NATIONAL CYBER SECURITY POLICY 2021

TABLE OF CONTENTS

FOREWORD BY THE MINISTER

Protecting Papua New Guinea's national security and promoting the prosperity of the PNG Citizens are among my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors. Cyberspace is an integral component of all facets of our new digital economy, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and hackers have increased the frequency and sophistication of their malicious cyber activities. We must make sure to secure and preserve cyberspace for future generations.

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.

Papua New Guinea's success depends on its ability to harness these technological advances to drive economic growth and raise productivity and living standards for all Papua New Guineans. A key focus of the government's digital transformation efforts of government is ensuring PNG keeps pace with community needs and expectations

The digital economy is fundamentally changing how Papua New Guineans live, work and interact with the Government. The PNG public expects government services to be simple, easy and fast to use. To meet these expectations we must be innovative, practical and user-centred in our work. Cyber-related risks are evolving rapidly as PNG becomes increasingly reliant on ICT, as such, it is of paramount importance that PNG's technical and intelligence capabilities must also be developed to international standards and in accordance with international best practice to protect PNG's critical infrastructure systems and essential services. If these cease to function or are compromised, our Government, economy and society can be adversely affected.

The National Cyber Policy demonstrates the Government's commitment to strengthening the Government of PNG's cyber security capabilities and securing PNG from cyber threats. It is a call to action for all PNG Citizens, our universities and all educational institutions, all branches of Government, the private sector, civil society, and the Technical Communities to take the necessary steps to enhance our national cyber-security.

To support the Government's drive towards the 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 Cyber Security.

Cyber Security 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 Cyber Security 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 Cyber Security-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 Cyber security initiatives and enable the Government to assume the lead role in ensuring a safe and secure cyber environment.

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.

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. I must stress here Cyber Security and Cyber Protection is every one's responsibility and not the Government alone.

I call on all Government agencies, partners, international institutions, businesses, policy makers and practitioners to partner and collaborate with my Department and Ministry to develop cyber security capability and capacity that promotes inclusive development towards the Digital Economy and ensure a cyber safe Papua New Guinea.

HON. TIMOTHY MASIU, MP
Minister for Information and Communication Technology.

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to delineate and describe the National Cyber Security Policy for Papua New Guinea (PNG). Cyber-related risks are evolving rapidly and as PNG becomes increasingly reliant on ICT, it is of paramount importance that its technical and intelligence capabilities in cyber security be developed in par with international standards and in accordance with international best practice in order to provide adequate protection for its citizens, critical infrastructure systems and national security. In this modern day and age open connection is enabled by the internet, if without an in-country mature cyber security capability and capacity, PNG may be subjected to cyber incidents that may adversely affect PNG’s economy.

This National Cyber Security Policy sets out the Government's approach toward addressing every changing and dynamic cyber security risks and challenges. The Policy defines the Government's vision, goals, objectives, evolving governance and the principles to guide the development of relevant strategies and action plans on minimize cyber security risks.

Considering the current landscape, this Policy sets a direction for the Government to:

- partner and collaborate across all stakeholder groups, including private sector and civil society, academia and technical community to promote best practices and develop strategies to overcome market barriers to the adoption of secure technologies;
- improve awareness and transparency of cyber security risks and practices to build market demand for more secure products and services;
- partner and collaborate with international partners to promote open, industry-driven standards and risk-based approaches to address cyber security challenges, including cloud security platform;
- collaborate with the private sector, civil society and the cyber security community to promote awareness on cyber hygiene and cyber safety;

- work with all Ministries, including the Ministry of Education and the Ministry of Higher Education to include cyber security and cyber safety in future curriculum that can equip students with relevant cyber knowledge and etiquette, and further generate interest to pursue cyber security professional careers in PNG.
- Government to create in its strategy inclusive partnership approach with clear short term and long term on professional capacity and capability plan, with the focus on development of national expert workforce in both public and private sector, including attractive renumeration and retainer packages to retain these developed national human capacity in the public sector and in PNG.

1.2 Background

Over the recent past years, PNG has seen a rapid increase in the adoption of digital technologies across all sectors of the economy. The increased use of digital technologies inevitably increases PNG's exposure to cyber security risks. PNG remains vulnerable to cyber-based crimes which may increase due to faster and better internet connectivity enabled by Coral Sea Cable commissioning, hence this policy intervention is imminent.

The PNG National Security Policy 2013 recognizes 'Cyber-based Threats' and the 'National Information Security' as two of the generic threats to PNG's survival, however, the cyber landscape and threats has changed drastically, and this policy intents to capture these changes, and serves as an update and reference to future national security policy dialogues and reviews.

In 2020, the Government adopted a PNG Digital Transformation Policy that recognizes and sets a pathway for the Government to drive digital transformation across all sectors of the economy. Cyber security is a paramount objective of the Government under the PNG Digital Transformation Policy.

Cyber-attacks have become more sophisticated, targeting specific organisations in the public and private sector through victim reconnaissance and if the country's critical systems and infrastructure cease to function or are compromised, the Government, economy and the society can be adversely affected.

Malicious cyber activity is one of the most significant threats impacting the world and PNG is part of the global society impacted by malicious cyber activities. The COVID-19 pandemic highlighted the evolving nature of cyber threats in particular that associated widespread Infodemic daily. PNG citizens must have adequate knowledge of these threats and risks as individuals or other be informed through Government trusted awareness channels so each individual may take informed decisions to understanding the risks.

Nation states and state-sponsored actors seek to compromise networks to obtain economic, policy, legal, defence and security information for their own advantage. Nation states and state-sponsored actors also seek to achieve disruptive or destructive effects against their targets. These actors tend to be sophisticated, well-resourced and patient adversaries, whose actions could impact PNG's national security and economic prosperity.

