REPUBLIC OF GHANA

MINISTRY OF COMMUNICATIONS

Ghana National Cyber Security Policy & Strategy

Final Draft

March 2014

Document Contact

Table of Contents

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
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

In the early 2000's, the focus of ICTs in Africa was on expanding Internet access. With the advent of submarine fiber optics Internet transit, countries within the Africa region have access to high speed broadband at reasonable prices. The focus on access today is the rollout of terrestrial fiber optics backbone in countries.

The availability of Internet access means more people today have access to Internet. The expansion of Internet access has brought with it risks of attack from person with disruptive tendencies to dupe other Internet users and commit cybercrimes. These disruptive activities by cyber criminal has cause the debate on cyber security to be on the top of the agenda for almost every African country and many countries are planning strategies to combat the cyber criminals. Several Global activities are taking place around the fight against cyber criminals and cyber security. The ITU's IMPACT program is providing several member countries early warning systems 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 policy and Infrastructure. At the African regional level, the AU developed a cyber security convention which was ratified by African heads of states last year.

The cyber menace in Ghana had been more of cyber fraud. The popular "Sakawa" menace where cyber criminals tend to dupe unsuspecting Internet users from Ghana and abroad of large sums of money remain prevalent because inadequate laws on cyber crime which does not help law enforcement properly prosecute cyber criminals. The Electronic Transaction Act (2008), however, has provisions for law enforcement to fight against cyber crime. However this not adequate and does not address fully all aspects of cyber security, especially the multi-stakeholder approach to fighting the cyber menace. Several initiatives are on going to address the cyber menace and needs 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 Ghana's ICT for accelerated Development (ICT4AD) policy document to include recent developments in ICTs that was not originally included in the document. Cyber Security is one of the four thematic areas under this review

and the ministry has appointed an Adhoc technical committee and a resource person to develop a national cyber security policy and strategy for Ghana. This document is the report submitted by the Adhoc committee on cyber security which outlines the proposed policy and implementation strategy with specific initiatives to get enforcement of cyber security up and running in Ghana.

a. SECTION ONE: BACKGROUND

I. CHALLENGES, DEVELOPMENTS WITH FOCUS OF THE POLICY

i. Overview

Ghana has had a number of websites defaced by hackers in recent times. The most recent one being Ghana’s official web portal. Very important websites like the website of National Communication Authority, the National Information Technology Agency (NITA) and the website of the vice president of Ghana have all being defaced in recent past. These attacks have indented the national image of Ghana and indicated a security weakness of our cyber infrastructure and space.

Since the turn of the century, we have seen the high growth of the Internet in Ghana. The growth has brought along cyber attacks on various information infrastructure as well as cyber fraud perpetuated by criminally-minded persons popularly known as “Sakawa”. The biggest problem is that victims of “Sakawa” and other cyber fraud activities had often not found an advertised central point in the country to report the incidences. Even when these incidences had been reported to the Ghana Police Criminal Investigation Department (CID), it has taken many years to apprehend any suspect because of the lack of know-how on tracing these criminal using computers –based investigative skills. Worse of it all, when such cyber criminal were apprehended and processed to court, there were no sufficient legal bases to prosecute these criminal as the legal system was not up to date to convict and punish cyber criminals resulting in Ghana’s image been dented as a cyber crime pronged location.

For many years, cyber cafes have been the main source of Internet access as many could not afford the high cost of obtaining personal Internet access. However, with the advent of high speed mobile Internet access via 2.5 to 3.5G modems, many of the cyber fraud perpetuators are shifting their operations from the cyber cafes to working from their home and obscure places that are not easily accessible. The cyber cafes are still used by many cyber fraudsters because the cyber cafe business in Ghana is not regulated and there are not specific rules guiding their operations.

Ghana’s mobile penetration today stands at over 92% as at July 2012. The high mobile penetration has brought about an increase in mobile phone threats and fraud. A few years ago, there were calls from an anonymous caller who started rumors of an impending earthquake which caused panic and threatened national security. The Ministry of Communications through the National Communications Authority reacted swift to mobile phone threats by announcing SIM card registrations which ended recently bringing some sanity to mobile security.

