National Cybersecurity Policy
2020

Draft – Not Approved
March 2020

TABLE OF CONTENTS

FOREWORD BY THE MINISTER

Information and communication technology (***ICT***) is an integral part of public administration, global trade and social interaction in today's world. Major economic partners such as APEC are focusing on e-Trade and e-Commerce, as governments across the region set their agenda on implementing e-Government. The 2018 APEC theme which centred around "Harnessing Inclusive Opportunities, Embracing the Digital Future", is at the forefront of the Government's vision for socio-economic development in the country.

To support the Government's drive towards digital economy, current government policy encourages competition through the use and development of ICT. As a result, ICT activities in the country have increased significantly and have impacted immensely on society. However, the use of ICT poses risks to the security of electronic systems and infrastructure. These risks are appropriately addressed through the enhancement of Cybersecurity.

Consequently, Cybersecurity is a fundamental and integral component of ICT development. Cyber-related risks are evolving rapidly and as our country becomes increasingly reliant on ICT, it is of paramount importance that our technical and intelligence capabilities in Cybersecurity must also be developed to international standards and in accordance with international best practice in order to provide adequate protection for our critical infrastructure systems. When our critical infrastructure systems or essential services do not function properly, our Government, economy and society can be adversely affected.

Recent technological progress has for instance, enhanced the level of convenience with which we conduct our business and carry out daily tasks that previously required cumbersome physical attendances and manual processes. The internet of things (***IoT***) has simplified such processes as computers have now replaced most of these functions. We are now able to purchase electricity on mobile platforms, airplane tickets online and perform numerous tasks from the comfort of our homes.

To be prepared for the compounded risks associated with the increased dependence on the use of ICT, this National Policy Framework helps define how Cybersecurity-related activities should be organized and how roles and responsibilities should be shared among institutions. In particular, the Policy provides for the establishment of PNG's technical and intelligence capabilities and our collaboration with other governments and similar regional and international establishments, in our efforts to protect our critical infrastructure and systems.

Moreover, to manage cyber threats, appropriate laws and structures must be developed to address incident management. This Policy provides for relevant legislation, regulations and guidelines to be developed and the establishment of organisations to support Cybersecurity initiatives and enable the Government to assume the lead role in ensuring a safe and secure cyber environment.

The Policy is developed in accordance with guidelines from International Telecommunication Union (***ITU***) albeit tailored to suit our circumstances. The main focus is on establishing PNG's own national computer incidents response teams (***CIRTs***) and other capabilities at the national level to provide guidance and advisory support to government, industry and citizens. The Policy provides for capacity building within the Government for the protection of its information and infrastructure systems.

The successful implementation of this Policy hinges on effective coordination amongst the implementing agencies and sufficient and sustainable resourcing through Government and industry commitment. The onus is on the lead implementing agencies to develop appropriate strategies and advise the Government from time to time to commit necessary resources.

On this note, I acknowledge the support of the ITU, APNIC, CWG, and those who contributed through stakeholder consultation towards the development of this Policy. The Policy will be reviewed from time to time to ensure its objectives continue to be relevant and commensurate with the fast advancing pace of technological development.

HON. TIMOTHY MASIU, MP
Minister for Communications and Information.

ABBREVIATIONS

APEC	Asia Pacific Economic Cooperation
APNIC	Asia Pacific Network Information Centre
ASMS	Automated Spectrum Management System
CBD	Central Business Districts
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIRT	Computer Incidents Response Team
COPWG	Child Online Protection Working Group
CSIRT	Computer Security Incidents Response Team
CSOC	Cybersecurity Operations Centre
CWG	Cyber Working Group
DCI	Department of Communications and Information
DDOS	Distributed Denial of Service
DFA	Department of Foreign Affairs
DJAG	Department of Justice and Attorney General
GCA	Global Cybersecurity Agenda
ICT	Information and Communication Technology
IFMS	Integrated Financial Management System
IGIS	Integrated Government Information System
IoT	Internet of Things
ISO	International Standards Organisation
ITU	International Telecommunications Union
LNG	Liquefied Natural Gas
MDGs	Millennium Development Goals
NCPISC	National Cybersecurity Policy Implementation Steering Committee
NCSC	National Cybersecurity Centre
NCSAC	National Cybersecurity Strategic Advisory Committee

NICTA	National Information and Communications Technology Authority
NID	National Identification
NIO	National Intelligence Organisation
NISIT	National Institute of Standards and Industry Technology
NSAC	National Security Advisory Committee
NSA	National Security Agency
NSC	National Security Council
OCC	Office of Chief Censor
OSCA	Office of Security Coordination Authority
PNGCERT	Papua New Guinea Computer Emergency Response Team
PNGDF	Papua New Guinea Defence Force
PPP	Private Public Partnership
RPNGC	Royal Papua New Guinea Constabulary
SDGs	Sustainable Development Goals
UN	United Nations
UNGA	United Nations Global Agenda

PART I CYBERSECURITY ENVIRONMENT

1. BACKGROUND

1.1 Cybersecurity refers to the assortment of tools, policies, security concepts and safeguards, guidelines, risk management practices, activities, training, best practices, assurance and technologies that can be used to protect cyberspace, organisational and user's assets, including, interconnected electronic devices, personnel, infrastructure, applications, services, telecommunications systems, and the entire information transmitted and or stored in the cyber-environment.[1]

1.2 The Government of Papua New Guinea (***Government***) has defined key priorities with regard to the development of ICT in its 2008 National Information and Communication Technology Policy (***ICT Policy***). The ICT Policy paved the way for the liberalisation of the industry and caters for increased competition in the telecommunications sector.

[1] *A Definition of Cybersecurity – ITU http://www.itu.int*

1.3 The ICT Policy highlights the importance of building confidence and security in our ICT systems[2]. It underlines the need to protect fundamental rights of citizens as well as enables the investigation and prosecution of crimes. Cybercrime is one of the Security components mentioned in the ICT Policy[3]. In 2014, the Government introduced the National Cybercrime Policy (***Cybercrime Policy***) and subsequently in 2016, enacted the ***Cybercrime Code Act* 2016** (***Act***).

1.4 However, the ICT Policy does not limit security concerns to Cybercrime. It also highlighted that "*criminal law is only a small part of the cybersecurity framework*"[4]. The Government further elaborated that Government and Private Sector agencies need to cooperate in improving the security of their systems by applying sound security practices, improving and securing the sharing of information, and raising awareness.

1.5 ICT offers unique opportunities for the Government, businesses and people in PNG. Experiences with digitalization highlight the potential of ICT to stimulate the economy and strengthen the service sector. It can ease access to knowledge and play an important role in education both in the urban areas and rural areas of the country.

1.6 Moreover, ICT can help improve the efficiency and reliability of national critical infrastructure such as the supply of electricity, water and other government services. However, it is necessary to be mindful that the integration of ICT is inevitably associated with Cybersecurity risks; hence, requires risk assessment, risk management and countermeasures to minimise such threats, and mitigate loss in order to maximise the benefits. Whilst increased connectivity will support the development of the service sector, cyberattacks have the potential to indiscriminately harm both businesses and individual users.

1.7 As outlined in the ICT Policy, access to information is beneficial but it is important to be mindful that the same technology provides access to illegal and harmful content. Further, whilst ICT can support the operation of critical infrastructure, such essential services are susceptible to attacks remotely through the networks that connect them. This issue has been highlighted as a specific concern in the objectives of the ICT Policy.

1.8 In addition, Cybersecurity is identified as one of the pillars of PNG's National Security. The Government endorsed the National Security Policy 2013 (***Security Policy***) which identified potential threats to overall national security. Cybersecurity is among the priorities[5]. Whilst recognising the economic value of ICT and its development, the Security Policy also emphasises

---

[2] *National ICT Policy 2008* p.36

[3] *Ibid.*

[4] *Ibid*., p.38 *ff*

[5] *National Security Policy 2013*, "*Level Two Threats"*. p.44

the negative impacts of breaches to Cybersecurity particularly, of its potential to compromise national security for example, through attacks targeted at our critical infrastructure.

1.9 The Government of PNG, in support of the United Nations (***UN***) and other member States and governments around the world, strongly believes that the potential of ICT far outweighs the risks. The Government is supporting on-going activities to strengthen the use of ICT within the implementation of the ICT Policy by adopting this Policy to be referred to as the National Cybersecurity Policy (***Policy***).