Highly sophisticated nation states and state-sponsored actors continue to target governments and critical infrastructure providers. It is not uncommon for more than 30% of these incidents to be directed towards nation's critical infrastructure providers that deliver essential services including healthcare, education, banking, water, communications, transport and energy.

Protecting Papua New Guinea's national security, ensuring the security of cyberspace and promoting the prosperity of the citizen through the safe use of digital technologies to drive economic growth and raise productivity and living standards for all Papua New Guineans are among top priorities.

Minimum requirement for PNG to improve its cyber protection and safety is to have the following:

- Relevant national policies, laws, rules and procedures to foster coordination, collaboration and cooperation;
- Specialized cyber security technical capabilities;
- Proper institutional structures and skilled personnel;
- Proper mechanism for information sharing and awareness

PNG's National Cyber Security Centre (NCSC) was established in 2018, with the support of the Australian Government, and attempts to establish operational capacity through facilitating internal capacity building programs for Government IT managers and the industry. Presently the NCSC houses the Cyber Security Operations Center (CSOC) function and the PNG Computer Emergency Response Team (CERT)[1] function.

The NCSC is managed by a Steering Committee, comprising the Department of ICT, the Office of Security Coordination and Assessment (OSCA) which falls within the Department of Prime Minister and NEC and the National Information and Communication Authority (NICTA) as lead agencies and with other stakeholders Defence, Police, Justice and the National Intelligence Organization as key stakeholder agencies.

The NCSC has been providing incident response coordination and advisory as a service for whole of PNG society since 2019.

The NCSC in addition has been developing cyber security capability through implementation of endpoint protection for the whole of government, with monitoring and reporting capability at the NCSC.

Post APEC 2018, the NCSC is providing the current function of;

- Advisory services on Cyber matters and incidents,
- Coordination dialogue and collaboration between government and stakeholders,
- Promoting cyber security and cyber safety awareness,
- CERT and incident response coordination.
- Development of cyber security capability through implementation of endpoint protection for the whole of society;
- monitoring and reporting capability
- Professional cyber security skills training for IT personal,

[1] A CERT is a computer emergency response (or readiness) team and the term is trademarked by Carnegie Mellon University. A CSIRT is a group that responds to security incidents when they occur. CSIRT stands for a computer security incident response team and is a generic name for this type of service. The terms CERT and CSIRT are used interchangeably, despite the important differences.

2.0 POLICY ALIGNMENT AND FRAMEWORK

The goals of the National Cyber Security Policy is consistent with the provision of the National Constitution pertaining to the safeguarding of Papua New Guinea's national sovereignty. The Policy supports and complements the existing policies of the Government that point towards security and a safer and secure cyberspace for Papua New Guineans. These policies and legal framework include:

- The Papua New Guinea National Security Policy 2013
- The Papua New Guinea National Security Policy Strategic Action Plan 2014-2020
- The PNG Digital Transformation Policy 2020
- National ICT Policy 2008
- The National Intelligence Organization Act 1984
- The National Information and Communication Technology Act 2009
- The Classification of Publication (Censorship) Act 1989
- The Gaming Control Act 2007
- The Lukautim Pikinini Act 2015
- The Cybercrime Code Act 2016

The National Cyber Security Policy intends to focus on cyber related matters, complementing existing policies and legislations, where appropriate, to improve the governance and the operational framework that protects the Independent State of Papua New Guinea, its institutions, its environment, its resources and the people.

3.0 VISION, MISSIONS & GOALS

3.1 Vision

The Government envisages safer and trusted cyberspace for all citizens that harness the benefits of digital technologies.

3.2 Mission

Enable a safer cyberspace to protect our national sovereignty and promote inclusive growth in the digital economy.

3.3 Goals

Goal 1: Governance

- Establishing an effective coordination mechanism, with relevant organizational structure and specialized cyber security institutions to promote strengthening of cyber security capability and capacity in PNG.

Goal 2. Risk Management, Preparedness & Resilience

- Understanding the evolving cyber security risks and capabilities available, establish appropriate effective national capabilities to prevent, detect, mitigate and respond to major cyber security incidents and improve overall cyber resilience.

Goal 3. Critical Infrastructure & Essential Services

- Identify and establish a risk-management approach to protect national critical infrastructure and essential services, through public private partnership.

Goal 4. Capability & Capacity Building and Awareness raising

- Develop national capability and capacity, increase knowledge, develop specialized skills on cyber security and raise awareness on cyber security and protection, cyber safety and cyber hygiene to all stakeholders.

Goal 5. Legislation and Regulations

- Develop appropriate legislative and regulatory framework to promote cyber protection and to protect society against cybercrime, including protection of citizens' rights and data and fostering conformance and compliance.

Goal 6. International Cooperation

- Forge and foster cooperation and engagement with relevant international cyber security partners and institutions to manage cross border cyber incidents and combat cross border cybercrimes in mutually acceptable solutions inline with applicable foreign policies.

3.4 Guiding Principles

The following Guiding Principles will lead PNG towards realizing its aspired Vision, Mission and the Goals:

- Cyber security operation capacity and PNG CERT function are national security functions that shall be managed by all national teams.
- Protecting citizens, visitors, businesses and government agencies and Critical National Infrastructure by providing the necessary security frameworks, strategies and guidelines, building national cyber security skills capacity, implementing information sharing techniques and raising awareness;
- Building a strong cyber security environment that will guard the 'Sovereignty' of our Independence and safeguard the 'Privacy' of our citizens as enshrined in our National Constitution;
- Engaging all stakeholders nationally and internationally in consultations and in collaborations to ensure all stakeholders understand the policy goals and objectives for inclusive participation;
- Strengthening the current legal framework to ensure that all existing policies are updated for the digital economy, including child protection legislation and privacy and data protection, critical infrastructure protection, digital identification and e-Commerce;
- Cultivating strong linkages with international partners and institutions including the different UN organizations, regional organizations, experts and civil society.
- Cyber Security and Cyber Protection is everyone's responsibilities and not the Government's alone.