Until recently, Ghana’s Internet backbone and resources have been largely private sector driven. Since the advent of Internet in Ghana in the early 90s, the National Communications Authority has registered over 100 Internet and data service operators. Government agencies have to buy services from private Internet service operators which run most of the critical information infrastructure. The result was highly sensitive government agencies using free email services like Yahoo and Google which expose these agencies to risk of exposure of sensitive government information. However, since 2008, Ghana has embarked on a massive government network rollout to bring about efficiency in government operations and citizens engagement through eServices. The first phase of the eGovernment network project has been completed and handed over to the National Information Technology Agency which has since July 2011 provided Internet and Data services to over 100 Ministries Departments and Agencies (MDAs) The includes project includes a national datacenter which will become the repository of all government records and information. The Datacenter has enable NITA to provide email and webhosting services under government designated second level domain (.gov.gh) and all MDAs are expected to migrate to the platform in the near future to ensure security of Government sensitive information. NITA is implementing the Public Key Infrastructure (PKI) and Digital Certificates to enhance secure communication within government. NITA’s eGovernment network has become critical information infrastructures which when attacked can adversely affect functioning of government and will dent the cyber image of Ghana.

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 the least developed networked computer infrastructure. As many countries with leased 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, we have seen massive submarine fiber optic cable Internet transit land on the shores and the massive in-country fiber optic back bones being rollout. An increase in network computer infrastructure will bring a proportionate risk to critical information infrastructure.

Since the year 2000, several countries with high levels of networked computers infrastructure been working around securing their critical information infrastructure and have developed cyber security policies and strategies to mitigate cyber incidences and crimes. The United States of America for instance recently revised its policy and strategy to meet high incidences of cyber attacks and increasing threats of cyber war.

Every cyber citizen (people in cyberspace) has a right to lawfully access to information from around the globe irrespective of the location of the information. However, many criminally-minded cyber citizens tend to misuse the grant of access to information and commit cyber crimes. Since no one country can control cyber space and everyone can have access to information anywhere it is important that countries to put in place a very robust security around critical national infrastructure, setup very swift response systems as risk of attacks cannot be eliminated, and use an international approach of cooperation to secure cyber space and mitigate cyber crimes.

Many countries have already formed nation Computer Emergency Response Teams (CERT) where cyber incidences are reported and coordinated actions taken to mitigate the impact and national emergency response systems to facilitate process of responses when the security of the nation is in danger by cyber attacks. CERTs have been set in very few developing nations, although there is much talk about the subject in many developing countries as networked computers infrastructure expands.

The International Telecommunication Union (ITU) through the International Multilateral Partnership against Cyber Threat (IMPACT) program has been playing a leadership role is providing early warning systems and training cyber security experts around the world. Today, IMPACT has over 142 countries as members. The IMPACT program has been used to prosecute a global cyber security agenda. ITU has indeed developed frame work 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) has also been a global platform of Computer Emergency Response teams in the world. Membership to FIRST is by recommendation and through testing of operational environment of country CERTs.

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 ICT discussion form 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 access challenge is waning. The networked computer infrastructure coming up in many African countries has open 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 draft cyber security convention that has been under review over the last few months and is due to be ratified by African heads of States. Harmonization, it can be argued, will establish regional cooperation in the fight against cyber crime.

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 us in dealing with future attacks.

NITA's concern of ensuring security of the network has forced it to initiate 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 national Computer Security Incident Response Team (CSIRT) initiative by the Ministry of Communications and the Commonwealth Cybersecurity Initiative (CCI) is an ongoing project for the creation of a national CSIRT. A CCI team were in Ghana recently on the scoping mission to assist Ghana develop a cyber security policy and strategy and, to help Ghana establish a national CSIRT. During the scoping mission, the team interviewed over 70 cyber security stakeholder in Ghana and interacted with the Adhoc Technical committee on the Cyber Security Policy and Strategy.