1.10 This builds upon existing relevant policies namely, the ICT Policy, the Security Policy and the Cybercrime Policy. It sets out the Goals and Objectives for PNG in maximizing safety and security in relation to the use of ICT; reflects, among others, the aims of the Millennium Development Goals 2000-2015 (***MDGs***)[6] and the Sustainable Development Goals 2015 (***SDGs***)[7], the Medium Term Development Strategy 2018-2022 (***MTDS III***) , and draws upon the recommendations related to ICT arising from the Final Acts of the ITU Plenipotentiary Conference (*Busan, 2014*)[8] and the ITU Global Cybersecurity Agenda 2007 (***GCA***)[9].

1.11 The Policy has been developed with technical assistance from International Telecommunication Union (***ITU***). Discussions were initiated with national, regional and international experts to ensure a broad participation incorporating governmental, non-governmental and open stakeholder consultations.

2. THE PAPUA NEW GUINEA CONTEXT

2.1 In 2017, the Government through its relevant agencies, undertook a national survey (***Survey***) to assess the current state of Cybersecurity in the country. A request for the completion of an online survey was published in the print media inviting responses from all over the country. The Survey was made available online and also in printable PDF format.

[6] MDGs superseded by SDGS in 2015; Goal 8 Develop a Global Partnership for Development (Target 8F- in cooperation with the Private sector to make available the benefits of new Technologies especially ICT).

[7] SDGs Goal 17 - Strengthen the Means of Implementation and Revitalise the Global Partnership for Sustainable Development (Target 17.8 Strengthen the Science, Technology and Innovation Capacity for Least Developed Countries)

[8] The UNGA Resolution 57/239, on the Creation of a Global Culture of Cybersecurity

[9] The ITU Global Cybersecurity Agenda launched 17 May 2007 – an ITU framework for International Cooperation aimed at proposing solutions to enhance confidence and security in the Information Society.

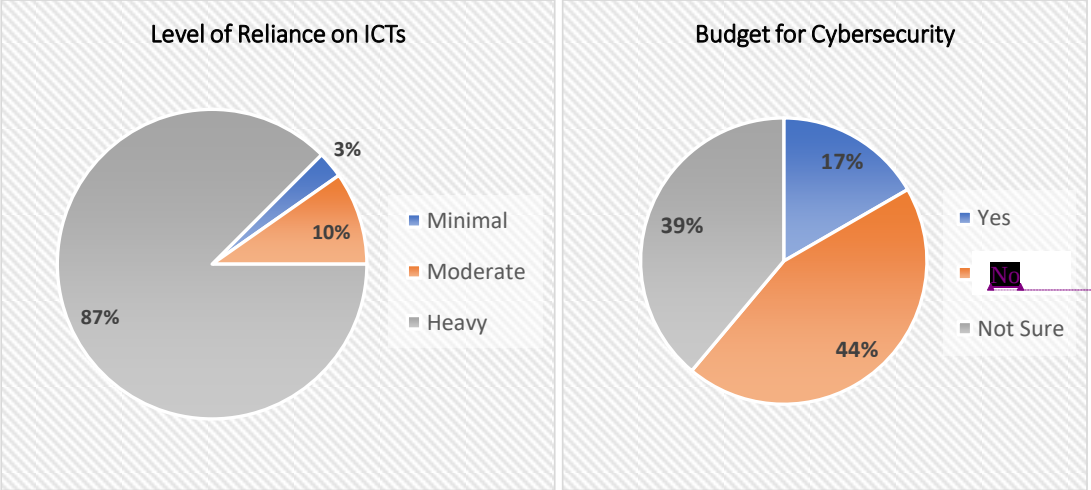
2.2 Responses were received from organisations in the public and private sectors, civil society, and individuals. Essentially, the Survey sought to establish the respondents' level of reliance on ICTs for personal use, work or business; and to assess whether or not measures are presently taken to counter Cybersecurity risks.

2.3 In terms of household internet usage, the Survey also covered Child Online Protection and the measures taken to safeguard children against cyber threats and abuse. Further, the respondents were required to provide an insight on their understanding of information sharing, privacy and data protection, and relevantly, available mechanisms for mutual legal assistance.

2.4 The Survey revealed that a vast majority of the total number of respondents (87%) relied heavily on ICT in their work or business. Many respondents claimed to have in place some sort of protective technical measures. However, in spite of this the results show a high indication of users experiencing some form of Cybersecurity concern (*Refer to full report on the survey,* ***Annexure "A"***).

2.5 At the same time, there is a high indication of a lack or absence of budgetary provisions for Cybersecurity both nationally and in various public and private sector organisations – *Refer to* **Figure 1**.

FIGURE 1 – Level of Reliance on ICT and Preparedness to Counter Cyber Threats and Attacks.

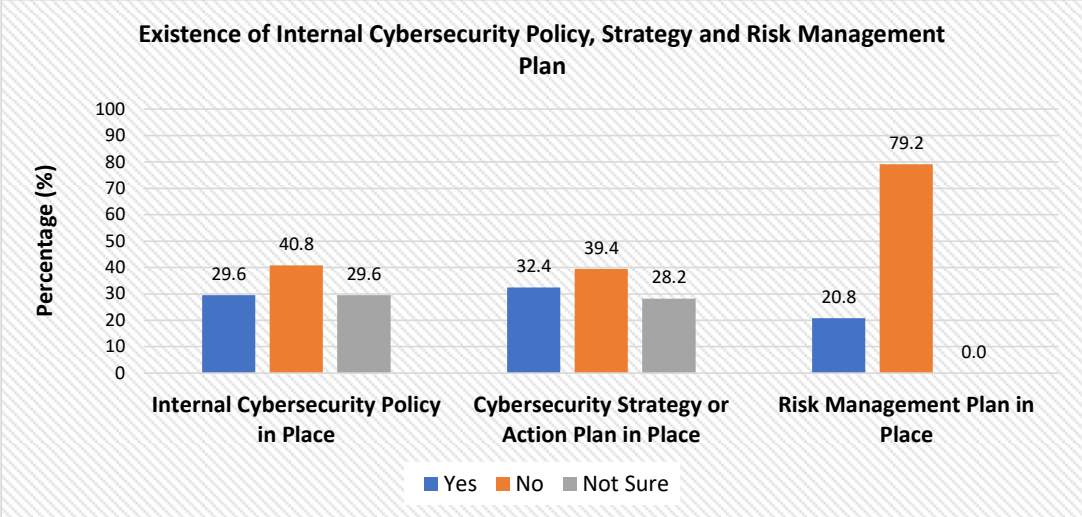


Formatted: Highlight

Formatted: Font color: Backgrou 2

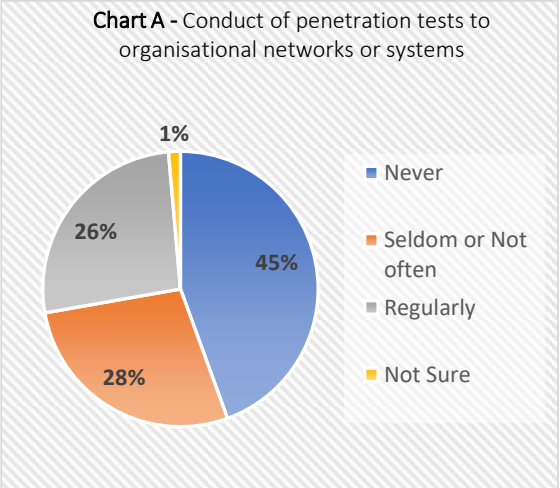
2.6 Generally, the responses highlight a marked inadequacy in terms of collective or coordinated efforts or measures for the prevention, detection, response to and or mitigation of Cybersecurity threats or attacks. At present, there is very minimal overall effort towards addressing Cybersecurity threats and attacks. The Survey revealed a significant lack of resilience in terms of policy, strategy and risk management plans – see **Figure 2**.

