PRESS RELEASE

Government of Samoa

MINISTRY of COMMUNICATIONS & INFORMATION TECHNOLOGY

MEDIA BRIEFING ON

Making Internet a Safer Place for Samoa:

Establishing Computer Emergency Response Team and Assessing National Cybersecurity Capacity

Apia, Samoa

16-20 April 2018

The past twenty years has been an extraordinary time for the development of Information and Communication Technologies (ICTs) – and with the 'mobile miracle' we have brought the benefits of ICT's within reach of virtually all the world's people. But we believe that the next twenty years will be even more dramatic with 200 billion devices being connected through Internet of Things(IoT) 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 the risk of losing trust and confidence in our ability to communicate securely. Security is key to building the trust and confidence in the use of ICT for e-transactions. Cybersecurity continues to be a big challenge as we embark on the Internet of Things, 5G, Smart Cities, Over the Top (OTT), Machine Learning, Autonomous Vehicles, Cloud Computing 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.

Pacific Islands Countries are considerably aware of the issues and cyber threats. Some Countries have made efforts in building a National Computer Incident Response Team (CIRT). The International Telecommunication Union (ITU) (United Nations Specialised 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 and Vanuatu. Despite efforts from the Pacific Islands 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 quoted "As a specialized agency, 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 and in cooperation with partners APNIC, ITU carries out assessments of CIRTs for Samoa, Tonga, Vanuatu and PNG along with building human and institutional capacity to ensure trust and confidence in use of ICT".

Recognising the significance and further enhance socio and economic development, Ministry of Communications & Information Technology, Samoa under the technical collaboration of the ITU carries out a CERT/CIRT assessment and builds capacity of the stakeholders between 16-20 April. The major stakeholders, including Ministries, Corporations, Authorities, Banking & Finance Institutions, ICT Service Providers, Academia, Private Sector and Non-Government Organisations, have been invited to participate in the week-long sessions. There will be latest information sharing presentations from by ITU, APNIC and GCSCC/OCSC. The outcome would cover the following:

- Stronger coordination, collaboration and information sharing between CERTs and other relevant players;
- Readiness assessments for national CERT establishment for Samoa;
- Design and implementation plan for each national CERT;
- Stocktaking of activities being undertaken in the selected countries by national, regional, and international organisations, and in the region in general; and
- Awareness and hands-on training workshops aimed at building and strengthening human capacity in cybersecurity related matters in general and CERTs in particular.

Additionally, ITU is partnering with the Global Cyber Security Capacity Centre (GCSCC) from the University of Oxford on this mission. Together with its regional partner, the Oceania Cyber Security Centre, the GCSCC conducts an assessment of the National Cybersecurity capacity based on *the* Cybersecurity Capacity Maturity Model for Nations (CMM). The systematic 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 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.

The Honourable Afamasaga Lepuia'i Rico Tupa'i, Minister of Communications & Information Technology, Samoa said that the *"Government has given high priority for cybersecurity especially establishment of CERT in Samoa under the National Cybersecurity Strategy 2016-2021."* He further stated that *"C.E.R.T. will be a focal point for the collection of reports about cyber security incidents and cybercrime, and provide a safe and secure digital environment for Samoa and its citizens, through coordination and collaboration with stakeholders to detect and manage cyber threats at the national level."*

APNIC: *"Cybersecurity is a complex challenge that requires stakeholders from all sectors to work together. APNIC has been working closely with the Pacific community to help bolster cybersecurity incident response capacity in Tonga, Papua New Guinea, Vanuatu, and Fiji, and is looking forward to contributing to Samoa's efforts to build strong community cooperation for a successful new CERT."*

GCSCC: "*The CMM review is an excellent opportunity for the Government of Samoa 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.*"

OCSC: OCSC's Director Dr. Carsten Rudolph welcomed the high priority given to Cyber Security including establishment of CERT in Samoa and thanked Afioga Afamasaga Lepuia'i Rico Tupa'i, Minister of Communications & Information Technology, for the commitment. *"We are delighted to work with Samoan Government, GCSCC in deploying the CMM model."*

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.

The Global Cyber Security Capacity Centre (GCSCC) – University of Oxford

The Global Cyber Security Capacity Centre (GCSCC) 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 created a first-of-its-kind model to measure cybersecurity capacity maturity across five areas (or 'dimensions'), which aims to enable nations to self-assess, benchmark, better plan investments and national cybersecurity strategies, and set priorities for capacity development.

Oceania Cyber Security Centre

The OCSC is a collaboration of 8 Victorian Universities with substantial support from the Victorian Government, with the broad aim of engaging with industry to develop research and training opportunities for dealing with cyber security issues including Cyber Security capacity building in the Pacific region.

About APNIC

APNIC (Asia Pacific Network Information Centre) is an open, member-based, not-for-profit organization, whose primary role is to distribute and manage Internet number resources in the Asia Pacific region's 56 economies. These number resources – IP addresses and AS Numbers – are the building blocks for the Internet to operate and grow.

APNIC helps build essential technical skills across the region, supports Internet infrastructure development, produces insightful research, and is an active participant in the multistakeholder model of Internet cooperation and governance.

APNIC performs these activities as part of its commitment to a global, open, stable and secure Internet that serves the entire Asia Pacific region. www.apnic.net