4.0 POLICY FOCUS AREAS

The PNG Government will develop a National Cyber Security Strategy that encompasses the protection of information systems and critical infrastructure, fight against cybercrime and development of the legal and regulatory framework, development of digital security skills and culture, promotion of digital trust and national coordination and international cooperation.

4.1 Cyber Security Coordination and Governance Framework

The policy recognizes effective governance and effective coordination which requires clear leadership, and this can only happen if mandated from the highest authority and with clear demarcation of roles and responsibilities of every stakeholder involved. As such cyber security should be promoted and sustained at the highest level of government.

As a pragmatic immediate approach (Phase 1), the government shall initially transition the current NCSC capability from being under partial foreign administration control to total national administrative control, evolving from the current operation capacity of national cyber security centre (NCSC) to National Cyber Coordinating Center (N3C) as depicted in Figure 1 in Attachment 1. The N3C function shall focus on effective central coordination and decentralized implementation. The steps necessary to invoke this transition includes;

- full national administrative control;
- build full national capacity in the Cyber Security Operation (CSO) and Computer Emergency Response Team (CERT) operation, and support with necessary short team special training and technical and tactical capabilities, to be followed with long term enduring capability;
- accelerate rollout of monitoring capability to all government agencies as priority and further PNG society wide;
- operationalize basic CSOC and Incident Response and CERT operations, with real time monitoring and routine reporting with clear plans to scale, if need arises.
- utilise the activated capabilities of CSOC, CERT and the Incident Response process to support operations of the Social Media Management Desk functions.

- utilise the activated capabilities of CSOC, CERT and the Incident to support other law enforcement agency requirement.

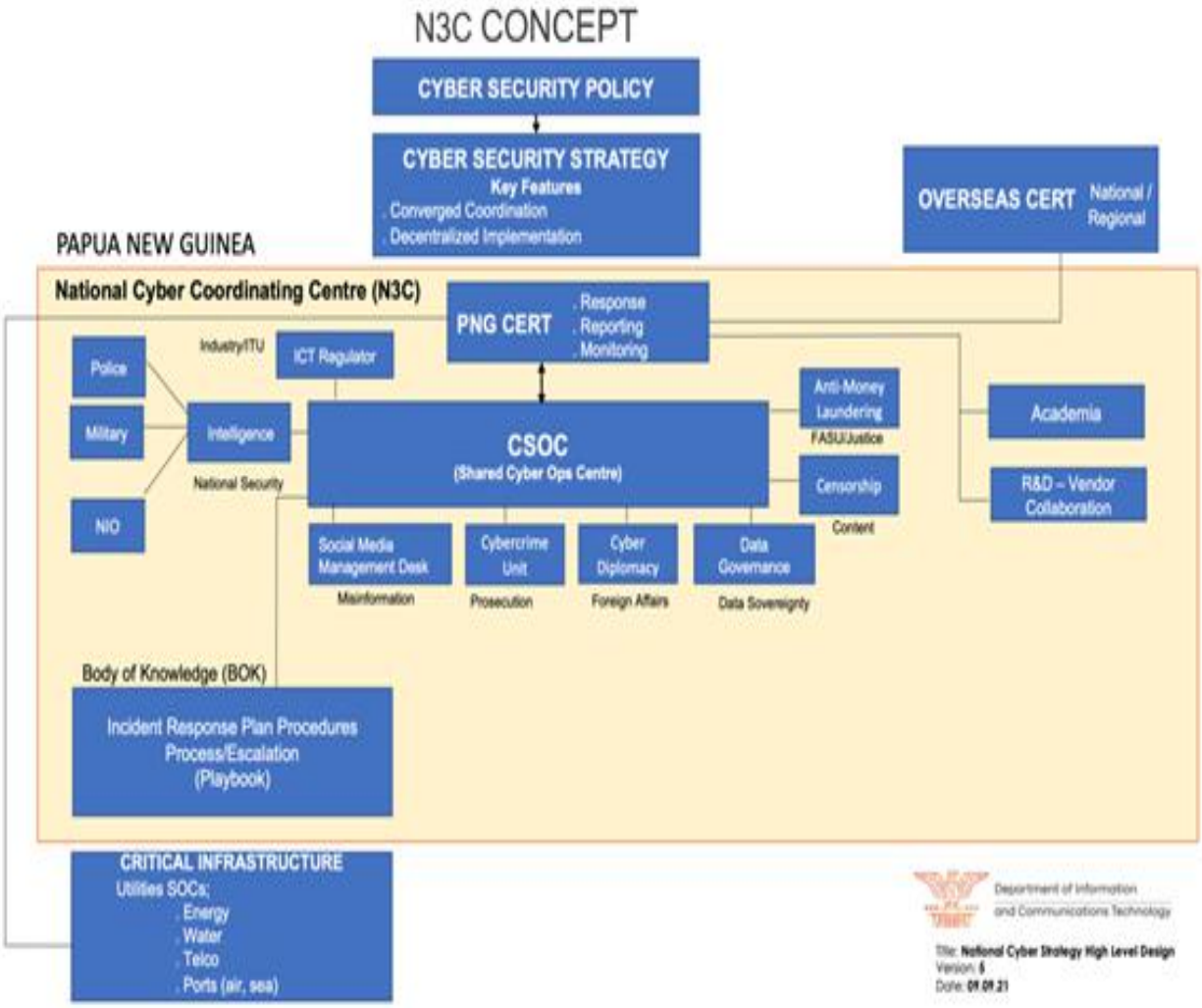

Figure 1. National Cyber Coordinating Center (N3C) structure

The long-term approach (Phase 2) is through a national cyber security strategy, transform the N3C operational capability and capacity to coordinated shared Cyber Security operations capability under the National Cyber Security Agency.