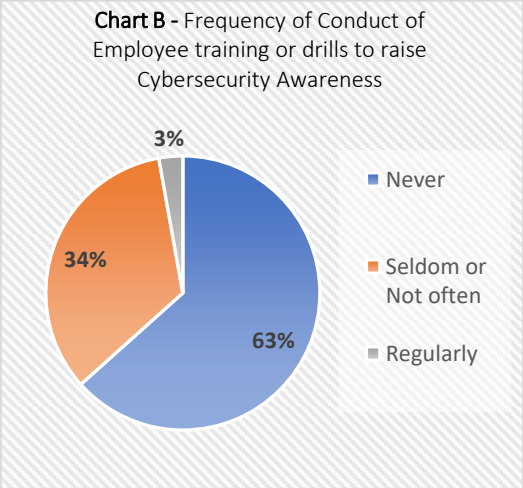
FIGURE 2 – Existence of Cybersecurity Policies, Strategies and Risk Management Plans and Overall Preparedness



2.7 In addition, the graphs in **Figure 3** show a general lack of awareness or preparedness. **Chart A** shows that about 45% of the respondents stated their organisation has never conducted penetration tests on their system(s) to determine the level of risk. Further, when queried if their organisations conducted employee training or drills to raise Cybersecurity awareness or determine their level of preparedness, 63% indicated that they had never conducted any such exercise.

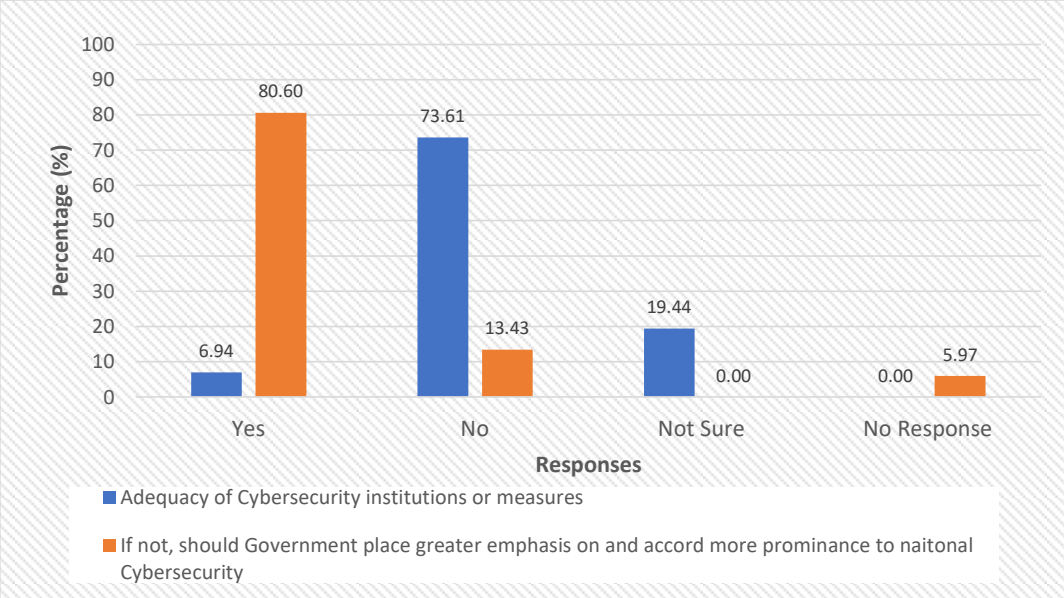
FIGURE 3 – Cybersecurity Preparedness and Awareness

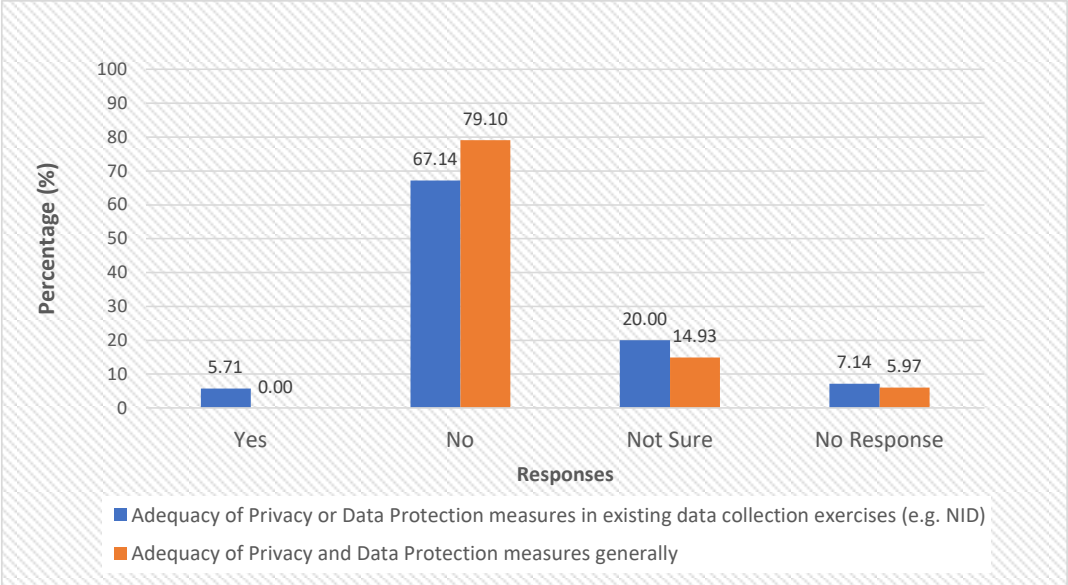




2.8 Moreover, the graphs in **Figure 4** confirm that there is overwhelming public support for Government intervention through the implementation of relevant policies, establishment of Cybersecurity institutions, raising of awareness, training and capacity building.

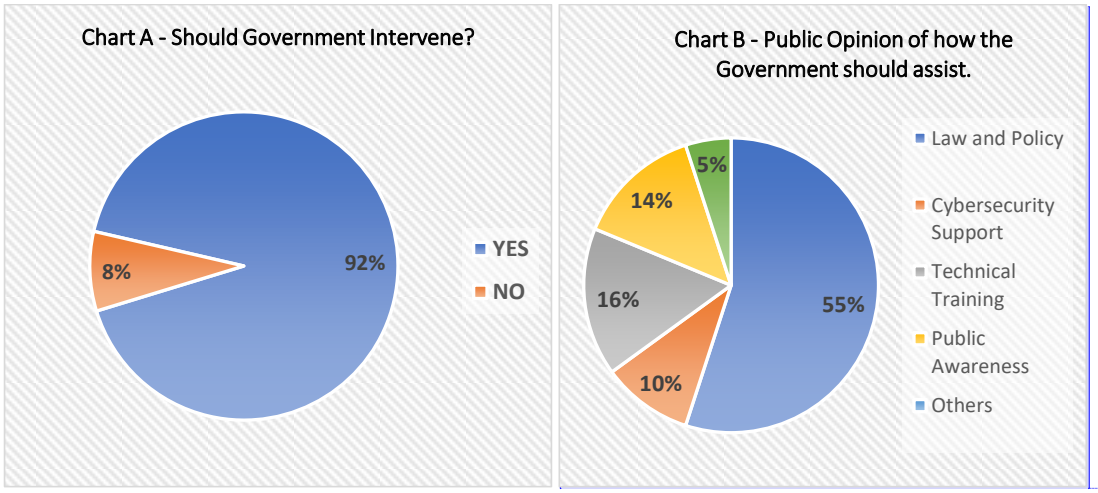
FIGURE 4 – Public Opinion of Adequacy of nationally available Cybersecurity Measures and the Need for Government Intervention





2.9 The results indicate that the majority of the respondents indicated the need for Government intervention. **Figure 5** illustrates that about ninety-two percent (92%) of those who answered the query were of the opinion that such intervention should include the formulation of policy and enabling legislation, technical training and public awareness.

FIGURE 5 – Public Opinion on Government Intervention



Comment [ZD1]: Change „Others to „No Response“ and correct colou coding.

3. VISION STATEMENT

3.1 The socio-economic development of PNG has become increasingly dependent on the use of ICT services and applications. The Government is therefore committed to ensuring that citizens, visitors, businesses and government agencies enjoy the full benefits of a safe, secure and resilient cyberspace.

3.2 In this regard the Government strongly believes that by enabling people to gain access to knowledge and information sharing whilst understanding and addressing the associated risks, it will be possible to secure more stable socio-economic development, and to protect essential democratic structures. This can be achieved through the implementation of this Policy in light of the ensuing Guiding Principles resulting in a better and trustworthy ICT environment.

