September 2019

ITI RESPONSE TO ENISA PAPER ON EU ICT INDUSTRIAL POLICY

1. Do you agree with the principles outlined in this paper? Please outline where you agree or disagree.

ENISA Conclusion 1: The EU should revisit its ICT industrial policy by recognising it as strategic, while also supporting its ICT sector.

ITI response: ITI welcomes the idea of revisiting the European industrial strategy in order to allow European ICT companies to scale up and compete globally. A successful European industrial strategy should allow for flexibility, encourage investment for start-ups and scale-ups. Any strategy should enable these companies to compete globally and avoid protectionist measures, while government funding should remain consistent with the EU's state aid framework.

ENISA Conclusion 2: Building on the Airbus success story, competition law should be interpreted flexibly and in a manner that supports and incentivises the European ICT industry;

ITI response: ITI strongly supports free and undistorted competition as key to promoting innovation and consumer welfare. Europe is a leader in several segments of the digital economy, with cybersecurity becoming a growing areas of expertise. While the EU competition law framework is sufficiently flexible to address new challenges, the underlying principles for the debate on its future should be interoperability, transparency, nondiscrimination and consumer choice. Regulators should in particular focus on consumer welfare, not on protecting competitors or creating champions. Given the intersection between competition and other policies in an increasingly digitalised global economy, international dialogue is needed on these policies, focusing on the complementarity between competition, consumer welfare, and innovation.

ENISA Conclusion 3: The EU and Member States should reduce regulatory barriers and administrative burdens for EU ICT businesses;

ITI response: We strongly support ENISA's call for reducing regulatory barriers and administrative burden in order to advance European and global technology companies' success. ICT companies strive constantly to succeed in fiercely competitive, fast-growing markets. In order to enable ICT companies to grow and provide value to global societies, ITI encourages governments to ensure that markets remain open to innovative challengers, maintaining consumer welfare and economic efficiency as the final objectives and focusing on resolving proven market failures. Any regulatory approach should therefore be developed in a strictly evidence-based fashion in order to comply with Better Regulation principles that the European Commission has set out for itself.

Global Headquarters
1101 K Street NW, Suite 610
Washington, D.C. 20005, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
itic.org

ENISA Conclusion 4: European IP needs to be protected. The EU and Member States should consider identifying European IP developed with public funds as strategic and subjecting it to pre-export regulatory approval;

ITI response: Europe is a leader in the development of a range of intellectual property that supports technological growth and development within the EU and beyond. We fully acknowledge the necessity of maintaining export control regimes that ensure European physical and cybersecurity, and agree on the continued necessity of robust intellectual property protections. However, as the European Commission has noted, export control systems must continuously strike the right balance between the EU's overarching foreign and security policy objectives and its economic and commercial interests in a changing security, economic and technological environment. Any changes to European or Member State pre-export regulatory approval regimes should strive to achieve this balance, and take into account the possible impact on the competitiveness in technological development of companies operating in the EU. Where deemed necessary, such changes should adhere to international best practices in pursuing clearly-stated foreign and security policy objectives, rather than industrial policy goals. As we have seen in other economies, export control measures implemented in an overly-broad or unilateral manner can inadvertently disadvantage companies operating domestically, without advancing security interests. We look forward to continuing to engage directly with ENISA and the European Commission on these important topics.

ENISA Conclusion 5: Public procurement in the Member States should be used to stimulate the EU ICT industry;

ITI response: Public procurement should be as open and inclusive as possible to ensure fair competition and enable the best offer to win a tender. Public procurement rules should foster innovation and adoption of state-of-the-art technology, but should remain technology-neutral. Providers should not be favoured based on their country of origin or establishment but rather on their ability to meet the technical demands of a tender with the most competitive offer.

ENISA Conclusion 6: The EU needs a long-term strategy for building and maintaining a cyber-skilled Europe;

ITI response: There is a strong need to boost cyber-skills and capabilities in Europe and globally. Governments should assess education systems to meet today's ever-demanding labour markets in an increasingly digitalised world. The EU should also ensure sufficiently open labour markets that enable companies to hire the best talent from across the world.