The National Security Council (NSC), chaired by the Prime Minister, is the highest decision-making body on national security issues threatening the sovereignty, security and protection of the Independent State of PNG. The National Security Advisory Committee through the Office of the Security Coordination and Assessment (OSCA) provides technical advisory support to the NSC.

The Government will address cyber-related issues in a coordinated and converged manner where cyber security becomes a subset of a National Security Agenda. Through this approach the Government, while strengthening its existing structures, will establish an entity to coordinate and strategically address cyber-related issues with strategic oversight over various cyber related programs, functions and capabilities.

The diagram below depicts the coordinated approach where NCSA will have a strategic oversight over the cyber security issues in the country.

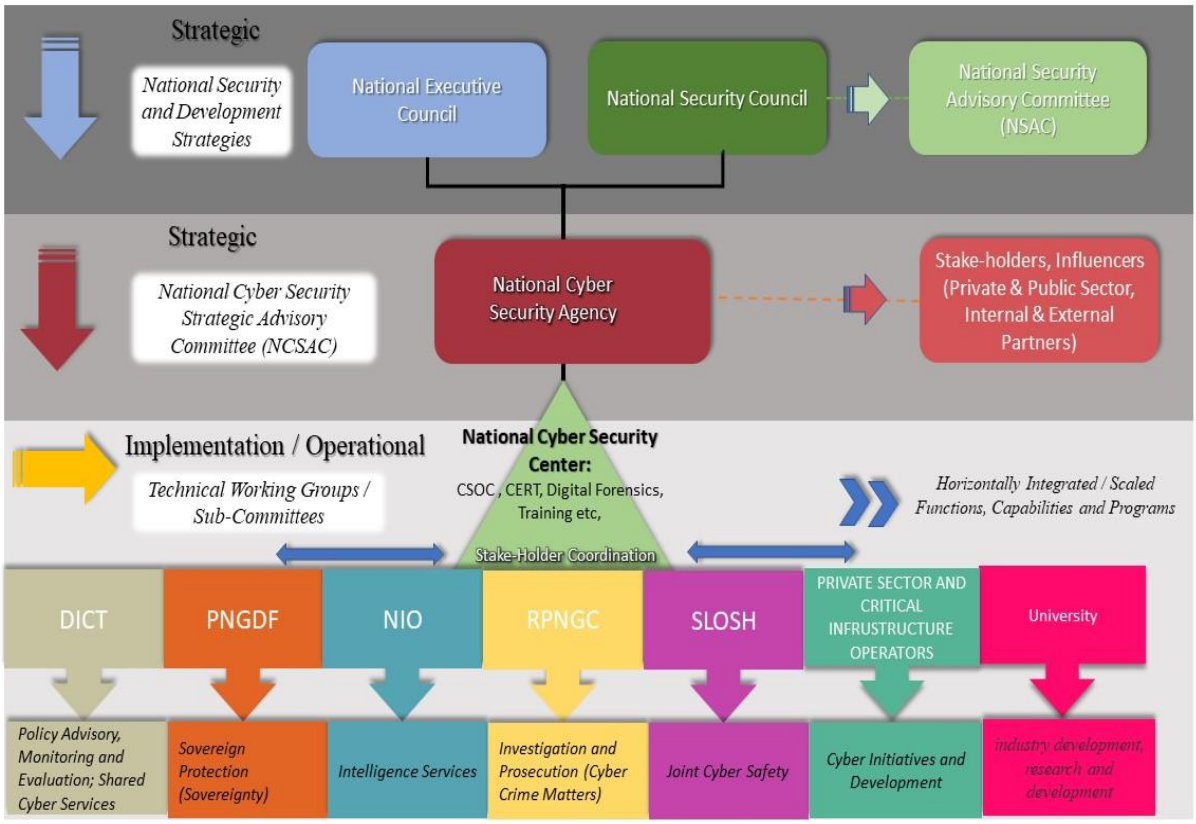

Figure 2. Coordination Mechanism and Specialized Cyber Security Institution with key stakeholder agencies.

4.1.1 National Cyber Security Agency (NCSA)

The PNG Government will establish a National Cyber Security Agency (NCSA) to coordinate national cyber security agendas and provide direction, to coordinate action and to monitor the implementation of the National Cyber Security Strategy. The NCSA will also act as a management entity to define and clarify roles, responsibilities, processes, decision rights and the tasks required to ensure effective implementation of the National Cyber Security Strategy.

NCSA will be established to be the coordinating arm of the Government on matters relating to cyber security. NCSA will, among others:

- elevate cyber security advisory to National Security Council level;
- be a platform for interaction with stakeholders and influencers, external and internal, including the private and public sector that are seeking cyber security services and support or are seeking to engage with operational agencies of Government on cyber security;
- coordinate and connect stakeholders, influencers and public and private sector bodies with appropriate functional and operational agencies, in particular, the operational agencies of Government will have within their oversight the critical digital infrastructures, systems and capabilities and any external and or foreign party seeking to engage with these agencies will enter through NSCA for check and clearance purposes; and
- coordinate research and development in cyber security.

4.1.2 National Cyber Security Advisory Committee (NCSAC)

The PNG Government will create a National Cyber Security Steering Committee (NCSAC) composed of members that include but limited to experts, authority figures and senior stakeholders within the private and public sector.

NCSAC comprising cyber security policy and operational agencies will be established within the NCSA and chaired by the Office of Security Coordination and Assessment to provide technical advisory support to the Government. Technical working group(s) and sub-committee(s) will be formed as and when required to deal with specific issues on cyber security and provide strategic directions through the NCSAC.