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 the National Communication Authority is another initiative to mitigate cyber crimes committed using mobile phones. The Ghana Police Service has also put in place the Anti-Fraud Unit to alleviate cyber and other crimes. The Economic and Organized Crime Office (EOCO) of the Attorney General's Department and Financial Intelligence Center for the financial sector are all government initiatives geared and mitigating crime in general and cyber crime in particular.

On the business side, the opening of an e-crime bureau in Ghana will help organization investigate cyber crime thoroughly and improve protection of cyber space.

In spite all these initiatives, the fact still remains that 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 information industry. In the information and knowledge economy, wars will be fought around information token of countries. 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 that is required to ensure national security and ensure that the information and knowledge economy continues to thrive and bring about wealth creation for citizens. As the infrastructure problems get solved in countries, there is an increase in attacks on networked computers and the critical information infrastructure that will 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 very robust incidence response system when any attacked is made on the CNII to avoid loss of revenue due to down time and ensure national security.

The need to create a culture of security which is absent today due to lack of awareness of the enormous threats that users of Internet are exposed must be addressed by a national cyber security policy. Awareness creation of the risks Internet users and other stakeholders are exposed to can drastically mitigate the risks of cyber attacks and consequential loss of revenue. This will create a very conducive environment in the information economy where Ghanaians can create worth 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 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 for combating cybercrime. The pillar among other things emphasis on capacity building, international cooperation and building infrastructure for security agencies to enable them use ICT to combat crime and also ensure that the legal text of the policy pillar is up to date to help security agencies prosecute any cyber crime offenders by the Attorney General’s office.

The Electronic Transaction Act (ETA) 2008 has specific legislation on cyber crime and prescribes punishment for cyber crime perpetuators. 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 fails 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 worth.

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

I. INTRODUCTION

Ghana's determination of securing 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 understanding 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. Our desire also recognizes that the threat is not restricted only to government but also to operators who provide public services to the citizens and private networks and looks to ensure that ally effort to ensure cyber security must be a private public partnership.

II. 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.

III. 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

IV. VISION

Our vision of developing a cyber security policy is to secure the Critical National Information Infrastructure (CNII) and make it resilient, and for Ghana to be self-reliant in securing its cyber space by infusing a culture of security to promote stability, social well being and wealth creation of our people by. All actors in law enforcement, national security, network security practitioners in government and business, and the public will take part in the vision.

V. MISSION STATEMENT

Our mission is to determine, analyze and address the immediate cyber security threats posed on identified critical national information infrastructure by providing adequately protection for the critical national information infrastructure and over time become a self sufficient country attending to its cyber security needs.

VI. POLICY SCOPE

This policy covers various aspect of cyber security including fight against cyber security, national security, legal measures, law enforcement and protection of critical national information infrastructure.

VII. POLICY CONTEXT

Ghana, like many countries in Africa 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. 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 draft convention under discussion at the regional level to harmonize the efforts of African countries in fighting cyber crime.

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 tarnished Ghana’s cyber credentials as a haven of cyber fraudster will be addressed by the policy. The policy also addresses the need to develop technology framework for combating cyber attacks and capacity building for cyber security expects to make Ghana self –sufficient in the fight against cyber crime 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.

VIII. 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 will in collaboration with the Attorney General's department setup 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 need 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 Ghana 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 assessment framework

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 the of 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 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

For each policy thrust, specific strategic actions will be implemented. 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
1.	Effective Governance	1. Government will setup cyber security institutions and 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: 1.1. National Cyber Security Council 1.2. National Cyber Security Center 1.3. National Computer Security Incidence Response Team (CSIRT) 1.4. National Cyber Security Policy Working Group	Ministry of Communications, National Security Council, NITA, NCA
2.	Legislative and Regulatory Framework	1. Government will setup Cyber Law Review Committee under the Attorney General's Department to do a study on the laws of Ghana to accommodate legal challenges in the Cyber environment and review every three year 1.1. Stage 1: identifications of issues in the cyber environment 1.2. Stage 2. Review current laws on cyber environment 1.3. Stage 3. Make recommendations for amendment of national laws	Attorney General's Department, Ministry of Communication

