



REPUBLIC OF GHANA

MINISTRY OF COMMUNICATIONS

Ghana National Cyber Security Policy & Strategy

Final Draft

July 23 2015

Document Version

Version	Date	Remark
Ver. 1.0	March 2015	Final Draft handed over to Ministry of Communications
Ver. 2.0	7 September 2015	Final version after Validation Workshop

Document Contact

Table of Contents

EXECUTIVE SUMMARY 7

a. SECTION ONE: BACKGROUND 9

 I. CHALLENGES, DEVELOPMENTS WITH FOCUS ON THE POLICY 10

 i. Overview 10

 ii. Global Activities on Cyber Security..... 12

 iii. Regional Initiatives 13

 iv. Local Initiatives 14

 II. NEED FOR POLICY 15

 III. RELEVANT PROVISION – ICT4AD 17

b. SECTION TWO: CYBER SECURITY POLICY 18

 INTRODUCTION 19

 DEFINITIONS 19

 CNII SECTORS FOR GHANA..... 20

 POLICY CONTEXT 22

 I. POLICY STATEMENT 24

Legislative & Regulatory Framework..... 24

Cyber Security Technology Framework..... 24

Culture of security and Capacity Building..... 25

Research & Development towards Self-Reliance..... 25

Compliance and Enforcement..... 26

Child Online Protection..... 26

<i>Cyber Security Emergency Readiness</i>	26
<i>International Cooperation</i>	27
c. SECTION THREE: NATIONAL CYBER SECURITY STRATEGY	28
I. STRATEGIC ACTIONS FOR POLICY THRUST	29
i. Strategy Implementation Timelines	35
ii. Specific Initiatives.....	36
APPENDIX	37
National Cyber Security Policy Working Group.....	38
National Cyber Security Awareness Program	42
National Cyber Security Center (NCSC).....	46
National Cyber Security Council (NCSCC).....	50
National Cyber Security Crisis Management Plan (NCSCMP).....	53
National Computer Security Incidence Response Team (National CSIRT).....	56

GLOSSARY

AU	Africa Union
CCI	Commonwealth Cyber Initiative
CERT	Computer Emergency Response Team
CSIR	Council for Scientific and Industrial Research
CSIRT	Computer Security Incidence Response Team
CNII	Critical National Information Infrastructure
CID	Criminal Investigation Department
COP	Child Online Protection
EOCO	Economic and Organized Crime Office
ETA	Electronic Transactions Act
FIRST	Forum of Incident Response and Security Teams
GARNET	Ghanaian Academic and Research Network
ICT4AD	Information and Communication Technology for Accelerated Development
ITU	International telecommunications Union
IMPACT	Multilateral Partnership against Cyber Threat
ISOC/IEC	International Organization for Standardization / International Electrotechnical Commission
LI	Legislative Instrument

MDA	Ministries, Departments and Agencies
NCA	National Communications Authority
NITA	National Information Technology Agency
NitaCERT	NITA Computer Emergency Response Team
NCSAW	National Cyber Security Awareness Program
NCSC	National Cyber Security Center
NCSCC	National Cyber Security Council
NCSPWG	National Cyber Security Working Group
NCSCMP	National Cyber Security Crisis Management Plan
PKI	Public Key Infrastructure
R& D	Research and Development
SIM	Subscriber Identification Module
UNECA	United Nations Economic Commission for Africa
WG	Working Group

EXECUTIVE SUMMARY

The expansion of Internet access in Africa, representing the largest growth in the world, means more people today have access to Internet, with its attendant risks of attack from people with disruptive tendencies to defraud other Internet users and commit cybercrimes. These disruptive activities by cyber criminals has caused the debate on cyber security to be on the top of the agenda for almost every country, and many countries are strategizing on how to combat the cyber criminals. Several global initiatives are also addressing cyber crime and enhancement of cyber security. The ITU's IMPACT program is providing several member countries early warning on cyber crimes and is helping these member countries secure their cyber space. The Commonwealth Cyber Initiative (CCI) is another initiative that seeks to help commonwealth countries adopt efficient cyber security policies and Infrastructure.

At the continental level, the African (AU) has developed a cyber security convention which was ratified by African Presidents.

The cyber menace in Ghana has been more of cyber fraud. The popular "sakawa" where cyber criminals defraud unsuspecting Internet users of large sums of money in Ghana and abroad remains prevalent because of inadequate laws on cyber crime to prosecute cyber criminals. The Electronic Transaction Act (2008) has provisions for law enforcement agencies to fight cyber crime. However, this is not adequate for law enforcement in the fight against cyber crime as there are legal gaps caused by rapidly change in the cyber landscape. There is, however, the need to fully address all aspects of cyber security, and apply a multi-stakeholder approach to fighting the cyber menace. Several initiatives are on-going to address the cyber menace, all of which need to be brought under one umbrella for Ghana.

The Ministry of Communications, Ghana with the support of UN Economic Commission for Africa (UNECA) began a process in 2011 to review some aspects of Ghana's ICT for Accelerated Development (ICT4AD) policy to identify gaps as a result the changing ICT

landscape and recent developments in ICTs that were not originally envisaged and put in the document. Cyber security is one of the four thematic areas under this review and the national cyber security policy and strategy for Ghana has been developed. The policy has nine policy pillars and includes effective governance, legal framework, technology framework, response readiness and international cooperation.

Five special initiatives have been included in the first five year strategic plan. These initiatives includes establishment of institutional frameworks, creating awareness, ensuring coordination of cyber security initiatives and enforcement of cyber standards in Ghana. When fully implemented, Ghana will have a solid cyber security base framework to address its cyber needs.

a. SECTION ONE: BACKGROUND

I. CHALLENGES, DEVELOPMENTS WITH FOCUS ON THE POLICY

i. Overview

In recent times, Ghana has experienced a number of cyber attacks including defacing of a number of government websites by Internet hackers. These attacks have a denting effect on the cyber image of Ghana and are indications of security weakness of our cyber infrastructure and space. Cyber attacks have become very sophisticated and widespread and many countries are not only focusing on protecting their critical information infrastructure but also ensuring that there are very good incidence responds teams in place to respond to incidents cyber security incidents.

