UNITED NATIONS COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT

Working Group on Enhanced Cooperation

Contribution to the guiding questions agreed during first meeting of the WGEC

Submitted by

Australia

CSTD Working Group on Enhanced Cooperation (WGEC)

Contribution from the Australian Government

Introduction

1. The Australian Government welcomes the opportunity to contribute to the Working Group's consideration of how to further implement enhanced cooperation as envisaged in the Tunis Agenda of 2005.

2. Australia characterises enhanced cooperation as the continuing ambition to improve collaboration between all stakeholders in internet governance and decision making. Global internet infrastructure is largely owned and operated by the private sector. Australia advocates the multi-stakeholder approach of internet governance that allows governments, the private sector, the technical community and the public to contribute on equal footing to discussions about the management of key internet resources.

3. Governments, industry, civil society, the technical community, academia and international organisations have all played an important role in shaping the evolution and use of the internet and should continue to do so in the future. This will ensure the internet remains a central point for innovation and a driver of global economic growth and socio-economic opportunities.

4. Australia's contribution to the Working Group provides an example of enhanced cooperation in practice, drawing on the development and implementation of Australia's 2016 Cyber Security Strategy. We offer this example to illustrate an open and transparent process which encourages the equal participation of all stakeholders. We also provide a brief overview of Australia's cyber cooperation program which will contribute to enhanced capacity and cooperation in the Indo-Pacific.

Enhanced cooperation in practice - Australia's Cyber Security Strategy

5. Australia's Cyber Security Strategy was launched in April 2016, after 18 months of consultation and preparation. The Strategy sets out a philosophy and program for meeting the dual challenges of the digital age – advancing and protecting Australia's shared interests online. The Strategy is clear that security and online freedoms are self-reinforcing. A secure cyberspace provides trust and confidence for individuals, business, the public sector and ultimately the global community to share ideas and innovate online for the benefit of all.

6. The Strategy was developed by drawing on the views of an Independent Panel of Experts, submissions received during a public consultation process, and one-on-one consultations with more than 180 business leaders, industry experts and academics. The result is five themes and 33 co-designed cyber security initiatives, all intended to pursue common prosperity and security in the digital

age. The development of the Strategy represented a commitment to openness and transparency where the final product is a multi-stakeholder effort—shaped by those who benefit from it.

7. One of the Strategy's five themes is a national cyber partnership between government, academia and industry to strengthen leadership and tackle emerging issues. This partnership involves regular meetings and information sharing initiatives to enhance cooperation between government and industry.

8. Australia's first Joint Cyber Security Centre, to be opened soon, will facilitate the safe sharing of sensitive information between government and the private sector quicker and easier. The Cyber Security Centre will be complemented by a secure online threat sharing network. These initiatives are about promoting greater collaboration, delivering better outcomes, as well as improving the security and performance of the online economy. Australia is also working to co-design with the private sector, practical national voluntary guidelines promoting good practice to improve cyber security resilience.

9. The Strategy also calls for government to partner with industry in building strong cyber defences intended to better detect, deter and respond to threats and anticipate risks. Australian Stock Exchange (ASX) top 100 companies will be able to improve their cyber security through voluntary governance health checks—enabling boards and senior management to better understand their cyber security status and how they compare to similar organisations. In time, these health checks will be available for all public and private organisations—tailored to size and sector. The Strategy also provides for support for some 5000 small businesses to have their cyber security tested by certified practitioners.

Enhanced cooperation in the Indo-Pacific - cyber cooperation program

10. Australia characterises enhanced cooperation as supporting sustainable development which incorporates the participation of multiple stakeholders from developing countries. This is reflected in Australia's approach to cyber capacity building in the Indo-Pacific, in which emphasis is placed on involving civil society, industry and the research community in delivering assistance.

11. Australia is implementing a cyber cooperation program to assist countries in the Indo-Pacific region to develop their institutional capacity to tackle cyber threats, enhance their cyber security and address cybercrime. The funding will be used for activities and initiatives that include helping ODA eligible countries develop Computer Emergency Response Teams, and national cyber security strategies; reform legal frameworks to combat cybercrime; working to raise awareness of cyber security issues and policy makers; and assisting countries to fill gaps in cyber capacity identified in studies such as the *Cybercrime Needs Assessment* conducted for the Pacific Islands Forum or the World Bank study into *Cybersecurity and Legal Frameworks needed to Facilitate the E-Economy in the Pacific* or their own cyber security strategies.