4. POLICY GOALS

4.1 Cybersecurity threats are rapidly increasing and therefore, Cybersecurity remains a fundamental component of any digital or electronic infrastructure or system. The Government is mindful that attacks on its critical systems and essential services and those of the country at large, can adversely affect administration, economy and society, which is becoming increasingly reliant on interconnectivity.

4.2 Moreover, the Government is wary of the potentially negative impact of creating new institutional capacities with every policy formulation, and accordingly focuses on strengthening existing structures. However, the Government, in recognising the lack of a coordinative Cybersecurity institution or agency, has established the National Cybersecurity Centre (***NCSC***), and commends the establishment of PNGCERT through the Public Private Partnership (***PPP***) arrangement. In addition, it acknowledges the requirement of a national and or government CIRT. The recently established CSOC under the proposed NCSC will therefore be a fundamental priority and focus of this Policy.

4.3 A coordinated approach led by the Government is a key step towards Cybersecurity preparedness and resilience. In order to counter cyber threats and attacks, common standards and practices on Cybersecurity within Government, and guidelines to businesses are necessary. Appropriate and relevant legal and regulatory frameworks are also required to define and support common standards, practices and guidelines. Capable institutions with adequate capacity are also essential to lead and enhance Cybersecurity activities.

4.4 Accordingly, the following Goals are aimed at fostering a coordinated approach led by the Government to ensure Cybersecurity preparedness and resilience through:

- developing and strengthening legal and regulatory frameworks consistent with the highest regional and international standards in the larger field of Cybersecurity, incorporating legislation on the protection of critical infrastructure, privacy and data protection,

information sharing, e-Commerce, freedom of information or access to information, and child online protection and to enhance Cybersecurity of people living with disabilities; to complement the existing ***Cybercrime Code Act*** **2016**, whilst maintaining a balance between individual and collective security and preserving the right to privacy and other fundamental rights and freedoms of citizens;

- creating institutional capacities and strengthening existing structures as Cybersecurity coordinative institutions;

- developing and implementing technical measures, appropriate frameworks, standards and guidelines and enabling capacity to protect critical infrastructure systems and services against cyberattacks;
- providing businesses and citizens with access to basic services and actionable intelligence related to Cybersecurity;
- creating and increasing knowledge and awareness of Cybersecurity and ways to protect against cyber threats to Government, businesses and citizens, and providing basic tools and services as well as expertise to the highest standards;

- creating a secure ICT environment that enables constant exchange of information amongst stakeholders;

- strengthening the country's ability to participate in international cooperation arrangements in order to harness the global nature of Cybersecurity challenges, and

- implementing protective technical measures aimed at reducing online threats and create a safe cyber environment for children.

4.5 A national Cybersecurity Strategy will be developed to outline action plans towards implementing the Goals set out in this Policy. This Strategy will harmonise differing standards and practices in order to strengthen and enhance Cybersecurity within Government and provide guidance to businesses and the country as a whole. The Strategy will take into account national demands as well as international best practices, and will be kept in the custody of the Prime Minister's Office as head of the NSC under the auspices of the National Security Advisory Committee (***NSAC***).

5. GUIDING PRINCIPLES

5.1 The Government is aware that the ongoing implementation of the ICT Policy will have a major impact on connectivity within the country, particularly in rural areas. With the increase in bandwidth, new services will be available and some of these services will encapsulate Cybersecurity and related concerns. Consequently, the Government gives priority to a timely

implementation of this Policy, to ensure that Cybersecurity measures are implemented in parallel with the increase in services and connectivity, and the country's emerging prominence within the region.

5.2 This is consistent with the government endorsed *ICT Sector Roadmap 2018*[10] that identified "cyber safety" as one of its six (6) digital framework pillars to promote a safe and secure digital environment. ICT Sector Roadmap identifies Digital Safety, Digital Infrastrcuture and Digital Skills as prerequisites that will encourage the take-up of electronic services (Digital Services), provide PNG consumers and businesses with the necessary confidence to undertake transactions online (Digital Business), and ensure the Cybersecurity of critical ICT infrastructure and Digital Government in PNG.

5.3 The successful adoption of the ***Cybercrime Code Act* 2016** is acknowledged. However, as underlined in the Cybercrime Policy, the Act is only able to address criminal conduct. This Policy shall therefore, be supported by appropriate legislation and regulations. Regulations will primarily focus on technical minimum Cybersecurity standards.

5.4 The Policy will therefore be guided by the following principles:

- protecting citizens, visitors, businesses and government agencies and critical infrastructure by providing the necessary security frameworks, strategies and guidelines, building national capacity, implementing information sharing techniques and raising awareness;

- engaging all stakeholders nationally and internationally, in the implementation of this Policy consistent with the Public-Private Partnership policies of the Government;

- ensuring timely implementation of this Policy so that Cybersecurity measures are implemented commensurate with the increase in services and connectivity and the country's emerging prominence within the region;

- according equal attention to strengthening existing child protection legislation and introducing or adopting technical measures for Child Online Protection, and enacting legislation in areas such as privacy and data protection, critical infrastructure protection and e-Commerce;

- ensuring appropriate legislation and regulations focusing on technical minimum standards to support the implementation of this Policy; and

[10] The *ICT Sector Roadmap 2018*, endorsed through NEC Decision No. 289/2018

- taking into account in the implementation of this Policy, relevant national, regional and global best practices in building confidence and security in ICT by cultivating strong linkages with the applicable UNGA resolutions, as well as ITU recommendations.

6. ROLE OF GOVERNMENT IN CYBERSECURITY

The Government plays a significant role in the protection and enhancement of Cybersecurity in the country. It will:

- assume the lead role in coordinating nationally and internationally, efforts in addressing Cybersecurity threats;
- initiate the development of necessary frameworks;
- provide necessary resources including, funding, CIRTs, human resource training and capacity building, and necessary hardware and software infrastructure, to counter cyber threats;
- identify from time to time, and protect critical government assets and systems including the Integrated Government Information System (***IGIS***), NICTA's Automated Spectrum Management System (***ASMS***), Integrated Financial Management System (***IFMS***), NID System and other functions which are dependent upon or functional on electronic systems;
- raise awareness and education;
- facilitate victim welfare, where necessary, and
- generally initiate and facilitate activities to protect and enhance Cybersecurity in the country.

7. KEY ISSUES AND CHALLENGES

7.1 Cyber threats and attacks are rapidly evolving in form and level of sophistication. It is therefore important to ensure that people and businesses in PNG have access to regularly updated information about threats and vulnerabilities as well as best practices to manage and mitigate risks and prevent attacks.

7.2 Government will address the challenges by creating institutional capacities within the country to monitor developments and provide related services, guidance and information which, will be entrusted to respond to Cybersecurity threats and or incidents to raise awareness, disseminate information and provide relevant services for citizens, businesses and Government.

7.3 Government recognizes the global challenge of cyber threats. As underlined in the Cybercrime Policy, cyberattacks are largely transnational and offenders act with a great degree of sophistication and anonymity. In order to effectively deal with those threats, international cooperation is required. Government will address the challenges by bringing its institutional capacities as well as policy and legal frameworks in line with international best practices.

7.4 It is acknowledged that no government, whether in developing or highly developed countries, is capable of single-handedly protecting businesses and its citizens from all possible threats to Cybersecurity. The Government will address the challenge by initially defining focus areas for government action and will combine this with strong PPPs in order to encourage and empower businesses as well as citizens to take preventive measures.

7.5 The prevention of attacks, the detection of illegal activities as well as the recovery from breaches to Cybersecurity, require skilled experts. Currently, there are very few such experts in PNG and the demand for relevant expertise in both the private and public sectors is increasing. PNG will address the challenge by introducing and supporting programs to create and strengthen expertise within the country.

7.6 In order to respond to trends and new developments, the Government and the specialized institutions require up-to-date information about attacks both within the country and globally. PNG will address the challenges by developing a bi-directional reporting mechanism including, information sharing which is fundamental to effective Cybersecurity.

7.7 A Cybersecurity policy is vital as it provides a clear direction for the Government to deal with issues of Cybersecurity. This Policy ensures a collaborative and coordinated approach towards effectively addressing the national Cybersecurity agenda.