Since the turn of the century, we have seen a rapid growth of the Internet in Ghana. The growth has brought in its wake extensive cyber activities and subsequently attacks on various information infrastructure as well as cyber fraud popularly known as “Sakawa”. The biggest challenge is that the designated central point in the country where victims of “Sakawa” can report to at the Police CID Cybercrime Unit is not visible nationally and is under resourced. In cases when these incidences had been reported, it has taken many years to apprehend any suspect because of the lack of expertise in tracking these criminals using computers–based forensic skills. To make matters worse, when such cyber criminals were apprehended and processed to court, there are, more often, not enough legal basis to prosecute these criminal, as the legal system is inadequate to convict and punish cyber criminals. Consequently, Ghana’s image continues dwindle in cyberspace and is therefore considered as a cyber crime prone country.

For many years, cyber cafes have been the main source of Internet access, as many people could not afford the high cost of personal computers and Internet access and, as

a result of lack of operational guideline, cyber cafes have become fertile ground for cyber crime.

Ghana's mobile penetration stood at 115.64% as at the end of March 2015. The high mobile penetration has brought about an increase in mobile phone threats and fraud. The increased use of smart phones, especially with the introduction of M-commerce, is likely to bring more incidents like hackings and other attacks to mobile phone users. There is therefore a need to create awareness of risk of cyber attacks and exploitations for mobile users. As a result of mobile fraud, the National Communications Authority registered all SIM card in Ghana but there still remain high crime in the mobile space as cyber criminal continue to engage SIM Box fraud and other fraudulent activities.

Until recently, Ghana's Internet backbone and resources have been largely private sector driven. This result has been that many government officials send and receiving highly sensitive government information using free email services such Yahoo and Google making it vulnerable to information theft. However, since 2008, with the establishment of the National Information Technology Agency (NITA), Ghana embarked on a massive government network rollout to ensure efficiency in government operations and improved service delivery to citizens. . The result is that NITA now has Internet and Data services to all Ministries Departments and Agencies (MDAs) and has national datacenter facilities that enable NITA provide email and webhosting services under government designated second level domain (.gov.gh) NITA is also implementing the Public Key Infrastructure (PKI) and Digital Certificates to enhance secure communication within government. There is the need of a strong public private partnership in crafting our national cyber security policy to take care of the interests of the private and public sectors.

ii. Global Activities on Cyber Security

Cyber Security is central to the Information and knowledge economy. Countries which have high levels of networked computers and automation stand greater risks than countries with less developed networked computer infrastructure. As many countries with less developed network infrastructure strive to become a knowledge society, many network infrastructures will be rolled out with automation. This is evidenced in many African countries where over the last few years, massive submarine fiber optic cable Internet transit have landed on the shores and massive in-country fiber optic backbones are being rolled out. An increase in network computer infrastructure will bring a proportionate risk to critical information infrastructure.

For many years, many countries with high degree of networked computer infrastructure have been working around securing their critical information infrastructure and have developed cyber security policies and strategies to mitigate cyber incidences and crimes.

No one country control cyber space and everyone from anywhere in the world can access information from the Internet. It is therefore very important that countries put in place robust security around critical national information infrastructure and set up very swift response systems as risk of attacks cannot be eliminated. Additionally using an international approach of cooperation to secure cyber space and mitigate cyber crimes is also essential.

Many countries with high networked computer infrastructure and global companies already have Computer Security Incidents Response Teams (CSIRTs) in place where responses to cyber incidences are coordinated to mitigate the impact of cyber incidences. However in developing economies, very few CSIRTs have been setup,

although it is top of the agenda for many of these countries as networked computer infrastructure expands.

The International Telecommunication Union (ITU) through the International Multilateral Partnership against Cyber Threat (IMPACT) program has over the last few years played a leadership role in providing early warning systems and training cyber security experts around the world. Today, IMPACT has over 152 countries members. ITU has indeed developed a framework for developing countries to help them kick start a process of developing policies and strategy around cyber security.

Forum of Incident Response and Security Teams (FIRST Inc.) is a global forum of Computer Security Incidents Response Teams (CSIRTs). Membership to FIRST is by recommendation and through a rigorous standards process.

The Budapest Convention on Cyber Security which has been in force since 2004 was elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA. The Convention is open to any country which wants to participate. The convention is used as a guideline, reference standard or model law in more than 100 countries.

iii. Regional Initiatives

Governments in Africa today have moved the ICT discussion from infrastructure to cyber security. A decade ago, infrastructure was a major challenge to many African countries. Many countries have invested in massive in-country infrastructure and the connectivity and access challenge is waning. The networked computer infrastructure coming up in many African countries has opened up cyber space to many more citizens and accompanying this, the risk of using the Internet. A few countries like Tunisia, South Africa and Kenya already have a CERT in place. Many countries are also in the process

of developing cyber security policy and strategy (including formation of CERTs). In order to harmonize the development of cyber security policy and strategy, the Africa Union (AU) and the UN Economic Commission for Africa (UNECA) have developed a cyber security and cybercrime convention and has been ratified by African heads of States. Ratification of the convention, it can be argued, will foster regional cooperation in the fight against cyber crime.

In 2010, AfricaCERT was formed and have been undertaking capacity building program annually in different Africa countries on the establishment and management of CSIRTs for African countries.

iv. Local Initiatives

Today's society thrives virtually on using the Internet for communication and business. As networked computer infrastructure expands in the country, there is an increasing threat to business and communication.

Recent several cyber attacks on government websites in Ghana is a wake-up call for the development of a cyber security policy and strategy. Resolutions of cyber incidences have been uncoordinated and in many cases, there were no reporting structure put in place to guide in dealing with future attacks.

The National Information Technology Agency (NITA)'s concern of ensuring security of the government network initiated discussion amongst stakeholder in the Ministries, Departments and Agencies (MDAs) to setup a NITA Computer Emergency Response team (nitaCERT) to coordinate cyber incidences and assist in resolving future incidences within the government network.

The Ministry of Communication initiated the national Computer Emergency Response Team (CERT) project in 2013 in collaboration with the ITU-IMPACT. The national CERT was established in August 2014 is fully operational handling incidents and sending out early warning to its constituents. The National Security Council and many other institutions such as Ghanaian Academic and Research Network (GARNET) in academia are working on different projects towards securing cyberspace.

The SIM registration by NCA is another initiative to mitigate cyber crimes committed using mobile phones. The Ghana Police Service has also put in place the cybercrime Unit to alleviate cyber and other related crimes. The Economic and Organized Crime Office (EOCO) under the Attorney General's Department and Financial Intelligence Center for the financial sector are all government initiatives geared towards mitigating crime in general and computer crime in particular.

On the business side, the opening of an e-Crime Bureau in Ghana has greatly helped organizations investigate cyber crime thoroughly and improve protection of cyber space.

