prepare for a quantum world, developing and deploying new, quantum-safe encryption methods such as lattice-based cryptography will also be crucial.

Through "Security by Design", European and U.S. manufacturers of networked devices and digital services are striving to design commercial solutions that are highly resilient and prepared to withstand cyber-attacks. However, due to constantly evolving threat vectors and methodologies, no company can guarantee to be fully immune to cyber-attacks or to have all encompassing cybersecurity. Government agencies in the United States and the EU should directly notify companies of weaknesses and vulnerabilities they have discovered in IT solutions, since any unaddressed security issue in the IT domain jeopardizes overarching cybersecurity, in addition to companies applying best practices in cyber hygiene and secure service/product development. This would help them provide the best possible level of risk-based cyber resilience in services and products.

Vulnerabilities must be addressed and communicated to the public as soon as fix is available, or as soon as affected parties have been reasonably able to update their systems e. Consequently, all relevant parties of the EU and the USA must coordinate disclosure of information about vulnerabilities and support companies in their efforts to ensure high levels of cyber resilience in products and services.

To ensure a high level of cyber resilience, both governments should actively promote businesses in all sectors to certify their business processes based on international standards such as ISO 27001 and IEC 62443 and ensure that their regulations reference the same set of coordinated international standards, as for instance those developed by the IEC and ISO. Furthermore, government procurements should press suppliers to meet cybersecurity standards commensurate with the risk of the use case in question, for example through certifications based on international cybersecurity standards. To achieve this, the United States and the European Union would need to work towards the reciprocal recognition of certifications in the field of cybersecurity.