Part II FOCUS AREAS

8. DEVELOPMENT OF A NATIONAL CYBERSECURITY STRATEGY

8.1 A National Cybersecurity Strategy shall be developed. It should surpass policy statements and focus on concrete measures which should address the following issues: –

- responsibility within and between the Government and private sector, definition of processes, technical specifications and risk assessment, and emergency plans. The Strategy should clearly point out the roles and responsibilities of different institutions. This may include technical as well as management responsibilities.

- the Government's need to emphasises the maintenance of a sufficient crisis and incident management system as a key component of any Cyber defence strategy. Taking into account the potentially devastating impact of cyberattacks, clear rules and procedures are required to define the circumstances under which certain people and institutions need to take action.

- processes to define Cybersecurity-related requirements with regard to and in accordance with relevant government processes. This may range from mandatory training procedures for new staff to concrete security procedures for trans-border travel. In order to provide solution-oriented guidance, processes should be described as precisely as possible.

- processes to include and cover prevention, preparedness, detection, response and recovery.

- in addition, research and development plans to be addressed in the Strategy.
- defining clear, government as well as industry-wide technical specifications for Cybersecurity, such as minimum requirements with regard to the encryption of classified documents, to overcome conflicts caused by differing standards.

- the risk assessment and emergency plans to provide guidance with regard to the most likely threat scenarios.

8.2 The Strategy will be developed in a way that it allows for frequent updates wherever developments (either technical modifications or developments in the threat landscape) require review and adjustment. In addition, the Strategy will clearly point out links to, and interdependencies with the private sector.

8.3 A technical Cybersecurity working group known as the National Cybersecurity Strategic Advisory Committee (***NCSAC***) will be formed to drive the development of the Strategy. The NCSAC will be comprised of the following structure: -

xx, Chairperson, NICTA
xx, Deputy Chairperson, DCI
xx, Member, OSCA
xx, Member, DJAG
xx, Member, CLRC
xx, Member, NIO
xx, Member, RPNGC
xx, Member, PNGDF

Representative, Private Sector Member
Representative, Civil Society Member

8.4 With regards to classified components, the NCSAC should be limited to members with adequate security clearance.

8.5 The NCSAC will be responsible, among others, for the coordination and prioritization of Cybersecurity research and development activities focusing on building and strengthening a local Cybersecurity research community. Furthermore, it will identify minimum requirements and qualifications for information security professionals that will serve as a basis for the development of a related curriculum.

8.6 The Government is concerned about the use of unprotected private e-mail accounts used to send or receive Government work-related communications. Such communications are in general unencrypted, not secure and are beyond the control of the relevant national authorities. NCSAC will assess for the purposes of Cybersecurity, readiness of the central Government network known as the Integrated Government Information System (***IGIS***), and if necessary, suggest amendments. NCSAC shall determine a deadline as of which all Government communication must be carried out through the IGIS, and the use of private e-mail accounts for Government work related e-mail will be prohibited.

9. STRENGTHENING THE LEGAL AND REGULATORY FRAMEWORK

9.1 Legislation

9.1.1 The NCSAC will, in collaboration with the NCSC and relevant stakeholders, carry out a review of any existing legislation related to Cybersecurity.

9.1.2 This shall include a review and or if need be, enactment of legislation and regulations governing Cybersecurity including, protection of critical infrastructure, privacy and data protection (information security), National Security (***PM & NEC Act***, *Internal Security Act*, *NIO Act*) and Child Online Protection (***COP***).

(i) Cybercrime

9.1.3 The Government enacted legislation addressing Cybercrime in 2016. The NCSAC, in collaboration with the NCSC and other relevant stakeholders, organise and conduct training activities to assist with the implementation of the ***Cybercrime Code Act* 2016**.

(ii) Information Security - Privacy and Data Protection

9.1.4 The increase in reliance on the Internet and the use of electronic commerce in trade and commercial activities inevitably prompts the need not only for relevant legislation governing electronic transactions, e-Trade and e-Commerce, information sharing, access to information and

or freedom of information but more relevantly, the enactment of laws pertaining to the overall security of information including, privacy and the protection of personal data.

9.1.5 The NCSAC will, in collaboration with relevant stakeholders, oversee the development of various legislation as necessary to boost citizens' Cybersecurity when participating in the above activities which involve the unwitting sharing and transfer of data and information.

(iii) Protection of Critical Infrastructure

9.1.6 The Government has a responsibility to protect essential critical infrastructure against cyber threats. There will be legislation specifically ensuring a clear set of regulatory guidelines relevant to the protection of critical infrastructure. The NCSAC will consult with relevant stakeholders to ensure this is formulated for implementation.

(iv) Consequential Amendments

9.1.7 In addition, existing legislation relating to National Security, International Cooperation and Mutual Assistance, and People Living with Disabilities (***PLWD***) will be relevantly reviewed and updated where necessary.

(a) Laws Affecting National Security in General

- *PM & NEC Act*
- *National Intelligence Organisation Act*
- *Internal Security Act*

(b) Laws relating to COP

- *Lukautim Pikinini Act*
- *Censorship Act*

9.1.8 The review shall include the identification of existing provisions that could be utilized in relation to Cybersecurity, a comparison with international best practices, a gap analysis, suggestions for amendments and the related drafting instructions.

9.1.9 The NCSAC, in collaboration with the NCSC and relevant stakeholders shall seek the assistance of international organizations active in this field to carry out the assessment and comparative analysis.

Formatted: Indent: Left: 0 cm, First line: 0 cm

10. TECHNICAL AND PROCEDURAL MEASURES

Comment [ZD2]: KA to insert fro existing clauses..

10.1 Vulnerabilities of software applications

10.1.1 The NCSC shall leverage the experience of the software and hardware security industry to address the challenges related to standardising methods of accreditation for software applications in order to reduce their vulnerabilities and make it safer for access to information society.

10.1.2 The NCSC through CSOC, in collaboration with its public and private sector counterparts, shall develop and implement an evaluation or certification program for Cybersecurity services, products and systems.

10.1.3 The NCSC through the CSOC shall jointly together with its private sector counterpart(s)and National Institute of Standards and Industry Technology (***NISIT***), create the necessary infrastructure for conformity assessment and certification of compliance with Cybersecurity best practices, standards and guidelines (e.g. ***ISO 27001***).

11. STRENGTHENING THE NECESSARY ORGANIZATIONAL STRUCTURES

11.1 Establishment of a National Cybersecurity Centre (*NCSC*)

11.1.1 A national focal centre responsible for overall Government Cybersecurity will be established. The National Cybersecurity Centre (***NCSC***) will be commissioned under the joint auspices of the following departments:

(i) Department of Prime Minister & National Executive Council,
(ii) Department of Communications and Information (***DCI***),
(iii) Department of Defence,
(iv) Department of Police,
(v) Department of Justice and Attorney General (***DJAG***) and
(vi) Department of Foreign Affairs,

11.1.2 The core functions of the NCSC will initially include: -

- development of necessary frameworks;
- awareness activities for the prevention of and management of Cybersecurity risks;
- collecting of pertinent data reporting on the nature and extent of threats to Cybersecurity;
- encouraging reports of Cybersecurity incidents;
- monitoring, detecting, analysing and investigating or responding to threats to Cybersecurity;
- coordinating national Cybersecurity operations and capability;
- the lead Government agency for operational response to cyber incidents and
- facilitation of capacity building of Cybersecurity personnel and infrastructure.

11.1.3 The NCSC will be tasked with the underlying purpose of: -

- creating and nurturing mutual coordination of all government Cybersecurity capabilities;
- fostering enhanced collaboration and information sharing amongst Government and state agencies and critical infrastructure providers, and
- promoting collaboration and cooperation between the public and private sectors, foreign governments and international partners;

with the common view of combatting the ever-increasing threats to Cybersecurity.

11.1.4 The CSOC which will be established under the NCSC and will function as the CIRT for all government departments, state agencies and other government or public institutions.

11.2 Establishment of a Cybersecurity Operations Centre (*CSOC*)

11.2.1 The Government will establish a Cybersecurity operational centre or CSOC which will be responsible for providing Cybersecurity support predominantly to the public sector, including the Government, State Owned Enterprises, law enforcement and government institutions and agencies. CSOC will be the operational arm and of the NCSC. CSOC's operations, consistent with international best practices, will focus on:

- promoting Cybersecurity;
- providing support in the prevention, detection and response to Cyberattacks upon request;
- maintaining 24/7 points of contact;
- coordinating and collaborating with domestic partners and international counterparts;
- auditing and providing special support to critical infrastructure providers.
- carrying out digital forensic investigations;
- receiving and distributing reports about incidents,
- advocating capacity building through the introduction of best practices and measures in the promotion of Cybersecurity, and
- awareness raising and dissemination of information regarding threats and emerging trends.

