NATIONAL INFORMATION & COMMUNICATIONS TECHNOLOGY AUTHORITY OF PAPUA NEW GUINEA

MEDIA BRIEFING ON

Making Internet a Safer Place for PNG:

Enhancing Computer Incident Response Team and Assessing National Cybersecurity Capacity

3-7 JUNE, 2019

PORT MORESBY, PNG

The past twenty years has been an extraordinary time for the development of information and communication technologies (ICTs) – and with the 'mobile miracle', has brought the benefits of ICTs within reach of virtually all the world's people. But the next twenty years will be even more dramatic with 200 billion devices being connected through Internet of Things by 2020 and the benefits of broadband become available to everyone, wherever they live, and whatever their circumstances.

Greater connectivity also brings with it greater risk, not least the risk of losing trust and confidence in the networks we rely on, and also in our ability to communicate securely. Security is key to building the trust and confidence in the use of ICT in all aspects of life. Cybersecurity continues to be a big challenge as we embark on the Internet of Things, 5G, Smart Cities and Artificial Intelligence that will affect each and every aspect of our lives. In such an interconnected world a loophole anywhere in the global ICT network represents a challenge anywhere in the network. This includes emergency services; water supplies and power networks; food distribution chains; aircraft and shipping; navigation systems; industrial processes and supply chains; healthcare; public transportation; government services; and even our children's education.

Recognising the significance and to further enhance socio-economic development, National Information & Communications Technology Authority of Papua New Guinea (NICTA) under the technical collaboration of the ITU carried out a CIRT assessment and builds capacity of the stakeholders between 3-7 June 2019. The major stakeholders, including ministries, ICT service providers, specialized institutions for ICTs, academia and relevant non-government agencies, were invited to participate in the weeklong sessions.

Additionally, ITU partnered with the Oceania Cyber Security Centre (OCSC) from Melbourne/Australia to conduct an assessment of the national cybersecurity capacity based on the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford. The systematic and holistic model reviews a country's cybersecurity capacity maturity in terms of five dimensions: Cybersecurity Policy and Strategy; Cyber Culture and Society; Cybersecurity Education, Training and Skills; Legal and Regulatory Frameworks; and Standards, Organisations and Technologies. The review report that the OCSC team will produce in the upcoming months and submit to NICTA will enable the Government to benchmark national cybersecurity capacity and set priorities for strategic investment and capacity development. Support for the CMM review comes from the Government of Victoria.

Pacific Island Countries are considerably aware of the issues and cyber threats. Some countries have made efforts in building a National CIRT. The International Telecommunication Union (ITU), the United Nations Specialized Agency for Telecommunications and ICT, has assisted countries in the Pacific with regard to cybersecurity. For examples, ITU conducted a Readiness Assessment on National CIRT Establishment in Fiji, Samoa, Tonga, Vanuatu. Despite efforts from the Pacific Island Countries and international community, a number of challenges are yet to be addressed either partially or fully in respect of cybersecurity in general and CIRTs in particular. These are such as:

- Assessment, establishment and strengthening of national cybersecurity framework (policy, legislation and strategy), where there are still gaps;
- The need of national CIRTs and CIRT-to-CIRT collaboration;
- Investments and sustainable model of national CIRTs;
- Human and institutional capacity;
- Regional / International coordination and collaboration.
- Awareness in government, public and private sectors, and among citizens and other members of society
- Child Protection Online

Mr. Sameer Sharma, Senior Advisor, ITU *said "As a specialized agency of United Nations on ICT, ITU provides a global forum for discussing cybersecurity, and has been entrusted by world leaders to facilitate international dialogue and cooperation through its Global Cybersecurity Agenda to develop a comprehensive and inclusive international framework for cooperation with the international community aimed at building a common understanding on ways of ensuring peace and stability in cyberspace. With the support from the Department of Communications and Arts, Government of Australia, ITU carried out assessments of CIRTs for Samoa, Tonga, Vanuatu and this week in PNG with focus on building human and institutional capacity of PNG CERT imparting relevant technical skills, tools as well as suggesting organisational structure ensuring effective operations."*

Chief Executive Officer Charles Punaha, *National Information & Communications Technology Authority of Papua New Guinea (NICTA) said that the government has given high priority for cybersecurity especially establishment of PNG CERT and enhance its capabilities to react, respond in coordinated manner to ensure safe and secure ICT access for people of Papua New Guinea.*

UN Resident Coordinator, Mr. Gianluca Rampolla *in Papua New Guinea: "The United Nations through our specialized agency on ICT is pleased to assist Papua New Guinea in ensuring secure and safe cyber culture for citizens by delivering specialized technical skills, simulation and tools engaging the government agencies, private sector, academia and other stakeholders because cybersecurity is the responsibility of everyone."*

OCSC Project Lead – CMM in the Pacific, Dr. James Boorman: "*The CMM review is an excellent opportunity for the Government of* Papua New Guinea *to benchmark its national cybersecurity capacity. The review results will enable the decision-makers to better plan investments in cybersecurity, set priorities for capacity-building initiatives, and support its ambition to enhance coordination and cooperation regarding cybersecurity in the region.*"

Contact person:

Name: Mr. Jackson Kariko

National Information & Communications Technology Authority of Papua New Guinea (NICTA)

Phone: +675 303 3240

Email: jkariko@nicta.gov.pg

About

ITU

ITU is the United Nations specialized agency for information and communication technologies – ICTs.

ITU allocates global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide. ITU is committed to connecting all the world's people – wherever they live and whatever their means. Through ITU's work, ITU protect and support everyone's fundamental right to communicate.

Oceania Cyber Security Centre

The Oceania Cyber Security Centre (OCSC) is a not-for-profit collaboration of 8 Victorian Universities with substantial support from the Victorian Government, Australia. The centre provides a 'front door' to collaborative opportunities with over 120 experts from a broad spectrum of disciplines in the cyber security field - from technical expertise through to strategy, policy and law. The broad aims of the centre include: engaging with industry to develop research and training opportunities for dealing with cyber security issues including Cyber Security capacity building in the Pacific region.

Global Cyber Security Capacity Centre

The Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford is a leading international centre for research on efficient and effective cybersecurity capacity-building, promoting an increase in the scale, pace, quality and impact of capacity-building initiatives across the world. It has developed the Cybersecurity Capacity Maturity Model for Nations (CMM) a first-of-its-kind model to assess cybersecurity capacity maturity across five dimensions, which aims to enable nations to self-assess, benchmark, better plan investments and national cybersecurity strategies, and set priorities for capacity development.