4.1.3 National Cyber Security Center (NCSC)

NCSC is the cyber security headquarter which houses PNGCERT, CSOC and other proposed national cyber security functions. NCSC will provide full support with cyber security controls as defence tools, safety measures and resilience to GoPNG and critical infrastructure operators. businesses, civil society and educational institutions will be supported through PNGCERT on advice, investigation and information basis on cyber safety and cyber security.

NCSC may collaborate with international partners to improve its cyber security standards depending on the need when the cyber landscape changes, and priorities shift which cannot be addressed nationally.

4.1.3.1 PNG Computer Emergency Response Team (CERT)

The PNG Government will coordinate cyber security capability implementation through the National Cyber Security Centre ensuring the PNGCERT is well equipped and functioning together with all relevant CERT's locally, and at regional and global level.

The Papua New Guinea Computer Emergency Response Team (PNGCERT) shall promote awareness, provide advisory assistance, and coordinate responses to cyber-security incidents in PNG.

It's mission is to establish to function as national point of contact for:

- coordinating the management of national cyber security incident;
- promoting cyber security situational awareness with respect to local, regional and global;
- advocating professional capacity building through the introduction of best practices and measures in the promotion of cyber security
- coordination and collaboration with international counterparts in managing or addressing cross cyber security incidents and cybercrime, and with respect to the advanced cyber security capabilities;
- the overall promotion of secure systems and networks for its constituency, that is for the whole of PNG digital society; and
- conduct regular cyber security risk assessment exercise to ensure updated information is used to update incident response decision making and where needed issue advisory on the update risks or threats to its constituency.

PNGCERT's main focus is to help support the prevention, detection and response to cyber incidents, conducting minor digital forensic investigations, and maintaining consistent points of contact and presence.

4.1.3.2 Cyber Security Operation Center (CSOC)

CSOC monitors, detects, analyses and investigates cyber security threat alerts within an organisation's networks. The CSOC conducts detailed investigations into such cyber security threats, and reports their findings to the appropriate bodies, such as PNGCERT to assist with remediation.

CSOC assists post-incident investigation, where it conducts deeper analysis, audit and reviews and provides further recommendations. CSOC also provides threat intelligence when required to the appropriate bodies, coordinated through OSCA

4.1.4 Government Stake-Holders by Implementation and Operational Functions

There are Government departments and agencies that are overseeing certain functions and operations on cyber security. These functions and operations relate to:

- development, implementation, monitoring and evaluation of appropriate policies and strategies on cyber security;
- cyber defense and offensive capabilities;
- cyber investigation and intelligence; and
- counter-espionage, cybercrime and cyber safety.

The Government shall strengthen and equip these institutions with appropriate capabilities to perform its functions and operations effectively to safeguard PNG's cyber environment, its sovereignty and its people.

4.1.4.1 Office of Security Coordination and Assessment (OSCA)

OSCA's responsibility is to provide high quality and timely policy advice to the National Security Council (NSC) for the effective management of issues of national security, Defence & international relations.

As any cyber threats has potential to threaten national security, OSCA shall continue to maintain strategic oversight of cyber security matters through its chairmanship of the National Cyber Security Steering Committee.

4.1.4.2 Department of Information and Communication Technology (DICT)

DICT as the Government's lead agency on ICT policy matters shall oversee and lead the development, implementation, monitoring and evaluation of appropriate policies and strategies on cyber security.

4.1.4.3 PNG Defense Force (PNGDF)

The PNGDF shall be responsible for PNG's cyber defense and offensive capabilities and other related matters.

4.1.4.4 National Intelligence Organization (NIO)

The NIO shall be responsible for cyber investigation and intelligence service and other related matters.

4.1.4.5 Royal PNG Constabulary (RPNGC)

The RPNGC shall be responsible for counter-espionage and cybercrime and cyber safety enforcement and other policing related matters.

4.1.4.6 Department of Justice and Attorney General (DJAG)

DJAG and its other relevant offices and agencies shall be responsible for enforcement of Cyber related legislations and regulations, and collaborate on development of new cyber related laws and regulations and other related legal matters.

4.1.4.7 Office of the Censorship (OOC)

OOC will be responsible for Cyber Hygiene and aspects of online safety and other related matters.

4.2 Risk Management, Preparedness & Resilience

Cyber risks cannot be fully eliminated, and are very dynamic and unpredictable. Cyber Security is about risk management and resilience. Risk management involves identification of critical assets and essential services for proper functioning of the society and economy, their dependencies, inter-dependencies, threats and risks associated and establish the best approaches to take to manage these.

Government and all stakeholders shall foster ongoing collaborate to identify measures that includes creating and maintaining real time map and other presentations or reports of the threat landscape for informed decision based for the best use of current capabilities to protect, detect and respond to cyber threat actions and identify where the gaps are, thereby creating an effective and functional incident response ecosystem.

4.2.1 Statistical Data on Cyber Security Compromises

Better statistical data on the national impact of cyber security compromises is required to enable the PNG Government and businesses to make informed decisions when managing cyber risks. Data collection measures will help the Government and the private sector to better make decisions that address cyber security threats to PNG's economy and security.

The Government through the Department of Information and Communication Technology will establish and maintain a database on the national impact of cyber security breaches.

4.2.2 Cyber Security Emergency Readiness

The Government is committed to introducing measures, adopting legislations, standards and strengthening the institutional framework on cyber security to safeguard PNG's cyber environment.

Throughout the capability build up and organisational transition under this policy, in the case of national cyber threat emergency, a Joint Strategic Centre (JSC) functional unit shall be established to provide dedicated ICT support services for the control and management of a special situation and other related matters.