In spite all these initiatives, the fact still remains that there is a general lack of education on cyber security amongst the consuming public of ICT products and services which needs to be addressed.

II. NEED FOR POLICY

As Ghana strives to become an information and knowledge economy, there is an increased emphasis on informational activities and the information industry. Businesses will compete on information and computer systems will work efficiently on the right

information to produce the output required. It is becoming extremely necessary for nations to protect critical national information infrastructure to ensure national security in the wake of recent cyber wars, and ensure a safe cyber space to enable wealth creation for citizens. As networked computer infrastructure increases, there will be an increase in attacks on critical information infrastructure that is required to sustain the economy of the information and knowledge society. There is therefore an increasing need to protect critical national information infrastructure (CNII) and create a robust incidence response system when any attack is made on the CNII, to avoid loss of revenue due to down time and ensure national security.

The need to create a security culture by creating awareness of the enormous threats that users, especially children, of the Internet are exposed to must be addressed by a national cyber security policy. Awareness creation (education) of the risks users of the Internet are exposed and the vulnerabilities on our phones, computers and PDAs to can drastically reduce cyber incidences with its consequential loss of revenue when business are involved. This will create a very conducive environment in the information economy where Ghanaians can create wealth in peace without fear of harassment by cyber criminal and fraudsters.

Government business can be brought to a halt if the NITA infrastructure is attacked. In the same way, many businesses may grind to a halt if the infrastructure of ISPs and other public Internet and phone services are attacked. There is therefore the need to develop technical capacity of local technocrats to enable them manage the cyber security risks to government and private sector critical information infrastructure. In order to share knowledge on incidence response and ensure that there is a uniform risk management of all critical information infrastructures (both public and private), the policy

must address the need for a central coordinating body and work with a public private partnership model.

III. RELEVANT PROVISION – ICT4AD

Pillar 14 of the ICT4AD policy relates to Security Agencies using ICT to combat cybercrime. The pillar among other things places emphasis on capacity building, international cooperation and building infrastructure for security agencies to enable them use ICT to combat crime. Additionally, the pillar is to ensure that the legal text of the policy is up to date to help law enforcement agencies prosecute any cyber crime offenders.

The Electronic Transaction Act (ETA) 2008 has specific legislation on cyber crime and prescribes punishment for cyber crime perpetrators. The Act addresses issues on the fight against cyber crime.

The Data Protection Act which has been passed by the Parliament of Ghana ensures protection of private data of government, citizens and businesses in Ghana.

The Pillar 14 and the ETA fail to capture a holistic approach to securing the cyber space as a means of mitigating cyber incidences that may affect the ability of citizens to create wealth.

The several on-going initiatives which are not coordinated makes it impossible to know what different agencies of Government, academia and business are doing to enhance cyber security. A National Cyber Security framework covering policy and implementation strategy done holistically will ensure coordination and greatly enhance the national cyber security of Ghana.

b. SECTION TWO: CYBER SECURITY POLICY

INTRODUCTION

Ghana's determination to secure its cyber space is driven by a desire to ensure that our people are free from cyber attacks with devastating effects. This is informed by the fact that a people with a culture of cyber security achieved through awareness creation and capacity building are in a better position to handle cyber attacks as and when they occur. Our ability to identify and understand threats and how they can be handled reduces the number of actual attacks significantly and enhances the continuous operation of the national infrastructure on which critical information are held in the interest and security of the nation. We also recognize that the threat is not restricted only to government but also to operators who provide public services to citizens and private networks, thus the need for private public partnership.

DEFINITIONS

For the purpose of this policy document,

Critical National Information Infrastructure (CNII) may be defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on:

- **National economic strength**

Confidence that the nation's key growth area can successfully compete in global market while maintaining favorable standards of living.

- **National image**
Projection of national image towards enhancing stature and sphere of influence.
- **National defense and security**
Guarantee sovereignty and independence whilst maintaining internal security.
- **Government capability to functions**
Maintain order to perform and deliver minimum essential public services.
- **Public health and safety**
Delivering and managing optimal health care to the citizen.

CNII SECTORS FOR GHANA

Countries identify the CNII based on the level of networked computers and how attacks on them can affect factors mentioned above. For the purpose of policy as it relates to Ghana, the following sectors have been identified as CNII sectors:

1. National Defense and Security
2. Banking and Finance
3. Information and Communications
4. Energy
5. Transportation
6. Water
7. Health Services
8. Government
9. Emergency services

10. Food and Agriculture

VISION

A secure and stable connected Ghana with Internet users working and creating wealth in a safe cyber space, with a well-researched and trained academic and professional community protecting Ghana's cyber space equipped with global standards and responding swiftly to cyber incidents, and with up-to-date laws and systems in place to efficiently prosecute cyber criminals.

MISSION STATEMENT

To identify, analyze, address and remediate the immediate and potential cyber security threats posed on identified critical national information infrastructures (CNIIs) and put measures in place that will adequately regulate and secure the system infrastructures and meet the countries cyber security needs.

POLICY SCOPE

This policy covers all aspect of cyber security and national response including fight against cyber crime, creating public awareness, investment in education, scientific research, and development of cyber laws and legal measures, national security, , law enforcement and protection of critical national information infrastructures. (We can rephrase sentence)

POLICY CONTEXT

Ghana, like many developing economies faces the risk of cyber-attacks. Different uncoordinated initiatives are being put in place to secure the cyber space of Ghana. Many custodians of critical national information infrastructure are unaware of their roles in ensuring the maintenance of cyber security within the country. The driving force behind the national policy is the realization that a combination of persistent computer vulnerabilities and worldwide connectivity has placed the national critical information infrastructures at risks.

In Africa, Governments are discussing how to secure their cyberspace in the wake of heightened threats to national information infrastructure. Several national initiatives are taking place to ensure that legal systems are updated to enable proper persecution of cyber criminals.

The threat that cyber-attacks pose to African governments has prompted the African Union Commission to develop a convention at the regional level to harmonize the efforts of African countries in fighting cybercrime and ensuring cyber security.

The cyber security policy will address major cyber risks facing Ghana from attacks on the national information infrastructure. The policy seeks to address the lack of awareness of risks users and businesses face doing business in cyber space. The problem of “Sakawa” which has tagged as a haven of cyber fraudsters will be addressed by the policy. The policy also addresses the need to develop knowledge base, systems and technology framework for combating cyber-attacks and capacity building for cyber security expects to make Ghana self-sufficient in the fight against cybercrime and in the near future create a culture of cyber security in Ghana.

The National Cyber Security Policy (NCSP) seeks to address the risks to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors.

