GAMBIA NATIONAL CYBER SECURITY STRATEGY AND ACTION PLAN 2020-2024

Commissioned by
The Ministry of Information and Communication Infrastructure

JUNE 2020

LIST OF ABBRIVIATIONS 4

EXECUTIVE SUMMARY 5

1. INTRODUCTION 7

2. NATIONAL CYBER SECURITY STRATEGY 8

2.1 VISION 9
2.2 MISSION 9
2.3 STRATEGIC GOALS 9

3. STRATEGIC PLAN 10

3.1 KEY ELEMENTS FOR A SUCCESSFUL STRATEGY 10

4. IMPLEMENTATION MEASURES 11

4.1 REQUIREMENTS FOR CYBER INFRASTRUCTURE PROTECTION 11
4.3 GENERAL DIRECTION AND GOALS 11
4.4 GUIDING FRAMEWORK 12

5. SPECIFIC OBJECIVES AND ACTIONS 12

5.1 STRATEGIES AND PROGRAMMES 12

6. DIMENSION 1: ESTABLISHING NATIONAL RISK ASSESSMENT 14

6.1 **STRATEGY 1: UNDERSTANDING RISK** 14

6.2 PROGRAMME 1: NATIONAL THREAT ASSESSMENT 15

7. DIMENSION 2: BUILDING CYBER SECURITY CAPABILITIES 17

7.1 **STRATEGY 2: CONTROLLING RISK** 17

7.2 PROGRAMME 2: PREVENTIVE CAPABILITY PROGRAM 17
7.2 PROGRAMME 3: PROTECTIVE CAPABILITY PROGRAM 18
7.3 PROGRAMME 4: RESPONSE CAPABILITY PROGRAM 21
7.4 PROGRAMME 5: ENHANCEMENT OF LAW ENFORCEMENT CAPABILITY 23
7.5 PROGRAMME 6: GOVERNMENT CYBER SECURITY EMHANCEMENT PROGRAM 25
7.5.5 ACTIONS 25