11.2.2 CSOC will also upon request, assist or work in collaboration with PNGCERT in providing Cybersecurity assistance to the country as a whole.

11.3 Establishment of a National CIRT - PNGCERT

11.3.1 The Government will facilitate the establishment of a national CIRT. PNGCERT will act as the national point of contact to register computer incidents, raise awareness on global incidents with international agencies and advocate capacity building of best practices in cyber and computer security for its constituency.

11.3.2 The PNGCERT constituency covers all users of the internet ecosystem in the country, including individuals, service providers, enterprises and government agencies**.**

11.3.3 PNGCERT will be financed through PPP arrangement.

11.4 Establishing the Office of the Information Commissioner

The Office of the Information Commissioner will be established to:

(i) handle complaints for breach of data protection including, breaches that may occur during administraion of the right to access to information, and

(ii) to ensure access to public information.[11]

11.5 Creating a Secure Cyber Environment

11.5.1 While the Government is committed to protecting businesses and the people in PNG from threats related to Cybersecurity, it emphasizes the importance of self-protection and underlines the responsibility of the individual. The Government will support self-protection by providing knowledge through the NCSC and CSOC in collaboration with other CIRTs including, PNGCERT.

11.5.2 Each government institution and business in PNG that utilizes ICT is encouraged to: -

(i) undertake an individual risk assessment;
(ii) develop and implement a Cybersecurity policy and or strategy that addresses the main risks;
(iii) designate a member of senior management as Chief Information Security Officer responsible for Cybersecurity efforts and initiatives;

[11] A separate Policy will be developed to address the right to access public information.

(iv) maintain state-of-the art Cybersecurity technology that reflects its risk landscape;

(v) implement risk assessment and risk management processes;

(vi) have business continuity management and crisis management plans in place, and

(vii) carry out regular Cybersecurity drills.

11.5.3 The CSOC will collaborate with its private sector counterpart(s) and PNGCERT to undertake the following:

(i) develop a standard risk assessment framework for businesses in PNG and businesses are encouraged to utilize this framework;

(ii) develop and implement an evaluation or certification program for Cybersecurity services, products and systems, and

(iii) develop and implement technical and organisational protection measures as well as emergency plans to protect essential government services.

11.5.5 The CSOC in collaboration with its public and private sector counterparts shall develop and implement technical and organizational protection measures as well as emergency plans to protect essential government services.

11.5.6 The NCSC through CSOC and its public and private sector counterparts, shall promote, guide and coordinate activities aimed at improving Cybersecurity measures by strengthening the national capacity to investigate, combat and prosecute any cyber threat using the intelligence collected.

11.5.7 The NCSC through the CSOC, and in collaboration with its private sector counterpart(s) will identify all existing government and non-government institutions that are currently active in the field of Cybersecurity and draft a report about the mandate, resources and experiences, and analysis of potential areas for synergy, overlapping and gaps.

11.5.8 Through the PPP approach, the NCSC will collaborate with its private sector counterparts to identify local contact points outside of the Central Business Districts that can facilitate the collection of input about recent developments as well as disseminate information to the Constituents.

11.5.9 The CSOC will collaborate with its private sector counterparts to carry out a coordinated survey and assessment to analyse how far their constituents - citizens, businesses and Government - are affected by Cybersecurity incidents.

11.5.10 The CSOC will, on a voluntary basis or upon request, provide to its constituents including, stakeholders, government departments and state agencies, government institutions, and law enforcement, the following support:

(i) information and training material relating to Cybersecurity;

(ii) cooperation with national institutions that already provide relevant or related services and participation in nationally available initiatives, and sharing of material and information on a non-commercial level and evaluating the possibility of building upon existing facilities rather than developing new resources and material;

(iii) assisting with policy development relating to the planning and management of information security, and

(iv) facilitating and administering regular Cybersecurity drills in order to assess the level of emergency preparedness in combating and dealing with incidents.

11.5.11 In addition, the CSOC will upon request, provide its constituents with information about Cybersecurity. They will maintain resources to handle requests, promote the adoption of global best practices in Cybersecurity and compliance, provide training material and practical information as well as refer to publically available tools. In addition, they will provide on-the-ground advisory support to critical infrastructure providers and law enforcement agencies.

11.5.12 The CSOC may request the assistance of its private sector counterparts in the planning and management of information security and Cybersecurity generally, including, policy making.

12. CAPACITY BUILDING

12.1 The NCSAC and shall collaborate with the relevant stakeholders to identify capacity building programs related to Cybersecurity that businesses and citizens can benefit from. To avoid duplication, a roadmap shall be developed outlining the different capacity building activities that the country requires or may require at any given time, identifying potential programs, and making suggestions as to which activities should be covered under the respective programs.

12.2 The Department of Education (***DOE***) will collaborate with the NCSAC and NCSC, as well as other relevant authorities to develop a curriculum to ensure that all students at primary school and secondary school level receive at least once a year, updated training on Cybersecurity that includes information about latest trends. Training materials, background information for teachers and sample presentations shall be developed. In addition, schools should receive a questionnaire to enable them to assess the use of ICT services by students as well as child-specific Cybersecurity

risks. The anonymous assessment shall be carried out on an annual basis and the results submitted to the NCSAC and the NCSC and included in their annual reports.

12.3 The Department of Higher Education Research Science and Technology (***DHERST***) and the universities will in collaboration with the NCSAC and NCSC, as well as other relevant authorities, develop a curriculum for specialized training courses for Cybersecurity professionals. This is aimed at developing an adequate number of security professionals trained to handle Cybersecurity-related issues in PNG.

12.4 The NCSAC and NCSC shall in collaboration with relevant stakeholders develop a sustainable Cybercrime training program for law enforcement officers, Financial Investigation Unit (***FIU***), the judiciary and other relevant stakeholders.

13. INTERNATIONAL COOPERATION

13.1 To ensure that PNG's legal framework and practice in respect of international cooperation is on par with international best practices, the NCSC in collaboration with the Department of Justice & Attorney General and the Department of Foreign Affairs and the Royal PNG Constabulary; will analyse the country's capacity to efficiently submit requests for mutual legal assistance, as well as timely responses to requests submitted to authorities in the country.

13.2 The NCSC will in collaboration with relevant national and international entities, develop recommendations for the establishment of a single point of contact. Furthermore, the NCSC, will collaborate with PNGCERT and other counterparts to analyse if the technology used for sending and receiving requests as well as the availability of the contact point are in line with international best practices.

13.3 The NCSC will in collaboration with relevant government agencies including, DJAG and DFA and other relevant national and international entities, make recommendations with regard to a potential access to regional or international agreements, current processes of developing binding standards where PNG should participate, as well as 24/7 networks including the Interpol Network.

13.4 In determining access to existing instruments that are relevant for PNG, compliance with legal standards and conformity with cultural specifics as well as the usefulness of cooperation with other countries, shall be taken into consideration. The NCSC will seek membership of regional and global CIRTs as required.

13.5 The NCSC will collaborate with relevant stakeholders to jointly carry out Global Cybersecurity Index[12] exercise to foster the culture of Cybersecurity and build confidence and security in the use of ICT in line with ITU Standards[13].

14. CHILD ONLINE PROTECTION

14.1 A Child Online Protection Working Group (***COPWG***) will be formed with the following structure:

xx, Chairperson, Office for Child and Family Services
xx, Member, Department of Community Welfare, Youth & Religion
xx, Member, Office of Censorship
xx, Member, Office of the State Solicitor
xx, Member, Department of Education
xx, Member, Department of Communication Information & Energy
xx, National Information and Communication Technology Authority
xx, Member, NCSC
xx, Member, RPNGC

Representative Private Sector, Member
Representatives Civil Society, Member

Formatted: Indent: Hanging: 0.2 cm

14.2 COPWG will identify aspects of child online protection that need to be integrated including, technical protection measures, curriculums for schools and information material for parents and guardians.