The policy recognizes the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets. It is being developed to ensure that the CNII are protected to a level that commensurate the risks faced.

The policy has been designed to facilitate Ghana's move towards a knowledge-based economy and will be based on a number of frameworks that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.

I. POLICY STATEMENT

Effective Governance

Government will centralize coordination of national cyber security initiatives and promote effective cooperation between public and private sectors. In order to sustain the gains from any initiatives, government will establish formal and encourage informal information sharing exchanges.

Legislative & Regulatory Framework

Government through the Attorney General's department set up a periodic process of reviewing and enhancing Ghana's laws relating to cyber space to address the dynamic nature of cyber security threats. In order to empower national law enforcement agencies to properly prosecute cyber security crimes, Government will establish progressive capacity building programs to acquire new skills and effective ways of enforcing cyber laws. Government will ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions.

Cyber Security Technology Framework

Policy measures will be put in place to develop a national cyber security technology framework that specifies cyber security requirement controls and baselines for CNII

elements. This will be accompanied will mechanism to implement an evaluation/certification program for cyber security product and systems.

Culture of security and Capacity Building

Government will invest every resource needed to develop, foster and maintain a national culture of security. As part of the process of development of culture of cyber security, government will support the standardization and coordination of cyber security awareness and education programmes across all elements of the CNII. Government will also:

- Establish an effective mechanism for cyber security knowledge dissemination at the national level
- Identify minimum requirements and qualifications for information security professionals

Research & Development towards Self-Reliance

In order for Ghana to become self-reliant in protecting the CNII to a level that is commensurate with the risk, Government will formalize the coordination and prioritization of cyber security research and development activities enlarge and strengthen the cyber security research community. Research and development will be encouraged by promoting the development and commercialization of intellectual properties, technologies and innovations through focused research and development. Government will also put measures in place to nurture the growth of cyber security industry.

Compliance and Enforcement

In order to ensure compliance and enforcement, policy measures and mechanism will be put in place to standardize cyber security systems across all elements of the CNII. Government will also strengthen the monitoring and enforcement of standards and develop a standard cyber security risk Management Framework.

Child Online Protection

Policy measures will be implemented through multi-stakeholder working by government industry, Civil Society, and relevant international child online protection agencies. Government will encourage dialogue at national and local levels to engage all concerned and create awareness of the possibilities and dangers of the Internet.

Cyber Security Emergency Readiness

To ensure cyber security emergency readiness, government together with all stakeholders will develop effective cyber security incident reporting mechanisms. This will include the development and strengthening of the national computer security incidence response team (CSIRT) and sector CSIRTs, dissemination of vulnerability advisories and threat warnings in a timely manner and the development of a standard business continuity management framework. The government will also encourage all elements of the CNII to monitor cyber security events and perform periodic vulnerability assessment programs.

International Cooperation

Policy measures will be put in place to encourage the active participation of Ghana in all relevant international cyber security bodies, panels and multi-national agencies. Government will make every effort to promote active participation in all relevant international cyber security activities by hosting an annual international cyber security conference.

c. SECTION THREE: NATIONAL CYBER SECURITY STRATEGY

FIRST 5 –YEAR CYBER SECURITY STRATEGIC PLAN (2016 – 2020)

For each policy thrust, specific strategic actions will be implemented under the first 5-year strategic plan. These actions may be implemented in isolation or in concert with other strategic actions from other policy thrusts.

I. STRATEGIC ACTIONS FOR POLICY THRUST

Action Item	Policy Thrust	Action Plan	Policy Drivers	Collaborators
1.	Effective Governance	<p>1. Government will set up cyber security institutions and put in place governance structure to ensure long-term sustenance of Cyber Security activity including information exchange. Action will be taken as collaboration of government, business and civil society (public private partnership Institutions). The institutions to be setup include:</p> <ol style="list-style-type: none"> 1. National Cyber Security Council 2. National Cyber Security Center 3. National Computer Security Incidence Response Team (CSIRT) 4. National Cyber Security Policy Working Group 	Ministry of Communications,	National Security Council, NITA, NCA, Attorney General
2.	Legislative and Regulatory Framework	<p>1. Government will set up Cyber Law Review Committee under the Attorney General's Department to do</p>	Attorney General's Department,	Ministry of Communication, Ministry of

		<p>a study on the laws of Ghana to accommodate legal challenges in the cyber environment and child online protection and review every three year</p> <p>Stage 1: identifications of issues in the cyber environment</p> <p>Stage 2. Review current laws on cyber environment</p> <p>Stage 3. Make recommendations for amendment of national laws</p>		Interior,
3.	Cyber Security Technology Framework	<ol style="list-style-type: none"> 1. Government in collaboration with key stakeholders will review and adopt international information / cyber security standards such as ISO/IEC 27000 series, NIST, etc to increase robustness of CNII sectors and ensure safety in cyberspace for all 2. Government and its partners will also expand the national certification scheme for information security management & assurance. 3. A standardized Digital Forensics Investigations Standards and Model will be developed that will be used by the academia to teach students, train law enforcement agencies and to be used by the lawyers and expert witnesses in cybercrime cases. 4. Setup professional strong association such as Digital Forensics 	NITA	Professional Security Associations, Standards Organizations, Universities and Professional Certification Centers

		Association of Ghana		
4.	Culture of Cyber Security & Capacity Building	<ol style="list-style-type: none"> 1. Efforts will be made to reduce number of Information/cyber security incidents through improved awareness creations & online skill development for all stakeholders including children by developing a National Cyber Security Awareness program and portal targeted at all stakeholders by content providers using different packaging for different demographics. 2. Capacity will be built through an increased certification course on information and cyber security to prepare Ghana for self-reliance in cyber security. 3. Targeted capacity building will be implemented for law enforcement on cyber investigation and enforcement to improve prosecution of cyber crime in Ghana. 	Ministry of Communications,	Non-governmental Organizations, Universities, Professional Certification Centers Cyber businesses
5.	Research & Development towards Self-Reliance	<ol style="list-style-type: none"> 1. A National R&D roadmap for Cyber Security will be developed to ensure that Ghana will be self sufficient attending to its cyber security needs. 2. Technologies relevant & desirable for CNII will be developed. 3. Domain competency development will be provided for: <ol style="list-style-type: none"> 3.1. Natural growth of Cyber Security Industry 	Ministry of Communications,	Ministry of Education, Universities, Council for Scientific and Industrial Research (CSIR), Professional Certification