3.	Cyber Security Technology Framework	1. Government in collaboration with key stakeholders will review and adopt international cyber security standard such as MS ISO/IEC 27001 to increase robustness of CNII sectors 2. Government and its partners will also expand the national certification scheme for information security management & assurance	Ministry of Communications, NITA
4.	Culture of Cyber Security & Capacity Building	1. Efforts will be made to reduce number of Information security incidents through improved awareness & skill level 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 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, Ministry of Information,
5.	Research & Development towards Self–Reliance	1. A National R&D Roadmap for Cyber Security will be developed to ensure that 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: 3.1. Natural growth of Cyber Security Industry 3.2. Updating R&D roadmap regularly	Ministry of Communications, NITA, Universities, CSIR, Professional certification Centers

6.	Compliance & Enforcement	1. A national Risk Assessment framework for CNII will be developed to ensure a uniform framework for all CNII.	New Institutions, NITA, NCA
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: 1.1. Setup of National Cyber Crises management Committee (under National Cyber security council) 1.2. Positioning National and sector CSIRTs in the line of responding to emergencies 1.3. Setup of National Cyber Crises Management WG continuously reviewing structures and making recommendations to be acted on by committee	National Security Council, Ministry of Communications
8.	International Cooperation	Ghana will engage in relevant international cyber security meeting and prioritize engagement and join or sign International/regional conventions	National Security Council, Ministry of communications, Ministry of Foreign Affairs.

i. Strategy Implementation Timelines

The policy will be implemented in three stages:

STRATEGY	TIMELINE	ACTIVITIES
Short Term	Year 1 -2	**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
		The short term will focus on following policy thrust: *Effective governance* - Implement Action 1.4 to assist ministry of communications and other stakeholders put in place a stop gap measure to identify CNIIs, evaluate vulnerabilities and develop measures to address immediate concerns. - Begin building institution by implementing Actions 1.1 - 13 *Culture of Cyber Security* - Implement Action 2 to begin awareness creation *Cyber Security Emergency Readiness* - Implement Action 1 to develop framework
Medium Term	Year 3 - 4	**Building the infrastructure -** Setting-up the necessary systems, process, standards and institutional arrangements (mechanisms) and, building capacity amongst researchers and information security professionals
		The medium term will focus on following policy thrust: *Culture of Cyber Security & Capacity Building* - Implement Action 1 *Research & Development towards Self–Reliance* - Implement Actions 1 - 2 and accompanying infrastructure *Compliance and enforcement* - Implement Action 1 and accompanying infrastructure *Legislative and Regulatory Framework* - Implement Action 1
Long Term	Year 5+	**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
		The long term strategy will focus on following policy thrust: *Cyber Security Technology Framework* - Continuous review and improvement *Compliance & Enforcement* - Enforcing adopted Risk Management framework within CNII for comliance *Culture of cyber security* - 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 INTIATIVE)

The Implementation Strategy: Programs and Initiatives	
Title of Program/Initiative	**National Cyber Security Policy Working Group**
Program /Initiative Strategic Objective	• Assist MOC to collation of all cyber security initiatives • Identifying critical national information infrastructure in sectors as defined by the policy • Support policy drivers to setup structures for medium term strategy • Design and implement a comprehensive National Cyber Security Awareness program
Relevant Achievable National ICT4D Policy Objective & Goals	National Security, Law and other 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 in the conversion. The NCSPWG will assist the ministry of communication in the establishment of 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	• Support implementing agency to begin actual implementation of strategy • Develop a National Awareness Creation Program on Cyber Security including the creation of Nation Cyber Security Awareness portal • Assisting policy implementing agencies to build the structures for the achievement of long term goals
Program/Initiative Time-Frame	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 Nation 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 with be 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 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 5 years. The main beneficiary is Government of Ghana.	
COST	Members of NCSWG must be rewarded for role for the period when they are actively involved in implementation. This must include a setting allowance and expenses cover for any activity performed. Estimated Budget of GHC200,000.00 for one year	
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	• Define Security Awareness Goals and Objectives • Identify Intended Audience (Stakeholders, General Public) • Define Topics to be covered • Identify Current Training Needs • Obtain Support • Establish Security Policy • Define Delivery Methods to be used • Develop a Strategy for Implementation • Design Awareness Strategy • Design Training Strategy • Develop Evaluation Methods • 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 aware 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	• To develop a level of awareness in the community to mitigate risk of cyber attacks by workshops, mass media and other awareness programs • Develop a National Awareness portal for easy access to information on cyber security and easily 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	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.