14.3 The COPWG, in collaboration with internet service providers, shall evaluate different technical measures and parameters that service providers can introduce to assist with the protection of children online. Based upon the evaluation, the COPWG will develop guidelines for technical child online protection measures. The guidelines will be submitted to parents or guardians upon request, and will include recommendations for measures on how to prevent an abuse of the service.

14.4 Based upon the guidelines developed by the COPWG, internet service providers in PNG should be able to provide, upon the request of the user, technical measures intended to block content that is or may not be appropriate for children. Further, the provider should be able to provide, upon the request of the user, a special report for parents or guardians that highlights the services used and other parameters defined by the COPWG.

[12] .....

[13] .....

14.5 Based upon the guidelines developed by the COPWG, each provider of mobile communication services in PNG should be able to develop processes and procedures to manage online child sexual abuse.

15. INFORMATION EXCHANGE

15.1 Citizens, businesses and government agencies shall be encouraged to report cyber incidents to the relevant CIRTs, and the providers of critical national infrastructure shall also be obliged to submit such reports.

15.2 To support the idea of information sharing, the NCSC and PNGCERT shall develop routines to: –

(a) detect recent trends in relation to Cybersecurity incidents,
(b) create an emergency levels system,
(c) summarize incidents in a reporting format and provide background information,
(d) develop a network to communicate such reports through the relevant communication channels (e.g. press releases, information submitted to cooperation partners in rural areas) and submit this information. This shall include the regular publication of relevant, non-confidential information.

15.3 Once a year, the CSOC, PNGCERT and other CIRTs shall submit to NCSC a summary report on their work, and notifications received. They will provide the Government through NCSC with regular briefings and provide additional information upon request.

15.4 The CSOC, PNGCERT and other CIRTs shall ensure that the information submitted to the different stakeholders reflect their needs with regard to details including, an executive summary for relevant Ministers and detailed information for system administrators on the technical aspects of an attack; which information shall not be distributed to recipients that are not affected.

15.5 The NCSC and PNGCERT shall forward reports of incidents that have a potentially criminal background to the responsible law enforcement agencies. Law enforcement should create a single point of contact and ensure that the secure infrastructure provided by the NCSC and or PNGCERT is utilized. The Government will form an appropriate institutional structure within the law enforcement agency to handle cases of criminal nature which are reported by the NCSC and PNGCERT.

15.6 In order to facilitate the exchange of sensitive and confidential information between the NCSC and or PNGCERT and others, the NCSC and PNGCERT shall set up a system of secure infrastructure.

Communications, information collection and reporting shall, as much as possible, exclusively take place through such infrastructure.

15.7 The Government recognizes the advantages of mobile communication. The NCSC and PNGCERT will enable the submission of reports from mobile devices and explore the possibility of push services and mobile applications software to submit information about recent attacks on citizens and businesses.

16. PROTECTION OF CRITICAL INFRASTRUCTURE

16.1 Definition

16.1.1 Critical infrastructure refers to interconnected information and communication infrastructures which are essential for the maintenance of vital societal functions (health, security, safety, economic or social well-being of people) – the disruption or destruction of which would have serious consequences.

16.1.2 The Government defines Critical Infrastructure (***CI***) as the essential assets and services that underpin PNG's society and serve as a backbone of its economy, security and health. CI covers but is not limited to:

(i) Healthcare and Public Health,
(ii) Energy in general,
(iii) Water and Sewage,
(iv) Extractive Industry,
(v) Transportation,
(vi) Information and Communication Technology,
(vii) Food and Agriculture,
(viii) Financial Services,
(ix) Government Facilities,
(x) Education,
(xi) Emergency Services,
(xii) Law Enforcement and Judiciary,
(xiii) Defence Forces – Land, Sea and Air Elements and
(xiv) Critical Manufacturing[14].

16.1.3 In determining the list of CI providers, international best practices will be considered with regard to the definition and determination of infrastructure and assets that will be categorised as CI.

[14] This includes processing of consumable items e.g. food and beverages

16.2 Critical Infrastructure

16.2.1 The NCSC will oversee and manage activities relating to the protection of CI in collaboration with other key Cybersecurity institutions. It will, among others, undertake the following: -

- Facilitate consultation with relevant stakeholders from time to time to determine which assets and or infrastructure providers in PNG will be considered as CI.

- notify and provide to the National Executive Council (***NEC***) through the National Cybersecurity Policy Implementation Steering Committee (***NCPISC***)[15], with a list of CI assets and or providers in the country.

- create an initial database of CI assets and or providers and update the database as and when necessary;

- maintain the database to capture information about the size and relevance of the CI asset or provider including, the number of households using their service, an overview of the ICTs utilized and the relevance for core services, a risk self-assessment, an overview of countermeasures - technical and risk management - and a list of previous incidents.

- obtain required data from providers of CI, who will be obliged to provide the required data;

- may request information about the purpose and scope of security standards as well as practical methods for satisfying security standards

- collaborate with the NCSAC at least once a year to submit a questionnaire to the providers of CI to update …..

16.2.2 The NCSC and the NCSAC, in collaboration with PNGCERT and other private sector CIRTs, shall develop a national contingency plan and organise regular exercises for large scale network security incidents response and disaster recovery. Those exercises shall include latest trends and developments to allow CI providers to prepare for Cybersecurity attacks, cover technical components and risk management.

16.2.3 The NCSAC and the NCSC in collaboration with PNGCERT, shall regularly review policies and legislation related to cyberattacks against CI assets and or providers as well as the national risk management process.

Comment [ZD3]: Should we char tthis to "will" instead?

Comment [ZD4]: Both statements can be merged. Repetition here.

Comment [KA5]: Specific policie and legislation in relation to Critica Infrastructure or in general?

15

16.3 Critical Information Infrastructure

16.3.1 The Government is committed to strengthening the protection of CI and particularly critical information infrastructure (***CII***) providers, with regard to cyber threats. This shall include owners of CI as well as operators of services using CI/CII.

16.3.2 The Government recognizes that with an increase in the use of ICT by the citizens, the dependency on the availability of information infrastructure increases. Significant parts of information infrastructure today can be considered as CII since a failure or limited operation would cause detrimental impact on the vast majority of citizens.

16.3.3 Concerns related to possible attacks against CI are not limited to CII. Various CI providers that do not focus on information infrastructure, such as electricity and transportation providers, intensively use ICT. Therefore, substantial impact does not only refer to direct damage but also indirect damages.

16.3.4 With this Policy the Government lays the foundation to increase the ability of networks and information systems operated or utilized by CI assets and or providers to resist at a given level of confidence, accidents or malicious actions that may compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, or the related services offered by or accessible via that network and information system.

16.3.5 To ensure that the implementation of any mandatory standards is based upon the needs as well as capacities of the affected operators of CI and CII, the Government through the NCSC will:

- carry out a needs and risk assessment, focusing on CI providers including, small to medium enterprises as well as large enterprises and public and private operators.

- through relevant agencies, promote a nationwide as well as a regional debate, involving all relevant public and private stakeholders, to define priorities for the long term resilience and stability of CI and CII against cyberattacks.

- collaborate with the NCSAC and PNGCERT to carry out information exchange, prevention and early warning, detection with a focus on promoting security, reaction; and crisis management including mitigation of loss and recovery.

16.4 Funding

16.4.1 The Government is aware/mindful/acknowledges that effective implementation of a Cybersecurity Policy and Strategy is significantly dependent on adequate funding availability.

Comment [b6]: This sub-section talks about **information infrastructure**. Policy needs to def and distinguish information infrastructure from critical infrastructure

Comment [ZD7]: Which is I, CI o CII?

16.4.2 The NCSC, NCSAC and PNGCERT will be provided with the necessary funding through the PPP arrangement to maintain adequate technical, financial and human resources to carry out effectively and efficiently the tasks assigned to them to fulfil the objectives of this Policy.

16.5 Role of Government

16.5.1 The Government acknowledges its significant responsibility in the facilitation, coordination and enhancement of Cybersecurity….

16.5.2 The Government will coordinate and facilitate an effective PPP arrangement to ensure collaborative efforts are implemented to achieve the outcomes envisaged in the Policy and emanating Strategy.