		3.2. Updating R&D roadmap regularly 4. Build Research Labs at Universities		Centers, NITA,
6.	Compliance & Enforcement	1. A national Risk Management framework for CNII will be developed to ensure a uniform framework for all CNII.	Ministry of Communications	NITA, NCA, Ministry of Environment, Science & technology, Professional IT Security Bodies, Private Sector (Finance, Network Operators), Research and Education Network
7.	Cyber Security Emergency Readiness	1. A framework for mitigation of risk of cyber attacks and ensuring structures for swift responses to attacks that threaten national security through: <ul style="list-style-type: none"> • Setup of National Cyber Crises management Committee (under National Cyber security council) • Positioning National and sector CSIRTs in the line of responding to emergencies • Setup of National Cyber Crises Management WG continuously reviewing structures and making recommendations to be acted on by committee 2. Organize Hacking Workshops to	Ministry of Communications	National Security Council, Private Sector (Financial, Operators), Ministry of Interior, NITA

		exploit systems and identify vulnerabilities		
8.	Child Online Protection	<p>Develop a framework for the protection of children as they engage with the Internet which ensures that agencies and stakeholders work together to address children’s online risk by</p> <ol style="list-style-type: none"> 1. Ensuring that Organizational Structures put in place for <ul style="list-style-type: none"> • A Monitoring Framework • Technical and Procedural Measures for working with all stakeholders 2. Capacity Building – Awareness raising and public education. 3. Legal Measures 4. Implementation and International Cooperation 	Ministry of Communications	Ministry of Gender, Children and Social Protection; Ministry of Interior, Ministry of Educations
9.	International Cooperation	Ghana will engage in relevant international cyber security and child online protection meetings and prioritize engagement and join or sign International/regional conventions	Ministry of Foreign Affairs.	Ministry of Communications, National Security Council, Ministry of Interior, Ministry of Gender and Child and Social Protection

i. Strategy Implementation Timelines

The policy will be implemented in three stages:

STRATEGY	TIMELINE	ACTIVITIES
Short Term	Year 1 -2	<p>Identifying CNII and addressing immediate Concerns – Identify CNII, analyze vulnerabilities and put in place stop gap measures while setting up institutional structures and creating public awareness</p>
		<p>The short term will focus on following policy thrust:</p> <p><i>Effective governance</i></p> <ul style="list-style-type: none"> - Implement Action 4 to assist ministry of communications and other stakeholders put in place a stop gap measure to identify CNII, evaluate vulnerabilities and develop measures to address immediate concerns. - Begin building institution by implementing Actions 1 - 3 <p><i>Culture of Cyber Security</i></p> <ul style="list-style-type: none"> - Implement Action 2 to begin awareness creation <p><i>Cyber Security Emergency Readiness</i></p> <ul style="list-style-type: none"> - Implement Action 1 to develop framework <p><i>Child Online Protection</i> Develop framework for engaging with all stakeholders</p> <ul style="list-style-type: none"> •Coordinate with local universities or existing entities to help with the expertise. •Set up the COP stakeholder Committee to serve as the leading expert group advising the national Government on the formulation and implementation of a national COP plan for the Ghana. (Other actions stipulated in the Ghana COP strategy)
Medium Term	Year 3 - 4	<p>Building the infrastructure - Setting-up the necessary systems, process, standards and institutional arrangements (mechanisms) and building</p>

		capacity amongst researchers and information security professionals
		<p>The medium term will focus on following policy thrust:</p> <p><i>Culture of Cyber Security & Capacity Building</i></p> <ul style="list-style-type: none"> - Implement Action 1 <p><i>Research & Development towards Self-Reliance</i></p> <ul style="list-style-type: none"> - Implement Actions 1 - 2 and accompanying infrastructure <p><i>Compliance and enforcement</i></p> <ul style="list-style-type: none"> - Implement Action 1 and accompanying infrastructure <p><i>Legislative and Regulatory Framework</i></p> <ul style="list-style-type: none"> - Implement Action 1
Long Term	Year 5+	<p>Developing self-reliance - in terms of technology as well as professionals, monitoring the mechanisms for compliance, evaluating and improving the mechanisms and creating the culture of cyber security</p>
		<p>The long term strategy will focus on following policy thrust:</p> <p><i>Cyber Security Technology Framework</i></p> <ul style="list-style-type: none"> - Continuous review and improvement <p><i>Compliance & Enforcement</i></p> <ul style="list-style-type: none"> - Enforcing adopted Risk Management framework within CNII for compliance <p><i>Culture of cyber security</i></p> <ul style="list-style-type: none"> - Continuous awareness creation

ii. Specific Initiatives

Details of Specific initiatives including strategic objectives, estimated cost and drivers are attached in the appendix.

APPENDIX

TECHNICAL PROPOSAL
APPENDIX -1

(STRUCTURING THE IMPLEMENTATION STRATEGY PROGRAMS AND INITIATIVE)

The Implementation Strategy: Programs and Initiatives	
Title of Program/Initiative	National Cyber Security Policy Working Group
Program /Initiative Strategic Objective	<ul style="list-style-type: none"> • To assist MoC to collate all cyber security initiatives • To identify critical national information infrastructure in sectors as defined by the policy • To support policy drivers to setup structures for medium term strategy • To design and implement a comprehensive National Cyber Security Awareness program
Relevant Achievable National ICT4D Policy Objective & Goals	National Security, Law and order and enhanced cyber Security
Background to Program /Initiative	In order to have continuous activity on the Cyber security policy and strategy, it is proposed that the current Adhoc technical

	committee for cyber security be converted to a Working Group (WG) to keep the momentum of the cyber security agenda to ensure a quick implementation of the policy and strategy.
Description of Program/Initiative	The National Cyber Security Policy WG (NSCPWG) will be made up of current policy drafting Adhoc technical committee which composition represent a public private collaboration and by virtue of the selection of the members, also represent a bottom-up approach. New members may be added to overcome any shortfall in skill such as legal expertise in the conversion from the Adhoc Technical Committee to the Working Group. The NSCPWG will assist the Ministry of Communication to establish recommended specific programs that require immediate attention such as the awareness campaign for the first year of the policy.
Program/Initiative Implementation Rationale	The rationale for the setting up of WG is to avoid any vacuum between the adoption of the policy and the implementation of the long term structures of the policy as well as begin a process of awareness creation.
Program/Initiative Implementation Specific Goals	<ul style="list-style-type: none"> • Support implementing agency to begin actual implementation of strategy • Develop a National Awareness Creation Program on Cyber Security, including the creation of National Cyber Security Awareness portal • Assisting policy implementing agencies to build the structures for the achievement of long term goals
Program/Initiative Timeframe	One year in active engagement with policy implementation (may be extended if necessary) but will continue in advisory role after first year
Program/Initiatives Deliverables and Target	