7.6 **CRISIS MANAGEMENT** 27

7.6.1 PROGRAMME 7: BUSINESS CONTINUITY / RESILIENCY PROGRAM 27
7.7 PROGRAMME 8: REMEDIATION PROGRAM 30

8. DIMENSION 3: INSTITUTIONAL GOVERNANCE FRAMEWORK 30

8.1 **STRATEGY 3: ORGANIZATION AND MOBILIZATION FOR CYBER SECURITY** 30

8.2 PROGRAMME 9: ESTABLISHING NATIONWIDE MONITORING POINTS 31

9. DIMENSION 4: NATIONAL & INTERNATIONAL COOPERATION 31

9.1 PROGRAMME 10: ESTABLISHING PUBLIC AND PRIVATE PARTNERSHIP/COOPERATION 31
9.1.2 ACTIONS 31

10. DIMENSION 5: CYBER SECURITY CAPACITY BUILDING AND AWARENESS.............33

10.1 PROGRAMME 11: ADVOCACY AND PUBLIC AWARENESS 33

10.1.5 ACTIONS.. 33

12. DIMENSION 6: LEGAL AND REGULATORY FRAMEWORK 38

12.1 STRATEGY 4: INSTITUTIONAL BUILD-UP 38

12.3 SPECIFIC OBJECTIVES 1: PASSAGE OF CYBER-CRIME LAW..38

12.6 SPECIFIC OBJECTIVES 4: BUILDING THE CAPACITY OF LAW ENFORCEMENT 40

13. PROGRAMME 12: BUILDING CYBER SECURITY INDUSTRY... 41

13.2 ACTIONS 41

14. INSTITUTIONAL FRAMEWORK...42

APPENDIX (A) MONITORING AND EVALUATION FRAMEWORK......................................48

APPENDIX (B) CYBER SECURITY PROGRAM RISK ASSESSMENT FLOW 60

APPENDIX (C) CYBER SECURITY GOVERNANCE ORGANOGRAM..................................60

APPENDIX (D) NATIONAL CYBER SECURITY COMMISSION COMMITTEES 61

APPENDIX (E) LOGICAL FLOW OF ACTION PLAN 62

LIST OF ABBRIVIATIONS

ICT	Information Communications Technology
ICI	Information Communications Infrastructure
NICI	National Information Communications Infrastructure
CI	Critical Infrastructures
ICT4D	Information Communications Technology for Development
NCII	National Critical Information Infrastructure
GICTA	Gambia Information Communications Technology Agency
GoTG	Government of The Gambia
KPI	Key Performance Indicator
WARCIP	West African Regional Communications Infrastructure Program
GSC	Gambia Submarine Cable
ACE	Africa Coast to Europe Submarine Cable
GAMTEL	Gambia Telecommunications Services Company
GM-CSIRT	The Gambia Computer Security Incident Response Team
CSIRT	Computer Emergency Response Team
SOC	Security Operation Center (constituent of GM-CSIRT)
NOC	Network Operation Center (sector network operation center)
NCSC	National Cyber Security Commission
NCCD	National Cybersecurity Coordination Directorate
NCSS	National Cybersecurity Strategy
NDP	National Development Plan
CMM	Cybersecurity Maturity Model
PURA	Public Utility and Regulatory Authority
MOICI	Ministry of Information Communications infrastructure
GSC	Gambia Submarine Cable Company
GPF	Gambia Police Force
MOJ	Ministry of Justice
ISP	Internet Service Provider
MoD	Ministry of Defense
MOI	Ministry of the Interior
BCP	Business Continuity Plan
PKI	Public Key Infrastructure
DR	Disaster Recovery
Fintech	Financial Technology
NIE	National Intelligence Estimate
SIS	State Intelligence Service
GNA	Gambia National Army
NDRA	National Disaster Recovery Agency
CSIRT	Computer Emergency Response Team
GCSA	Gambia Cyber security Alliance
KM	Knowledge Management
R & D	Research & development
SOU	Special Operations Unit
AIC	Availability, Integrity and Confidentiality

EXECUTIVE SUMMARY

An increased dependence on ICTs has brought enormous benefits to society; and the internet has become a driving force for productivity and development for national economies. Currently, innovative transformations are happening in many organizations especially in the area of moving business operations and services online. By extension, the pervasive use of mobile applications, fintech solutions and automation have also impacted positively on businesses around the world.

This goes to suggests that as long as our critical infrastructure continues to connect to computers and information networks, we will inevitably continue to rely on them to deliver services. In recent years, Cybersecurity is increasing its significance due to the overwhelming use of devices which require the use of internet. This development has implications for criminal exploitation of information systems.

In an attempt to address the cybercrime challenge and continue to remain proactive in national response, the Gambia government has embarked on measures designed to facilitate ICT integration into all sectors of Gambian economy. For this to be realized, safety and security should be central in national development initiatives.

The formulation of the draft Gambia Cyber Security Strategy and Action plan 2016 is a positive step and a long-term measure for protecting the country from cyber related security risks. The initiative ushered in a call for the development of a national cyber security policy and strategic Action plan. This will ultimately pave the way for full implementation of the objectives and goals set in the policy.

The purpose of this Strategic Plan is to build Gambia's capability to prevent, protect, detect, respond and manage cyber threats against information systems, critical infrastructures and services. By extension, establish and strengthen the organizational policy and institutional foundations for cyber infrastructure protection across all sectors. It would be also useful in identifying loopholes, inadequacies and other necessities that must be address by government and the private sector in order to adequately meet the challenges ahead.

1. INTRODUCTION

Being an entity of numerous opportunities, the cyberspace is a promising avenue for transforming and strengthening national economies into a knowledge-based society. However, criminal misuse of cyber space is a serious challenge and threat to our information systems, services and critical infrastructures. It is precisely because of this phenomenon, critical infrastructure protection should be an important component of Gambia's national security program.

This National Cyber Security Plan will serve as a guide to protect the nation's information systems, critical infrastructures and Gambia's Cyberspace in general. It is a working plan envisaged to eventually generate a platform for coordination, cooperation and collaboration between the public and private sectors. It also envisions the harmonization of national cyber security policies and programs. The National Cyber Security Strategy and Action Plan shall be the cornerstone of the country's cyber security policy.

2. NATIONAL CYBER SECURITY STRATEGY

This national Cyber security strategy provides guidance on the development of a national cyber-security ecosystem. This includes legal, regulatory and institutional framework, building cyber-security capacity and capabilities and development of standards and guidelines to:

(i) Ensure that critical ICT systems and infrastructure in public and private sectors are protected and made resilient.

(ii) Foster adoption of security standards and guidelines within Government and the private sector.