Comment [b8]: Need clarification on **workable avenue**
Refer/references to ***PPP Act* 2018**

16.5.3 The Government will ensure that the NCSC has all the powers necessary to investigate cases of non-compliance by CI providers with their obligations and the effects thereof on the security of their systems with regard to cyberattacks. It will especially ensure that the NCSC has the power to require CI providers to furnish information needed to assess the security of their networks and information systems, including documented security policies, and carry out a security audit. In this regard, the Government will ensure that the institution has the power to issue binding instructions to CI providers. The Government will ensure that any obligations imposed on CI and CII providers under this Policy may be subject to judicial review.

16.5.4 The Government will, through the NCSAC, request the NCSC and PNGCERT and or other private sector CIRTs to contribute information on CI related issues to the development of technical Cybersecurity guidelines. These guidelines should include CII elements. In addition, it should maintain an incident management system as well as the necessary technical and human resources to support CI providers in dealing with cyber incidents. The purpose of this support is not to substitute the required resources on the part of the CI providers but to provide additional support.

16.5.5 In collaboration with the PNGCERT and other relevant counterparts, the NCSC will provide guidelines, promote good security and, manage and monitor progress. It will also provide a complete set of processes to ensure preparedness, prevention, protection, response and recovery from natural and malicious threats. It will introduce a certification system for providers of CI and will carry out a related feasibility study.

16.6 Obligation of Critical Infrastructure Providers

16.6.1 The providers of critical infrastructure are required to take appropriate technical and organisational measures to manage the risks posed to the security of their networks and information systems which they control and use in their operations. Having regard to the status

quo, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide. This is to ensure the continuity of the services underpinned by those networks and information systems.

16.6.2 To coordinate the activities, the providers of CI will appoint a member of senior management as Chief Information Security Officer (***CISO***) and ensure that it allocates a specific budget for implementing Cybersecurity measures. Based on the local requirements, capital turnover, total number of employees and total number of customers, the NCSC, in collaboration with PNGCERT, will assess and suggest the creation and installation of organizational CIRTs in those organizations providing CI.

16.6.3 CI providers will be required to cooperate and exchange information with the NCSC, PNGCERT and other private sector CIRTs. Furthermore, the providers of CI will be obligated to carry out a risk and exposure self-assessment at least once a year and document this process. In addition to national exercises, they should at least once a year carry out realistic exercises that simulate realistic attack scenarios and allow the providers to verify that technical measures in place are adequate, and risk management processes are based on international best practice.

Comment [KA9]: Should be mov to section of 'Information Sharing"

16.6.4 CI providers will be required to comply with mandatory minimum security standards which will be introduced/imposed based upon an analysis of the assessment referred to in the preceding sub-clause. In determining mandatory minimum standards, the speed of technological development, different capacities of small and large size providers, and the required update of any concrete standards will be considered.

16.7 Information Sharing

16.7.1 Information sharing plays a key role in Cybersecurity and forms an essential component of effective response to cyber threats.

16.7.2 The NCSC, will collaborate with PNGCERT and other private sector CIRTs and collect relevant information in order to get a more accurate understanding of the exposure of CI to cyberattacks. The NCSC and PNGCERT will be responsible for furnishing the providers of CI as well as the Government departments and agencies with required information on the status of readiness, incidents, trends and developments.

16.7.3 The Government will require the NCSC to establish a national forum to share information and good policy practices on security and resilience of Cybersecurity in relation to CI. This forum shall include CI providers, CII providers, government institutions, law enforcement agencies, civil society and other interested parties. The NCSC, in collaboration with PNGCERT and other private sector CIRTs, should in addition, take action to foster the cooperation between the public and

the private sector on security and resilience objectives, baseline requirements, good policy practices and measures.

16.7.4 The NCSC, in collaboration with PNGCERT should explore possibilities to foster innovation through public-private research and development projects focused on the improvement of Cybersecurity of CI. In addition, it shall develop and implement an awareness raising strategy to reach out to CI providers within the country.

16.7.5 In order to ensure that the NCSC and PNGCERT and other private sector CIRTs have access to up-to-date information about on-going developments within the country, CI providers are obliged to notify the NCSC and PNGCERT or other relevant private sector CIRTs as the case may be, through the secure infrastructure, of any incidents in relation to ICT that has a significant impact on the security of the core services they provide. In this regard, the NCSC and PNGCERT may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which CI providers are required to notify incidents.

Comment [KA10]: Could be repletion from other previous statements. Already reflected in 13.

16.7.6 The NCSC in collaboration with PNGCERT and other relevant stakeholders shall each be entitled to define the formats and procedures applicable to the reporting of such incidents. The Government emphasizes that it is the intention of this Policy to create a bi-directional exchange of information. The NCSC and PNGCERT shall analyse the collected information and use it for information sharing and more importantly, incident warning. They may inform the public, or require the CI providers to do so, where it is determined that disclosure of the incident is in the public interest.

16.7.7 The NCSC and PNGCERT may also inform other CI providers about details of an attack if there is a likelihood that other CI providers will be targeted in the near future. Therefore, sharing such information allows other potentially affected critical infrastructure providers to prevent a similar attack. The NCSC and PNGCERT will ensure that wherever possible, information is anonymized prior to sharing, so as to protect the interests of the reporting CI providers.

PART III: IMPLEMENTATION, MONITORING AND EVALUATION

17. IMPLEMENTATION OF POLICY FRAMEWORK

17.1 A National Cybersecurity Policy Implementation Steering Committee (***NCPISC***) will be formed at the Department of Communication and Information (***DCI***) with the following structure:

Comment [ZD11]: Composition o the NCPISC is the same the existing NSAC with the inclusion of DCI an NICTA – should we retain or divert/incorporate NSAC?

(i) Secretary, Department of Communications and Information, Chairperson
(ii) Chief Executive Officer, NICTA, Deputy Chairperson
(iii) Secretary, Department of National Planning and Monitoring,
(iv) Secretary, Department of Finance, Member
(v) Secretary for Justice, Member

(vi) Commander Papua New Guinea Defence Force, Member
(vii) Commissioner, Royal Papua New Guinea Constabulary, Member.

17.2 The NCPISC will report to the Minister responsible for ICT. The primary role of the NCPISC is to provide overall coordination support for the effective implementation of policy provisions along with monitoring and evaluation of policy interventions.

17.3 The NCPISC will form a sub-committee comprising of representation from the stakeholder community and domain experts, including the private sector, to provide it with domain specific expert advice and recommendations in relation to the execution of Policy provisions.

18. MONITORING AND EVALUATION

18.1 Monitoring and evaluating the implementation of the objectives of this Policy is an important component of the Policy. Through this process, the Government will ensure: -

(i) the respective agencies or institutions with delegated responsibilities under the Policy continue to perform their respective functions;

(ii) the measureable indicators are evaluated to show performance achievements or non-achievements;

(iii) challenges or emerging issues impeding or deemed to impede the implementation of the Policy are identified and addressed in a timely manner; and

(iv) regular updates are provided to the Government on the implementation of the Policy.

18.2 The Department Communication and Information as the Government's lead agency in ICT Policy advisory services will lead the monitoring and evaluation exercise in collaboration with the Department of National Planning and Monitoring, NICTA and the NCSC as well as other relevant stakeholders.

18.3 A detailed Policy monitoring matrix and Policy evaluation matrix will be developed by the DCI in collaboration with the Department of National Planning and Monitoring, NICTA and the NCSC.

18.4 In ensuring that both matrices reflect the international best practice and covers a wider and relevant scope under the Policy, key stakeholders will be identified and consulted including, recognized international and regional organizational partners for comment.

18.5 The matrices will specify the frequency of the monitoring and evaluation exercises and the reporting obligations.

18.6 (Insert clause on GCI assessment participation) The NCSC in collaboration with the NCSAC shall take the lead in ensuring the country actively participates in the ITU Global Cybersecurity Index (***GCI***) assessment with the overall view to improve and raise the level of Cybersecurity in the country

19. POLICY REVIEW

19.1 This Policy must be reviewed on a regular basis and in a timely manner to be on par with advancement in technology, trends and practices in order to remain relevant.

19.2 The NCSAC will be responsible for the coordination of the review of the Policy.

19.~~2~~3 In reviewing this Policy, the outcomes of the monitoring and evaluation exercises shall be taken into consideration.

Annexure A: Cybersecurity Survey Report

Formatted: Font: +Body (Calibri
12.5 pt