Program/Initiative Deliverables	Time –Bound Measurable (TBM) Target
National Cyber Security Awareness Program (NCSAP)	3-months form policy adoption
National Cyber Security Awareness Portal (NCSP)	6-months from adoption of policy
Identification of Critical National Information Infrastructure as prescribed by the Policy (CNII) and immediate concerns.	12- Months from adoption of policy
Program /Initiative: Output, Outcome and Beneficiaries and Estimated Cost	
NCSAP	Document detailing awareness program including, workshops, media activities, online activities etc. and budget. The outcome of program will be well informed professionals and citizens on threats in cyberspace and how they can guard against these threats. The main beneficiaries will be government security professional, citizens and businesses in Ghana.
NCSP	Oversee the creation of Interactive Portal with all relevant information, downloads and support where citizens can report incidences, seek support and receive updates of latest cyber security information. Outcomes will include a one stop shop for citizens and business to find everything on cyber security. The main beneficiaries are the citizenry, government and businesses in Ghana.
CNII	Oversee investigative work to determine the National Information Infrastructure and determine critical ones based on policy documents. NCSPWG will assist in selecting consultants to do exercise. The outcome will be a document with all details of CNII as it is today and expansion plans for next five years. The main beneficiary is Government of Ghana.
	Members of NCSWG must be rewarded for role for the period when

COST	they are actively involved in implementation. This must include a seating allowance and expenses cover for any activity performed. If WG meets monthly, estimated Budget of GHC100,000.00 per year (seating allowance+ meals + venue) (In order to get the buy-in from any entity in support of this plan, it will be appropriate to state programme related costs as well or we simply refer to this budget as OVERHEADS.)	
Project Implementation Management, Monitoring and Evaluation		
Supporting Implementation Agencies and their Assignment Responsibilities	Supporting Implementation Agency	Assigned Responsibility
	Ministry of Communications	Oversight of NCSWG, project funding / monitoring and evaluation
	National Security Council	Technical/security input for defining CNII and security advisory for creation of new cyber security structure
	National Information Technology Agency/ National Communication Authority	Technical advisory and guide on collating CNII, web portal
Program /Initiative Critical Success Factors	Commitment of members to work to implement policy, motivation of WG members	
Program/Initiative Implementation Risk Factors	Inactivity of WG members or lack of needed support form Ministry of Communications	
Additional Comments and Remarks		
Non		

TECHNICAL PROPOSAL

APPENDIX – 2

(STRUCTURING THE IMPLEMENTATION STRATEGY PROGRAMS AND INTIATIVE)

The Implementation Strategy: Programs and Initiatives	
Title of Program/Initiative	National Cyber Security Awareness Program
Program /Initiative Strategic Objective	<ul style="list-style-type: none"> • To define Security Awareness Goals and Objectives • To identify Intended Audience (Stakeholders, General Public) • To define Topics to be covered • Identify Current Training Needs • To obtain Support • To establish Security Policy • To define Delivery Methods to be used • To develop a Strategy for Implementation • To design Awareness Strategy • To design Training Strategy • To develop Evaluation Methods • To create a National Awareness portal
Relevant Achievable National ICT4D Policy Objective & Goals	Culture of Cyber Security, Awareness creation
Background to Program /Initiative	The National Cyber Security Awareness Program shall be used to stimulate, motivate, and remind the audience what is

	expected of them.
Description of Program/Initiative	The National Cyber Security Awareness Program is a program to train different stakeholders on different aspects of cyber security with the intent of helping them provide a reasonable security consummate with the risks to avoid incidences of cyber attacks. This will take the form of identification ..., need assessment, training and evaluation of different sets of stakeholders. The program will include a cyber security awareness portal that will establish a permanent awareness campaign on the internet
Program/Initiative Implementation Rationale	The rationale for the setting up the Awareness Campaign is that an informed community is able to foresee any possible attack and take appropriate preventive measure to overcome such attacks. The campaign will be targeted at main stakeholders and the general public to help develop culture of cyber security.
Program/Initiative Implementation Specific Goals	<ul style="list-style-type: none"> • To develop a level of awareness in the community to mitigate risk of cyber attacks by workshops, mass media and other awareness programs • To develop a national awareness portal for easy access to information on cyber security and easy downloads for quick fixes
Program/Initiative Time-Frame	On-going program. In the first year, it is proposed that the National Cyber Security Policy WG begin work on the program and hand over to the emerging organization that will be responsible for ensuring that the country attains a level of awareness to mitigate cyber incidences.
Program/Initiatives Deliverables and Target	
Program/Initiative Deliverables	Time –Bound Measurable (TBM) Target

Detailed Awareness Program Time table	3-months from Policy Adoption	
National Cyber Security Awareness Portal	6-months from adoption of policy	
Start of Delivery of Holistic Awareness program	12 Months from adoption of policy	
Program /Initiative: Output, Outcome and Beneficiaries and Estimated Cost		
National Cyber Security Awareness Program	<p>Informed stakeholders and public. Outcome in substantial reduction in cyber incidences and crimes. Citizens and business in Ghana can work in emerging information economy in peace to create worth.</p> <p>Internet users in Ghana should Know how get themselves a basic level of protection against threats online</p> <p>Estimated cost of entire program for 5 years will be about GHC2.5m for year one. Annual budget of about GHC500, 000.00</p>	
National Cyber Security Awareness Portal	<p>One stop shop cyber security alerts, quick downloads and information on emerging threats. Interactive portal where questions can be asked through web 2.0 applications. Outcome will be informed community.</p> <p>Estimated cost of portal creation and maintenance for year one is GHC20,000.00 Subsequent year may be down to less than GHC10,000.00</p>	
Project Implementation Management, Monitoring and Evaluation		
	Supporting Implementation Agency	Assigned Responsibility
Supporting Implementation Agencies and their Assignment Responsibilities	Ministry of Communication & National Cyber Security Policy WG (year one). National Cyber Security Council and Center to take over by end of year 2	Oversight of program; funding, monitoring and evaluation (Capacity building after year 2)
	National Information Technology Agency/ National	Technical advisory and guide on web portal development. Capacity

	Communication Authority	building for year one
	Ministry of Information	Support the awareness creation programs
Program /Initiative Critical Success Factors	Availability of Funding Commitment of supporting agencies	
Program/Initiative Implementation Risk Factors	Lack of funds and commitment to implement portal	
Additional Comments and Remarks		

