***Eng Heba M Z AlSawan***

***Head of IT operations & infrastructure at Public Institution For Social Security (PIFSS), KUWAIT***

***Member of women in cybersecurity UK FELLOWSHIP***.

28/07/2023

Subject: Recommendations for Strengthening Cybersecurity Capacity Building

Dear Respected Chair,

I am writing to provide the collective recommendations discussed in our stakeholder meeting on the 26th of July 2023 as requested by the chair for strengthening cybersecurity capacity building platforms. These recommendations aim to foster global cybersecurity resilience and promote collaborative efforts among diverse stakeholders. I believe these steps will effectively address the evolving cybersecurity threat landscape and bridge the gap in workforce capabilities on a social and economic level as listed below.

***1. Regional Level Implementation and Multilateral Cooperation***

Highlight the significance of regional level implementation to strengthen multilateral cooperation in cybersecurity capacity building. Encourage the exchange of best practices and knowledge among countries and regions to harness their competitive technology and knowledge advantage.

***2. Consortium Building and Twinning Programs***

Promote collaboration through consortium building and the establishment of twinning programs, like the successful initiatives pioneered by the European Union and others within the GCC and the region. These endeavours will facilitate knowledge transfer, resource sharing, and research and development efforts to address cybersecurity challenges effectively.

***3. Vocational Cybersecurity Training Programs***

Emphasize the importance of vocational cybersecurity training programs to equip the youth with practical skills. By partnering with educational institutions and industry practitioners, such programs can create job opportunities for graduates and address the reported 3 million cybersecurity vacancies worldwide.

***4. Public-Private Partnerships:***

Encourage public-private partnerships to enhance cybersecurity capacity building initiatives. Governments and private organizations can collaborate to develop comprehensive training programs and resources, leveraging the expertise of both sectors.

***5. Point of Contact (POC) Role:***

Leverage the role of Points of Contact (POCs) to translate cyber threat information into affordable and practical training programs for youth. Ensure that these programs have measurable learning outcomes, enabling individuals to develop necessary skills and contribute to cybersecurity efforts.

***6. Continuous Updating of Training Programs:***

Advocate for regular updates of training programs by involving practitioners in the field. This will ensure that the training content remains relevant to address both existing and emerging cybersecurity threats.

In conclusion, by implementing these recommendations, we can work together to create a more robust and comprehensive approach to countering cybercrime. Strengthening cybersecurity capacity building is vital in safeguarding our digital ecosystem and protecting our societies and economies from cyber threats.

I look forward to collaborating with you and the esteemed delegates in advancing these recommendations to build a safer and more secure cyber landscape.

Thank you Chair,

***Eng Heba M Z AlSawan***

***Head of IT operations & infrastructure at Public Institution for Social Security (PIFSS), KUWAIT***

***Member of women in cybersecurity UK FELLOWSHIP***.