	Internet users in Ghana should Know how get themselves a basic level of protection against threats online Estimated cost of entire program will be about GHC500, 000.00 for year one. Annual budget of about GHC200,000.00 then after.	
National Cyber Security Awareness Portal	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. Estimated cost of portal creation and maintenance for year one is GHC200,000.00 Subsequent year may be down to less than GHC100,000.00	
Project Implementation Management, Monitoring and Evaluation		
Supporting Implementation Agencies and their Assignment Responsibilities	Supporting Implementation Agency	Assigned Responsibility
	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 Communication Authority	Technical advisory and guide on web portal development. Capacity 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 INTIATIVE)

The Implementation Strategy: Programs and Initiatives	
Title of Program/Initiative	**National Cyber Security Center (NCSC)**
Program /Initiative Strategic Objective	Strategic Objective of NCSC are : • 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 Assessment: Assesses and identifies 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	Effective Governance of National Cyber Security Policy

Policy Objective & Goals	
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	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. 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.
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. It will also spearhead all awareness and education activities on Cyber security after creation.
Program/Initiative Implementation Specific Goals	- 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 setup 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-month 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 Agencies and their Assignment Responsibilities	**Supporting Implementation Agency**	**Assigned Responsibility**
	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 Success Factors	Legislative approval of initiative 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	Strategic Objective of NCSC are : • Oversee the national cyber security policy and strategy; • Identify National cyber security priorities and initiatives • Coordinate cyber security measures at the national level • Help foster public-private relations required to address cyber security issues • 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 • Collaborate with the structures responsible application of the law at regional and International level • Coordination of measures and development of digital identity systems as well as management and best practice in digital identity • 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 National Cyber Security Council 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
Program/Initiative Implementation Rationale	The rationale for the setting up the NCSC is to serve as the high level governance institution overseeing all issues on cyber security.
Program/Initiative Implementation Specific Goals	- 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 and is playing its role as a leader in the region
Program/Initiative Time-Frame	To setup 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
Legal framework for establishment passed	By 12-month from the adoption of the policy
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 Agencies and their Assignment Responsibilities	**Supporting Implementation Agency**	**Assigned Responsibility**
	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 INTIATIVE)

The Implementation Strategy: Programs and Initiatives	
Title of Program/Initiative	**National Cyber Security Crisis Management Plan (NCSCMP)**
Program /Initiative Strategic Objective	Strategic Objective of NCSCMP are : • Increase preparedness of country against cyber attacks • Enhance capability to respond to cyber security issues • Provide coordinated effort in handling cyber attacks • 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 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	- 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 CNIIs 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,	Setup of Working Group

	CNII Sectors	
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 INTIATIVE)

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 : • to provide reactive and proactive services, • communicating 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: ▪ **Reactive services:** early warning and precaution notice, incidents processing, incidents analysis, incident response facility, incidents response coordination, incident response on the web, vulnerability treatment, vulnerability analysis, and vulnerability response and vulnerability response coordination; ▪ **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 by 18 Months from adoption of 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 Agency	Assigned Responsibility
Supporting Implementation Agencies and their Assignment	Ministry of Communications with support of CCI	Development of institutional structures of National CSIRT

Responsibilities	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		