TECHNICAL PROPOSAL

APPENDIX -3

(STRUCTURING THE IMPLEMENTATION STRATEGY PROGRAMS AND INITIATIVE)

The Implementation Strategy: Programs and Initiatives	
Title of Program/Initiative	National Cyber Security Center (NCSC)
Program /Initiative Strategic Objective	<p>Strategic Objective of NCSC are :</p> <ul style="list-style-type: none"> • National Cyber Security Policy Implementation: Defines, communicates and updates (when necessary) the national cyber security programs to all the CNII. • National Coordination: Closely coordinates cyber security initiatives of various key Agencies and organizations in Ghana. • Outreach: Promote and facilities formal and informal mechanism for information sharing across the CNII. This includes promoting cyber security awareness, training and education programs to grow the competency of information security professionals and the industry as a whole. • Compliance Monitoring: Facilities the monitoring of compliance to cyber security policies and standards across the CNII. • Risk management: Assesses, identifies and manages cyber security threats exploiting vulnerabilities and risks across the CNII • Assist the National Cyber Security Council in all its function activities and help industry to test its emergency plans • Contribute to application of international standards on

	cyber security as well as on accreditation and certification of ICT infrastructure, services and suppliers.
Relevant Achievable National ICT4D Policy Objective & Goals	Effective Governance of National Cyber Security Policy
Background to Program /Initiative	The NCSC is part of the proposed institutional structure to be created to sustain the cyber security policy in the long term.
Description of Program/Initiative	<p>The Ghana Cyber Security Centre is envisioned to become a one-stop coordination centre for national cyber security initiatives by adopting a coordinated and focused approach, with the key objective of strengthening the country's cyber security arena.</p> <p>The centre will be under the purview of the Ministry of Communications, and overseen by the National Cyber Security Council for policy direction and the National Security Council in times of national crisis.</p>
Program/Initiative Implementation Rationale	The rationale for the setting up the NCSC is the help establish and institutional approach to coordinating the policies of CNII sectors to ensure that the risks of attack are at the barest minimum and disaster recovery and business continuity processes put in place to take care of any eventual breach. It will also spearhead all awareness and education activities on Cyber security after creation.
Program/Initiative Implementation Specific Goals	<ul style="list-style-type: none"> - To make Ghana a safe destination for cyber activity - To boost national image in its sphere of influence and make it a leader in the region - To ensure that Ghana has technical skill to maintain low level of risk that will be achieved
Program/Initiative time frame	To be set up within first two years.

Program/Initiatives Deliverables and Target		
Program/Initiative Deliverables	Time-Bound Measurable (TBM) Target	
Creation of Structures and function of NCSC	By 6 months from Adoption of the policy	
Legal framework for establishment passed	By 12 months from the adoption of the policy	
Financial Sourcing & Establishment of NCSC	By 18 months from adoption of policy	
Program /Initiative: Output, Outcome and Beneficiaries and Estimated Cost		
NCSC	Center for operational coordination of all cyber initiatives and continuously creating culture of cyber security	
Project Implementation Management, Monitoring and Evaluation		
	Supporting Implementation Agency	Assigned Responsibility
Supporting Implementation Agencies and their Assignment Responsibilities	Ministry of Communications NCSPWG	Developing structures, paper work for legal establishment, sourcing funding for its establishment
	National Security Council, National Cyber Security Council (NCSCC)	Establishment of physical infrastructure to operationalize Center, oversee operations of Center after establishment
Program /Initiative Critical	Legislative approval of initiative	

Success Factors	Funding of initiative by GOG and/or development partners
Program/Initiative Implementation Risk Factors	Delay in passing necessary legislative instruments Lack of funding
Additional Comments and Remarks	
Non	

TECHNICAL PROPOSAL
APPENDIX -4

(STRUCTURING THE IMPLEMENTATION STRATEGY PROGRAMS AND INTIATIVE)

The Implementation Strategy: Programs and Initiatives	
Title of Program/Initiative	National Cyber Security Council (NCSCC)
Program /Initiative Strategic Objective	<p>Strategic objective of NCSC are :</p> <ul style="list-style-type: none"> • To oversee the national cyber security policy and strategy; • To identify National cyber security priorities and initiatives • To coordinate cyber security measures at the national level • To help foster public-private relations required to address cyber security issues • To collaborate with government agencies, security services, general directorate for security etc for the purpose of establishing standards and uniform investigative procedures and development of institutional consensus • To collaborate with the structures responsible application of the law at regional and International level • To coordination of measures and development of digital identity systems as well as management and best practice in digital identity • To development of standards training and capacity building programs for agencies and the creation of a national platform for the purpose of coordinating

	technical assistance and training initiatives at the international level
Relevant Achievable National ICT4D Policy Objective & Goals	Cyber Security and fight against cyber crime
Background to Program /Initiative	The NCSCC is part of the proposed institutional structure to be created to sustain the cyber security policy in the long term.
Description of Program/Initiative	The NCSCC shall be formed to serve as the high-level liaison center for cyber security and shall be responsible for adopting or approving the policies put forward for implementation of the function center to be known as the National Cyber Security Center. The council shall be chaired by the Vice-President of Ghana.
Program/Initiative Implementation Rationale	The rationale for the setting up the NCSCC is to serve as the high level governance institution overseeing all issues on cyber security.
Program/Initiative Implementation Specific Goals	<ul style="list-style-type: none"> - To ensure that appropriate policies are in place to make Ghana a safe destination for cyber activity - To boost national image in its sphere of influence and make it a leader in the region - To ensure Ghana is part international conventions and is playing its role as a leader in the region
Program/Initiative Time-Frame	To set up within two years
Program/Initiatives Deliverables and Target	
Program/Initiative Deliverables	Time-Bound Measurable (TBM) Target
Creation of Structures and function of NCSCC	By 6 months from Adoption of the policy
	By 12 months from the adoption of the policy

Legal framework for establishment passed		
Financial Sourcing & Establishment of NCSCC	By 18 months from adoption of policy	
Program /Initiative: Output, Outcome and Beneficiaries and Estimated Cost		
NCSCC	Governance institution with full oversight of policy and ensuring full implementation of policy after its creation	
Project Implementation Management, Monitoring and Evaluation		
	Supporting Implementation Agency	Assigned Responsibility
Supporting Implementation Agencies and their Assignment Responsibilities	Ministry of Communications, NCSPWG	Developing structures, paper work for legal establishment, sourcing funding for its establishment
	National Security Council,	Establishment of physical infrastructure to operationalize council, Oversee operations of council after establishment
Program /Initiative Critical Success Factors	Legislative approval for establishment Funding	
Program/Initiative Implementation Risk Factors	Delay or no approval of LI Lack of funding	
Additional Comments and Remarks		

