National Information and Communications Technology Authority

Public Notice

Proposed PNG Cybercrime Policy

Like many other countries, PNG has recognised the social and economic benefits to be derived from Information and Communication Technologies (ICTs).

Properly utilised, ICTs can be a significant tool in our country's development, and the realisation of the National Goals and Directive Principles (NGPDs).

However, the use of ICTs also introduces correlative security concerns for individuals, businesses, and the public sector that need to be addressed. If not appropriately addressed, the threats posed by Cybercrime can potentially circumvent the country's socio-economic growth.

Malicious software that affects millions of electronic devices, systems and networks and causes significant damage are only examples of the much broader problem of Cybercrime.

This has generated intensive debate where various solutions have been discussed to address the issue of criminal abuse of electronic devices, systems and networks. Therefore to address this challenge a National Policy response is required.

Cybercrime and Cybersecurity

- Cybercrime refers to offences committed using electronic devices, systems and networks. Cybercrime can be divided into the following categories to be better understood:

  a) **Offences against the confidentiality, integrity and availability of electronic data, systems and networks** (this include *illegal access to electronic systems and networks, illegal remaining in an electronic system or network, illegal access to electronic data, illegal interception of electronic data, illegal data interference, illegal data acquisition, illegal system or network interference and illegal obstruction of use of electronic data);*
  b) **Content-related offences** (this include *child pornography, SPAM and harassment, utilising means of electronic communication*);
  c) **Copyright-related offences**; and
  d) **Other offences**, including *computer-related fraud or forgery, identity-related crime and misuse of devices*.

- Cybersecurity, on the other hand, refers to the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organisation and users' assets.

The Cybercrime Policy also seeks to provide a legal and regulatory framework to:

- Protect Papua New Guinea communities from cybercrime;
- Preserve our cultural and traditional values;
- Create a safer cyberenvironment for all users;
- Build confidence in electronic commerce;
- Ensure that PNG laws on Cybercrime are in harmony with other similar regional and international laws dealing with Cybercrime;
- Promote and enhance international cooperation in addressing and combating Cybercrimes;
- Enhance and strengthen PNG's law enforcement capacity in addressing and combating Cybercrime;
- Create and increase awareness, education and training in Cybercrime within PNG; and
- Ensure effective coordination and collaboration amongst all stakeholders, especially the law enforcement agencies.

The PNG Cybercrime Policy

The strategies envisaged under the Policy to address Cybercrime are:

a) The adoption of criminal laws against attacks on the security and integrity of computer systems and information, thereby criminalising hacking, illegal interception and interference with availability of computer systems.
b) To have clear procedures meeting international standards for government access to communications and stored data when required for criminal investigations. Such procedures will allow government to carry out their investigations, but will also assure businesses and consumers that there cannot be any justified monitoring of all types of communications.
c) To put in place procedures and laws facilitating the use of credits and electronic forms of payment, in a legal framework ensuring consumers and business proprietors who transact business on line have resources if the transaction does go through of if the product or services purchased are unsatisfactory. It will also ensure that consumer data provided to merchants will not be missed.
d) To review the existing intellectual property laws to ensure there is adequate protection in the digital setting.
e) To have procedures and processes in place to take all critical systems offline in the event of war, disaster or civil unrest, which otherwise could jeopardise or place such systems at risk.

Proposed Regulation for the Registration of SIM Cards

NICTA is the peak Government body for the regulation of ICT services in PNG. Specific provisions of the National ICT Act 2009 gives it the general powers to propose and or make industry guidelines, standards, codes of practices, rules and regulations.

The proposed Subscriber Identity Module or SIM Card Registration Regulation is one of a number of various other technical instruments NICTA is required to make for the ICT industry.

The proposed Regulation is currently been redrafted by the State Solicitor's Office to ensure, among other things; that there are no ambiguities or inconsistencies in the implementation and administrative processes involved. It would then be submitted to Cabinet for its consideration and endorsement before a formal recommendation is made to the Governor General to give effect to the Regulation.

Calls by certain sections of the community that the Cybercrime Policy and the SIM card registration Regulation are intended to police social media and to block criticism of government are unfounded and misguided. The registration of SIM cards is a common practice in many countries including Australia, Singapore and Fiji where it is used to also support public safety actions and to deter and trace the use of ICT services in the commission of crimes.

The process involved in the formulation of the SIM card registration proposal was transparent and in accordance with the provisions of the National ICT Act 2009, which also involved public consultation with key industry stakeholders.
There is still a lot of work to be done in collaboration with the mobile phone operators and government agencies before the Regulation becomes effective. NICTA will inform the general public during the approval and implementation stages of the proposal.

Primary Objectives of the Regulation

The proposed Regulation will provide a regulatory framework for the registration of all SIM Card users as well as for the control, administration, and management of the Information Database.

The mandatory SIM card registration is intended to:

- Help law enforcement agencies identify the mobile phone SIM card owners;
- Track criminals who use phones for illegal activities;
- Curb other negative incidents such as loss of phone through theft, nuisance/ hate text messages, fraud, threats and inciting violence; and
- Help service providers (network operators) know their customers better.

Charles S. Punaha
Chief Executive Officer