The draft National Cyber Security strategy 2016 came as a result of several consultations and workshops conducted by MOICI-PURA in collaboration with international partners (Bird & Bird – Civipol, Expertise France and CMM Oxford) among others. The successful outcome of these engagements ushered in the draft National Cybersecurity Strategy Formulation and Action Plan 2016. This strategy outlines Gambia's Vision, Mission for Cyber security and ways to improve or calibrate the Cyber security posture. This initiative primarily seeks to address the national cybersecurity threats against information systems, and critical infrastructures and services.

While the proposed strategy focuses on the nature and characteristics of information and communication technology, the important physical aspects and dimensions of critical infrastructure protection including measures to respond to challenges of cyber threats were considered. To address cyber security awareness challenge, the involvement of civil society to help raise awareness, establish and promote cybersecurity education and Training and to build national capacity and capabilities all forms an integral part of the Gambia's strategic cybersecurity goals etc. This provides a holistic approach and direction to cyber security measures from strategic, tactical to operational aspects of Cyber security.

As a global challenge, Cyber security demands both domestic and international solutions. Given the shared nature of vulnerabilities, the national cyber security strategy would need strong partnership between public and private sectors. In this endeavor, the Strategy and Action Plan creates a coherent vision to ensuring that The Gambia cyberspace is secure through collective efforts of all stakeholders (i.e. government, private sector, civil society, citizens and international) cooperation and collaboration. To this end, GoTG is committed to collaborate with regional and international partner in creating solutions to address the Cyber security challenges.

2.1 Vision

To provide trusted, secure and resilient cyberspace for the Government, corporate businesses and citizenry to further enhance socioeconomic development of the people through ICT transformations.

2.2 Mission

To develop and deliver effective Cyber security capacity, services and infrastructure that instills confidence in Gambian cyberspace.

2.3 Strategic Goals

For the vision to be achieved, the Government of The Gambia aimed to achieve the following strategic goals:

- Identify and manage the critical information infrastructure of The Gambia
- Develop and enhance Cyber security-related capacity and infrastructure
- Strengthen legal, regulatory frameworks.
- Promote awareness, information sharing and collaboration on cyber security.
- Ensure continuous improvement of the safety of vulnerable groups in cyberspace, especially the safety of children.

- Enhance and coordinate the fight against all forms of cybercrime
- Promote the use of cyberspace to drive social and economic development

3. STRATEGIC PLAN

This Plan is designed to provide direction on the implementation of the strategic goals and specific objectives in line with national policy priorities. The plan outlines a framework for organizing and prioritizing efforts to manage cyber security risks in the Gambian cyberspace.

The draft Action Plan further identifies specific initiatives, roles, and responsibilities of key stakeholders with deliverables, timeline and indicators for measuring progress on the implementation of the national cybersecurity strategy. This Strategy and Action Plan shall be the cornerstone of the Gambia's cyber security policy.

3.1 KEY ELEMENTS FOR A SUCCESSFUL STRATEGY[1]

To secure the Gambian cyberspace demands the provision of adequate protection to all ICT systems, networks and critical infrastructure. The challenge is the lack of technology specific skills most systems owners and operators lack hence the need for cybersecurity products and services. The success of this cybersecurity strategy is based on the following six elements:

1. People and entities mobilized to secure each ICT System
2. People and entities in capacity to provide cyber security technology and services
3. The GM-CSIRT to operate the national Cybersecurity Centre
4. The Gambia Police Force and Justice to fight cybercrime
5. Promote Awareness, training and education for all stakeholders

[1] The Gambia National Cybersecurity Strategy – Proposed Formulation and Action Plan, MOICI, July 2016

6. Establish a national cybersecurity governance framework

4. IMPLEMENTATION MEASURES

4.1 REQUIREMENTS FOR CYBER INFRASTRUCTURE PROTECTION

Given the advances in technology, nature and characteristics of cyber threats, the challenge to protect information systems, services and critical cyber infrastructures becomes difficult. To overcome this challenge requires some degree of expertise in technology, collective action from local stakeholders, private sector, civil society, citizenry and international community. To be able to meet the cybersecurity challenges, the following are important measures adopted.

4.1.1 Having knowledge of the threats adopted:
4.1.2 Identifying the vulnerabilities
4.1.3 Put in place resilient protective measures
4.1.4 Establish effective response capability
4.1.5 Establish Recovery program
4.1.6 Ensure effective law enforcement

4.3 GENERAL DIRECTION AND GOALS

The general direction and goals of the plan is based on how the following will be achieved.