TECHNICAL PROPOSAL
APPENDIX -5

(STRUCTURING THE IMPLEMENTATION STRATEGY PROGRAMS AND INITIATIVE)

The Implementation Strategy: Programs and Initiatives	
Title of Program/Initiative	National Cyber Security Crisis Management Plan (NCSCMP)
Program /Initiative Strategic Objective	<p>Strategic Objective of NCSCMP are :</p> <ul style="list-style-type: none"> • To increase preparedness of country against cyber attacks • To enhance capability to respond to cyber security issues • To provide coordinated effort in handling cyber attacks • to minimize impact to socio – economic activities
Relevant Achievable National ICT4D Policy Objective & Goals	Cyber Security Emergency Readiness
Background to Program /Initiative	The NCSCMP was conceived to ensure that a coordinated swift response is made to any cyber incidences having a bearing on national security.
Description of Program/Initiative	A framework that outlines strategy for cyber attack mitigation and coordination amongst Ghanaian CNIIs through public and private collaboration
Program/Initiative Implementation Rationale	Rational for implementing this initiative to ensure the country's prepared to react to any cyber security emergency. The plan envisages a management committee which will under the council where ultimate decision are made on any major attacks and a working group created in as Public Private Partnership (PPP) and having membership from the center, the national

	CSIRT, CNII sectors and any related agencies to enforce any tactic adopted for resolving any major attacks.
Program/Initiative Implementation Specific Goals	<ul style="list-style-type: none"> - Help Ghana maintain a level of readiness to react to any major attacks - Ensure swift response to any major attacks by ensuring that decision making structures are in place and working smoothly - Ensure that all CNII's maintain their own emergency plan and test it from time to time.
Program/Initiative Time-Frame	Come into place when NCSC, NCSCC and National CSIRT have all been formed and in place. Time frame will be about 24 months from the adoption of this policy
Program/Initiatives Deliverables and Target	
Program/Initiative Deliverables	Time –Bound Measurable (TBM) Target
National Cyber Crises management Committee	6 months from the setup of NCSC, NCSCC and National CSIRT
National Cyber Crises management WG	6 months from the setup of NCSC, NCSCC and National CSIRT
National Cyber Crises management Plan	12 Months from the setup of NCSC, NCSCC and National CSIRT
Program /Initiative: Output, Outcome and Beneficiaries and Estimated Cost	
National Cyber Crises management Committee	Decision making body at the national level for cyber attacks of with national security implications
National Cyber Crises management WG	Implementation coordination of major cyber attacks that has national security implications
National Cyber Crises management Plan	Procedures for decision making and implementation of actions during cyber emergency

Project Implementation Management, Monitoring and Evaluation		
	Supporting Implementation Agency	Assigned Responsibility
Supporting Implementation Agencies and their Assignment Responsibilities	National Security Council, National Cyber Security Council	Oversee formation of crises management committee and its workings
	National Cyber Security Center, National CERT, NITA, CNII Sectors	Setup of Working Group
Program /Initiative Critical Success Factors	Setup of National Cyber Security council Setup of National and sector CSIRTs	
Program/Initiative Implementation Risk Factors	Delay in setting up structures prescribe by policy	
Additional Comments and Remarks		

TECHNICAL PROPOSAL
APPENDIX -6

(STRUCTURING THE IMPLEMENTATION STRATEGY PROGRAMS AND INITIATIVE)

The Implementation Strategy: Programs and Initiatives	
Title of Program/Initiative	National Computer Security Incidence Response Team (National CSIRT)
Program /Initiative Strategic Objective	Strategic Objective of National CSIRT are : <ul style="list-style-type: none"> • To provide reactive and proactive services, • To communicate timely information on relevant threats, whenever necessary, bringing their assistance to bear for response to incidents
Relevant Achievable National ICT4D Policy Objective & Goals	Cyber Security Emergency Preparedness
Background to Program /Initiative	
Description of Program/Initiative	The Ghana National Computer Security Incidence Response Team is to be established to take charge of the national information infrastructure protection actions and serve as a base for national coordination to respond to ICT security threats at regional and international level. The nation cert shall be empowered to execute the following minimum services.
Program/Initiative Implementation Rationale	The rationale for the setting up the NCERT will be to ...
Program/Initiative Implementation Specific Goals	National CSIRT will be created to perform the following tasks: <ul style="list-style-type: none"> ▪ Reactive services: early warning and precaution notice, incidents processing, incidents analysis, incident response

	<p>facility, incidents response coordination, incident response on the web, vulnerability treatment, vulnerability analysis, and vulnerability response and vulnerability response coordination;</p> <ul style="list-style-type: none"> ▪ Proactive services: public notice, technological surveillance, security audit and assessment, security installations and maintenance, security tools development, intrusion detection services and security information dissemination, etc; and ▪ Artifacts treatment: artifacts analysis, response to artifacts, coordination of response to artifacts, risk analysis, continuation and resumption of activities after disaster, security consultation and sensitization campaign, education/training and product appraisal or certification.
Program/Initiative Time-Frame	Should be in place in 18 months from the adoption of the policy
Program/Initiatives Deliverables and Target	
Program/Initiative Deliverables	Time –Bound Measurable (TBM) Target
National CSIRT institution	6 – months from approval of Policy
Laboratories, early warning system	12 –months from approval of policy
Full operational capacity	18 - Months from approval of policy
Program /Initiative: Output, Outcome and Beneficiaries and Estimated Cost	
National CSIRT	Fully functional CSIRT with well trained staff and fully equipped laboratories responding to cyber threats and maintain risk to the CNII

	at a reasonable level	
Project Implementation Management, Monitoring and Evaluation		
Supporting Implementation Agencies and their Assignment Responsibilities	Supporting Implementation Agency	Assigned Responsibility
	Ministry of Communications with support of CCI	Development of institutional structures of National CSIRT
	National Security Council	Support implementation by making security input and requirements definition
	National Information Technology Agency/ National Communication Authority	Provide technical support for implementation of National CERT
Program /Initiative Critical Success Factors	Agreement on Support of CCI Willingness of MOC to implement initiative	
Program/Initiative Implementation Risk Factors	No drive from MOC No agreement with CCI	
Additional Comments and Remarks		