ENISA Conclusion 7: The EU should embrace and encourage a more risk-based entrepreneurial culture. Venture capital should be more readily accessible to European ICT businesses with strong growth potential.

ITI response: ITI fully supports this goal and agrees that venture capital is a key resource to help start-ups and scale-ups grow.

2. Do you think Europe should focus on developing the cybersecurity market? If yes what do you think are Europe's competitive advantages and how do you envisage that these advantages will develop?

ITI's members are global companies with complex supply chains around the world, including both producers and users of cybersecurity products and services. We support the EU's continuous work with its international partners to strengthen cybersecurity in Europe and globally. Europe has a strong and growing cybersecurity industry. A high level of privacy and data protection for companies operating in Europe is further increasing the need for state-of-the-art cybersecurity equipment and software.

Cybersecurity is integral to the EU's modern economy and competitiveness. While cyberspace holds great benefits for society, it also presents opportunities for misuse and exploitation. Cybersecurity concerns hinder innovation and growth, and digital disruptions can threaten national security, businesses, and individuals. While ICT companies and governments are focusing on managing supply chain risks and the security of networks, malicious behavior is an increasing and ever-evolving threat for both the public and private sectors. Industry is in the process of building security into products, services, and supply chains, along with providing security solutions, while governments play a key role in advancing cybersecurity best practices. Cybersecurity is a shared responsibility – neither governments nor companies can address it alone. The private sector owns and operates elements of critical infrastructure that are targeted by malicious cyber activities. Those owners and operators should be viewed as partners in ensuring the protection of this critical infrastructure. The ICT community has been foundational in developing the infrastructure of cyberspace. It has also provided leadership, innovation, and stewardship in all aspects of cybersecurity for nearly two decades. Increasingly, companies in all sectors are investing in cybersecurity and want to contribute to public-private partnerships, which have proven to be an effective approach to tackle cybersecurity challenges as they enable targeted resource investment, shared technical expertise, and the identification of appropriate policy solutions.

We recommend that Europe's future cybersecurity policies support and align with international industry-backed approaches in order to ensure that cybersecurity companies in Europe can compete globally and are not confined to the European market only. We also encourage a multi-stakeholder, public-private approach to cybersecurity standards and policies in order to be able to collaboratively address supply chain security. We support future-proof policies, developed jointly by public and private actors, that recognise the growing complexity of emerging technologies.

3. Do you think competition policy and/or legislation or the interpretation thereof needs to be changed in respect of the European ICT and cybersecurity markets? Please explain.

ITI strongly supports free and undistorted competition as key to promoting innovation and consumer welfare. Europe is a leader in several segments of the digital economy, with cybersecurity becoming a growing area of expertise.

While the EU competition law framework is sufficiently flexible to address new challenges, the underlying principles for the debate on its future should be interoperability, transparency, nondiscrimination and consumer choice. Regulators should in particular focus on consumer welfare,

not on protecting competitors. Deeper analysis of network effects is needed – markets will not necessarily be less competitive or less innovative, as medium and smaller platforms continue to help customers reach a wide range of goods and services. Competitive dynamics across platforms offering different core services to the same customers should also be assessed.

Given the intersection between competition and other policies in an increasingly digitalised global economy, international dialogue is needed on these policies, focusing on the complementarity between competition, consumer welfare, and innovation.

4. Do you agree a more thorough market analysis needs to be carried out to identify where Europe has a competitive advantage in cybersecurity/ICT?

5. Which body or bodies do you think would be most appropriate to carry out this market analysis? Please explain.

6. What do you think could be done to improve the financial standing and ability to grow/expand of European cybersecurity undertakings?

7. Are there any other initiatives that could be put in place to stimulate the European cybersecurity/ICT market?

8. Are there any other issues that you would like to raise to contribute to this debate?

ITI welcomes this opportunity for debate and supports ENISA's initiative to provide input to the European Commission and European Parliament on future policy discussions on cybersecurity. ENISA is uniquely placed to do so due to its expertise and overall view of the cyber ecosystem in Europe.