The responsibilities of the JSC function or a similar body would be to:

- ensure inter-agency connectivity and resource sharing for emergency responses and public safety;
- provide emergency systems or digital infrastructure as shared services;

- use software and hardware to provide facial recognition services, vehicle recognition services and intelligent video recognition services;

- provide human behaviour analysis services for early detection of offenses;

- provide services to eliminate information and communication silos across public bodies;

- enable efficient collaboration amongst public bodies for data storage, data sharing, analysis and dispatch to support policy decisions; and

- otherwise enhance the control and management of any special situation and promote enforcement of any restrictions or other lawful requirements made in response to the special situation.

An Action Plan will be developed under the cyber security strategy to provide a clear path for the Government to respond to cyber security emergencies

4.2.3 Develop Incident Response capability

Preparedness include development of robust and effective incident response capabilities that involve all relevant stakeholders participation in managing an incident.

Understanding the risks and capabilities available, preparedness is about establishing appropriate and effective means, methods and to prevent, detect, mitigate and respond to these incidents with the intention to improve overall cyber resilience.

Government and stakeholder shall endeavor to use best practice methods in risk management to develop effective and inclusive incident response capability that is responsive, regularly updated and focused on resilience.

4.2.4 Development of standards

Cyber security standards enhance security and contribute to risk management in several important ways. Standards help establish common security requirements and the capabilities needed for secure solutions. Standards must be based on open standards and international best practices.

4.3 Critical Infrastructure & Essential Services

The Government recognizes the need to have a national cyber security technology framework that provides all the required standards and baseline for critical infrastructure (CI), in particular putting emphasis on Critical National Information Infrastructure (CNII) and essential services that follow international best practice.

The Government will develop and actively defend the critical infrastructure that all PNG citizens will rely on, including:

- work with the business community to create a voluntary code of conduct/practice for all products and services that will set out the Government security expectations for Internet-connected consumer devices.
- partner with the private sector, especially large businesses to assist small and medium enterprises (SMEs) to grow and increase their cyber security awareness and capability.
- work with the private sector to manage risks to critical infrastructure at the greatest risk;
- develop a comprehensive understanding of national risk by identifying national critical functions and will mature our cyber security offerings and engagements to better manage those national risks;
- prioritize risk-reduction activities across critical key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation.

4.3.2 Identifying Critical National Information Infrastructure

Critical National Information Infrastructure (CNII) are key components of any country's Critical National Infrastructure (CNI). The Government will identify Papua New Guinea's critical national infrastructure and critical network information infrastructure through a step-by-step risks assessment approach and establish specific criteria of operations as a partnership with services operators.

Among other criteria, this shall include;

- the size of the potentially affected population;
- intra-sector and cross-sector dependencies;
- geographic criteria; and
- the impact on personal safety and privacy.

Critical infrastructure top targets, but not exhaustive are:

- Public/government,
- Telecommunications,
- Health,
- Academic,
- Manufacturing,
- Power/utility,
- Transportation, and
- General information warfare threats.

4.4 Capability & Capacity Building and Awareness raising

Develop national capability and capacity, increase cyber knowledge and digital literacy, develop specialized skills on cyber security and raise awareness on cyber security and risks associated, cyber protection, cyber safety and cyber hygiene for the constituent.

4.4.1 National Cyber Security Capacity and Capability Development

Government and stakeholder shall partner in development of national cyber security professionals, institute cyber security as capability in every public and private ICT organisations and institutions. Further governments in partnership with the education sector shall embed cyber security and cyber safety knowledge as core to its education curriculum as soon as practical focusing on creating a new PNG generation who are cyber 'save' and digital literate, who shall in turn develop interest and career paths to become cyber security specialist and experts in PNG.

4.4.2 Cyber Awareness

Government in partnership with stakeholder and through PNG CERT shall endeavor to increase and maximise awareness on cyber safety and cyber hygiene, to combat threats including child online safety and other potential social and civil disturbance threats related to social media Infodemic, including that surrounding health pandemic covid 19 and or similar pandemic, national general election and others in future.

4.5 Strengthening Legal and Regulatory Framework

In order to protect openness and a safe environment, Papua New Guinea shall have a reliable legal framework that reflects the uniqueness of the country as well as international best practices

There are various policies the Government has adopted that both provide a framework for cyber security and act as an anchor for the Government's National Cyber Security Policy. The Legislative Acts listed in this Section are the key critical legislations that the Government will enact to lay out and describe the cyber security standards that will be required and provide clear guidance for the Public and Private sector on cyber security.

These legislations will give effect to the Government's policies, strategies, action plans and roadmaps on cyber security and ensure a structured, collaborative and coordinated approach towards effectively addressing national cyber security challenges.

4.5.1 Digital Government Legislation

The legislation will set the legislative framework for ICT governance particularly digital information management systems in all public bodies in PNG. It will deliver digital infrastructure, digital government, digital skills, innovation and entrepreneurship, digital cyber security and privacy, financial inclusion and information classification across the whole-of-government and sub-nationally for delivery of public services efficiently paving way for transformation of the economy into a digital economy.

The law will:

- Pave way for proper coordination of procuring and use of digital technologies in the public sector, ensuring highest level of security for government systems and government information and data;

- Establish, define and anchor the functions and powers of the Department of ICT as lead Government agency to provide oversight on digital transformation processes across the whole-of-government.