4.3.1 Coordinated and integrated response
4.3.2 Information assurance
4.3.3 Continuous operation of critical cyber infrastructures
4.3.5 Effective law enforcement and administration of justice
4.3.6 Public-private sector partnership
4.3.7 International cooperation
4.3.8 Sustainability of programs
4.3.9 Cyber security conscious society

4.4 GUIDING FRAMEWORK

4.4.1 Establishing a Secure Environment

4.4.1.1 **Identification and elimination of threats**. This involves knowing the threats and determination of ways in which they can be effectively neutralized.

4.4.1.2 **Assess and eliminate vulnerabilities**. To identify and remove weaknesses and increase the level of resiliency

4.4.1.3 **Defeat attacks**. By introducing appropriate and adequate countermeasures

4.4.1.4 **Reduce losses and damages.** By implementing contingency plans and other actions to mitigate potential losses and damages

4.4.1.5 **Implement a resiliency program.** This is a program for ensuring business continuity

4.4.1.6 **Institute effective law enforcement programs.** This is intended to enhance capacity and capabilities, legal and policy regime.

5. SPECIFIC OBJECIVES AND ACTIONS

This action plan is consistent with international standards and the primary goals are:

- Assuring the continuous operation of Gambia's information systems, services and critical cyber infrastructures.
- Implementing capacity-building measures to enhance Gambia's ability to respond to threats before, during and after attacks.
- Effective law enforcement and administration of justice
- Cyber-security conscious society.

5.1 STRATEGIES AND PROGRAMS

Based on the above, four (4) strategies have been formulated critical to information infrastructures protection and services of The Gambia.

A. Understanding the cybersecurity Risk

B. Controlling the Risk

C. Organizing and Mobilizing for Cyber security

D. Institutional and Policy Build-Up

Each strategy has specific programs to be implemented. Generally, the Action Plan seeks to institutionalize the necessary capabilities in government and the private sector to adequately meet and respond to challenges and threats against critical infrastructures, information systems and services that are critical to national security and well-being. For the strategic goals to be achieved, specific objectives and actions are required.

The plan consists of programs, strategic goals, specific initiatives and required actions to support the implementation of the strategy. It also includes deliverables, supporting agencies, timeline, estimated financial resources and indicators to evaluate performance for the implementation. The following are the key elements necessary to successfully implement the strategy.

- **Strategic Goal:** The substantive long-term goal that The Gambia would like to achieve in each priority area;
- **Specific Objective:** The specific steps to be undertaken to achieve the Strategic Goal
- **Actions:** The activities that must be undertaken, under this Strategic Plan, in pursuit of the Specific Objective objectives
- **Deliverables:** The formal work products that The Gambia will achieve in the medium term
- **Responsible Institution:** The Gambian Institutions with primary responsibility for managing completion of each objective, and the institutions that will provide support.
- **Time Frame:** The period of time within which deliverables are produced and or Actions are implemented
-

- **Key performance Indicators:** The performance indices, data measurements, and trends that should be monitored to evaluate the progress in implementing the Strategy and achieving the objectives and deliverables
- **Funding Sources:** Different possible funding sources and mechanisms can be adopted to fund the implementation of the strategy and action plan.

6. DIMENSION 1: ESTABLISHING NATIONAL RISK ASSESSMENT

Strategic Goal 1: Identify and Manage Risks to Critical Information Infrastructure of The Gambia.

The protection of critical information infrastructure (CIIs), calls for collaboration of all relevant stakeholders - public and private institutions that own or operate the information infrastructure which supports the functioning of the Gambian society. The Government of The Gambia (GoTG) will work with all relevant stakeholders to identify, understand the vulnerabilities and Cyber security posture of The Gambia's information infrastructure CIIs.

The Government will also work with relevant stakeholders to establish measures that will address current and future cyber threats and risks to the national information infrastructure, and to drive improvements where necessary.

6.1 STRATEGY 1: UNDERSTANDING RISK

The most important strategy in protecting the national critical cyber infrastructures is to first understand the nature of threats to Gambia's cyberspace. This strategy would involve continuing threat assessment.

This will also include assessing the vulnerabilities, protective measures being implemented and the significance of potential targets. This strategy also entails the need for a Cyber security, and Institutional and Policy Build-Up. Every strategy has corresponding programs to be undertaken.