The Digital Government Legislation will provide the legal basis for the Government to:

- Streamline national planning and coordination of ICT funding, infrastructure development and services primarily within the public sector;
- Define and ensure compliance of international best practices, national ICT and digital standards for all public and statutory bodies;
- Centralize and streamline procurement and usage of ICT products and services for all public and statutory bodies;
- Compel and facilitate the centralization of all government data and information, and sharing of data and information between government to government, government to citizen, government to business and vice versa;
- Facilitate and compel cyber security standards and compliance for all public and statutory bodies;
- Facilitate and coordinate digital government services specifically: government to government, government to citizen, government to business and vice versa, to increase public service delivery efficiency and reduce government expenditure. For example, e-Voting, e-Census, e-Tax, e-Agriculture, e-Police, e-Education, e-Parliament and range of e-services;
- Facilitate transformation of the economy to digital economy through development and implementation of other relevant regulations and standards, programs, and projects pertaining to digital skills, digital services, and digital infrastructure; and
- Facilitate and coordinate digital information dissemination and communication for government to government, government to citizen, government to business and vice versa.

4.5.2 National Cyber Security Legislation

A National Cyber Security Legislation will be developed to implement the goals and objectives of this Policy.

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services.

Cyber security challenges persist as a result of a number of factors including, among others, lack of a culture of cyber security consciousness and limited awareness on cyber security issues among businesses and individuals; challenge of enforcement of legislation; as well as limited capacity among law enforcement agencies in the detection, investigation and prosecution of internet-facilitated crimes.

Many Government agencies have a minimal understanding of cyber security risks and threats. The private sector has limited awareness of cyber security threats and risks. Moreover, SMEs within PNG have a lack of human capacity and resources to sufficiently deal with cyber security. Nationwide, larger international civil society organisation and development partners do not consider cyber security a priority for them as a result they are subject to a range of cyber-attacks. Despite having a CERT in PNG, the channels to report cyber incidents are not coordinated. Certification and accreditation of public sector cyber security professionals did not exist.

Cyber Security laws and regulations tend to cover the most common matters that arise from cyber threats. These matters include a focus on criminal activity, corporate governance, insurance matters, and the jurisdiction of law enforcement.

The legislation would establish a new agency to be responsible for all cyber security issues. Cyber security Authorities within the new Cyber Security agency and will regulate and promote developments within the country and manage and enforce its cyber security space. This mandate will see the new Cyber Security Agency play a key role in preventing, managing, and responding to cyber security incidents in PNG. This new Agency or Authority will work closely with the Agency or Department that Manages Critical Infrastructure in terms of cyber security activities, services and practices.

The Cyber Security Agency that will be set up will have a very wide mandate in ensuring that PNG is protected from cyber-attacks and breaches. To this end, the Agency will be monitoring cyber security threats within and outside PNG, taking measures in response to cyber security attacks and breaches, especially those with the potential of threatening PNG's national security, economy, international relations, and public health.

At the heart of the Cyber Security Act is the protection of computer systems. A computer system includes a variety of technological devices with computing capabilities such as an operational technology system, or any device which has supervisory control and data acquisition and distribution capabilities.

Considering the wide range of risk stemming from both physical and cyber threats and hazards, the Government will develop a legislation that will:

- harmonize with existing national laws;
- contain provisions compatible with international standards and best practices in order to enable and sustain cooperation regionally as well as on an international basis;
- provide for creation of a specialize cyber security agency;
- provide for a coordination framework to harmonize efforts across key cyber security agencies of Government; and
- enable collaboration and cooperation among all stakeholders to ensure protection of:
    - digital services and essential services;
    - e-identification and trust services; and
    - personal data; among others

4.5.3 Critical Infrastructure Legislation

The Government recognizes the need to protect essential critical infrastructure against natural disasters, terrorist activities and cyber threats. Disaster preparedness, response and recovery are top priorities. It will develop legislation to protect PNG's critical infrastructure and systems.

Systems that once stood alone managing critical infrastructure operations are connecting to the Internet and sharing sensitive data. Through convergence, physical structures are merging with digital structures and are connected to the Internet making these services becoming vulnerable to attacks.

While this increased reliance on interlinked capabilities helps make the PNG economy more efficient and stronger, it also makes the country more vulnerable to disruption and attack. This interdependent and interrelated infrastructure is more vulnerable to physical and cyber disruptions because it has become a complex system with single points of failure.

The elements of the infrastructure themselves are also considered possible targets of terrorism. Traditionally, critical infrastructure elements have been lucrative targets for anyone wanting to attack another country. Now, because the infrastructure has become a national lifeline, terrorists can achieve high economic and political value by attacking elements of it.

Disrupting or even disabling the infrastructure may reduce the ability to defend the nation, erode public confidence in critical services, and reduce economic strength. Additionally, well chosen terrorist attacks can become easier and less costly than traditional warfare because of the interdependence of infrastructure elements. These infrastructure elements can become easier targets where there is a low probability of detection.

The elements of the infrastructure are also increasingly vulnerable to a dangerous mix of traditional and non-traditional types of threats. Traditional and non-traditional threats include equipment failures, human error, weather and natural causes, physical attacks, and cyber attacks. For each of these threats, the cascading effect caused by single points of failure has the potential to pose dire and far-reaching consequences.

PNG’s access to power, electricity, transportation networks, drinking water and many other critical infrastructure services is increasingly at risk from cyber-attacks. These threats can have devastating consequences and could threaten entire communities. The success of critical infrastructure protection initiatives relies on strong and meaningful partnerships being built between governments, the private sector, technical communities, and our development partners. Success

also relies on the solutions that are used to manage and implement these initiatives.

Considering the implications on critical infrastructure and essential services, the Government will develop a legislation that will:

- harmonize with existing national laws;
- contain provisions compatible with international standards and best practices;
- provide a mechanism to identify PNG's critical infrastructures in respective sectors and provide necessary protection of these infrastructures;
- mandate and empower relevant responsible agencies to take necessary measures towards protecting these critical infrastructures, including measures on disaster preparedness, response and recovery.

4.6 International Cooperation

To tackle the transnational dimension of Cyber security incidents on the one hand and benefit from the support of different organizations for developing countries on the other hand, Papua New Guinea will utilize means of international cooperation and support.

The Government will work with its allies, donors, international partners and in the technical community to assist in strengthening PNG's capacity to prevent or respond to malicious cyber activity, including in response to sophisticated actors.

Cooperation and collaboration with other partners is critical. The Government recognizes that no Government can unplug itself from the world or exist in its own silo. It requires collaboration and partnership both with the private sector, civil societies, technical community as well as with international organizations and other governments. The Government will work with other governments and increase partnership and become members of international organizations working in the cyber security arena.

PNG is a member of the Global Forum on Cyber Expertise (GFCE), Pacific Cyber Security Operational Network (PaCSON) and Asia-Pacific Economic Cooperation (APEC), and the Government shall assess and join other related cyber organizations in order to strengthen its capacity to protect PNG's cyber environment.

PNG shall enter into bilateral and multilateral partnership on Cyber Security Cooperation. The partnership will focus on areas of:

- Developing and enhancing cyber security governance and best practice frameworks;
- Building capacity in incidence response, forensic analysis and crisis management;
- Establishing and equipping PNG's cyber security technical institutions to monitor the protected networks for threats and provide incident response support;
- Enhancing PNG CERT capacity (CERTs are the "first responders" during a cyber incident) by providing regular and advance training at the NCSC.

A coordinated approach led by the Government is a key step towards Cyber security preparedness and resilience to counter cyber threats and attacks.

In this vein, the Government will coordinate more collaboration with the private sector, technical communities, international cyber security bodies and other governments to:

- Create common standards and practices on cyber security within Government, and guidelines to businesses;
- Develop appropriate and relevant legal and regulatory frameworks to define and support common standards, practices and guidelines;
- Strengthen institutions responsible for cyber security with adequate capacity to lead and enhance cyber security activities;
- Encourage national co-leadership and cross-sectoral partnerships to foster strong cyber security.

5.0 IMPLEMENTATION PLAN/FRAMEWORK

The institutional and governance arrangements to oversee the implementation of various directives and technical measures on cyber security as provided in this Policy will be in phasal approach.

Phase 1 will be from the time the Policy is adopted. It will build on from the current effort. The Department of Information and Communication Technology will oversee the National Cyber Security Centre and provide technical support on cyber security and provide secretariat support to the National Cyber Security Centre Steering Committee. OSCA will provide chairmanship to the Committee. Major deliverables in Phase 1 are:

- Development of the Cyber Security Legislation that will establish the National Cyber Security Agency and define the roles of key stakeholders on cyber security and the working relationship among these stakeholders;
- Development of Legislation for Critical Infrastructure to protect PNG's national critical infrastructures and assets.
- Maintaining and upgrading the National Cyber Security Centre to meet international standards and best practice requirements;
- Training and capacity building on cyber security for PNG nationals to a competency level par with international experiences
- Facilitate necessary requirements for the establishment of a Cyber Security Agency.

5.1 Executive Sponsor

The OSCA is the Executive Sponsor of the National Cyber Security Strategy. OSCA will be primarily responsible for assigning relevant roles and responsibilities and allocating sufficient human and financial resources. OSCA is the Agency in the Government that has a clear understanding of the Government's broad security, digital and development ambitions.

5.2 Lead Authority

The Department of Information and Communication Technology will be the Lead Authority on cyber security strategy design and coordination of its implementation.

DICT will:

- lead the development of the cyber security strategy;
- be responsible for providing leadership on the culture and values that shape the strategy's focus; and
- in its capacity as lead 'project' authority, appoint various government departments to be involved in the design and development of the cyber strategy development process and implementation of the strategy's action plan

5.3 National Cyber Security Centre (NCSC) Steering Committee

A Cyber Security Steering Committee will provide guidance and play a critical role in quality assurance and assist the lead project authority to overcome any inherent bias and help avoid intra-government competition for resources. The Steering Committee will guarantee the transparency and inclusiveness of the process. Representatives on the Steering Committee will (as a minimum) be the following departments:

- OSCA to provide chairmanship
- Defence,
- Justice,
- Censorship,
- Police,

The National Intelligence Office and the Department of ICT to provide secretariat support

The Steering Committee will:

- be aided by an advisory committee composed of private sector companies and professionals as well as representatives from the Technical Community, the academic community and any cyber related NGOs in PNG;

- ensure that the Government has the correct Cyber resiliency standards and guidelines that are needed to protect all infrastructure and essential services from attack;
- work with the respective Ministry, Agency or department to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever-changing threats. As systems are protected, alerts can be issued in real time when events are detected to help protect networks across the government information technology enterprise and the private sector. This enterprise approach will help transform the way federal civilian agencies manage cyber networks through strategically sourced tools and services that enhance the speed and cost effectiveness of federal cyber security procurements and allow consistent application of best practices.
- work with its partners to provide Government Agencies with capabilities and tools that identify cyber security risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cyber security personnel to mitigate the most significant problems first. It is their goal to provide adequate, risk-based, and cost-effective cyber security and more efficiently allocate cyber security resources.

6.0 MONITORING & EVALUATION

Monitoring, evaluation (M&E) and learning from the outcome of M&E are important to ensure effective implementation of this Policy and to ensure relevant agencies and key stakeholders are progressively implementing the objectives and the directions of this Policy.

The Department of Information and Communication Technology, in collaboration with stakeholder agencies, will design and implement a monitoring, evaluation and learning framework to:

- track the progress on implementation of the Cyber Security Policy objectives;
- learn about the impact of activities/policy initiatives and the evolving cyber policy and threat landscape in PNG; and
- provide a status Report to the Government with recommendations where required to improve implementation.