6.2 PROGRAMME 1: NATIONAL THREAT ASSESSMENT

6.2.1 Strategic Goal 1: To Conduct National Assessment

This initiative consist two primary specific objectives:

- **A.** National cyber mapping
- **B.** National Risk assessment

6.2.2 Specific Objectives 1: National Cyber Mapping

This program involves acquisition of knowledge pertaining to demographics, traffic, statistics and other relevant information which may be used to map out the Gambia's Cyberspace for cybersecurity program formulation and implementation.

6.2.3 ACTIONS

A. Inventory

This initiative will identify and account critical infrastructures in order to determine their extent and degree of criticality to be able to prioritize and allocate resources for cyber security. This will include accounting of physical facilities, hardware, software and people.

6.2.4 Specific Objectives 2: Conduct National Risk Assessment

Risk assessment represents an important step in understanding the threats, vulnerabilities, countermeasures and impacts to national security. It will have the following components.

6.2.5 ACTIONS

A. National Threat Assessment

A national threat assessment initiative will be implemented to provide basis for and continuing understanding of the nature of cyber threats and how they can be addressed effectively from operational and strategic perspectives. Likewise, a cyber-intelligence program will be created. It will be undertaken to gain knowledge of the hacker's world, its personalities, operations and plans.

B. Vulnerability Assessment

Vulnerability assessment will be implemented on a periodic basis to identify weaknesses in CI protective programs and to institute appropriate corrective measures. This will include the following:

B.1 Formulation of a Vulnerability Assessment Framework and Checklist

This framework and checklist will be used to gather essential information on IT security threats and measures, critical security policies and practices on networks, systems, applications, and data and its classification, and external systems; cyber-attacks and recovery plan.

B.2 Security Audit, Survey and Inspection

This involves the conduct of a periodic security audit, survey and inspection as a way to ensure implementation of security programs as well as a means to identify weaknesses in the systems.

6.2.6 Impact Analysis

This will be implemented to periodically assess the implications of any attacks against information systems and critical infrastructures on the operations of government and the economy.

7. DIMENSION 2: BUILDING CYBER SECURITY CAPABILITIES
7.1 STRATEGY 2: CONTROLLING RISK

Risk control requires comprehensive security planning, effective resolution of crisis and risk monitoring. This strategy will address the aspects of mitigating or reducing vulnerabilities, likelihood of threat occurrence and potential losses or damages. Under Dimension 2, seven (7) major programs are formulated. These are Preventive Program, Protective Program, Response Program, Enhancement of Law Enforcement Capability Program, Government Cybersecurity Enhancement program, Crisis Management Program and Remediation Program.

7.2 PROGRAMME 2: PREVENTIVE CAPABILITY PROGRAM

7.1.1 Strategic Goal 1: Establishing Measures to Prevent Attacks

7.1.2 Specific Objective 1: Strengthen Cyber Intelligence Collection

Cyber intelligence is the process of acquiring and utilizing threat-related knowledge in the cyberspace that pertains, but not limited, to the nature and characteristics of cyber threats, their mode of operation, plans, organizations, personalities and other relevant information. The cyber-intelligence program will be intelligence operations against sources of cyber threats. This will be able to provide periodic assessments and address information requirements of law enforcement and military units in the interdiction of cyber-criminals. This involves the following actions:

7.1.2.1 Setting up a Cyber Special Operations Unit.

7.1.2.2 Produce monthly National Intelligence Estimates (NIE) targeting strategic and operational intelligence on cybercrimes

7.1.2.3 Develop and manage cyber-criminal Database

7.1.2.4 Ministry of Defense and SIS to develop and implement sectoral cyber-intelligence training program

7.1.2.5 Establish early Warnings and alerts systems

The warnings and advisories will provide the necessary information on threats and security alerts, as well as advisories to all critical infrastructure owners and operators, and the general public. It is intended to prepare and update them for any threat situation. These warnings and advisories will include computer attack information, trends or mode of operation, wanted cyber criminals and updates on patches and protective measures among other.

7.2 PROGRAMME 3: PROTECTIVE CAPABILITY PROGRAM

The protection of critical information infrastructure (CIIs), calls for collaboration of all relevant stakeholders - public and private institutions that own or operate the information infrastructure which supports the functioning of the Gambian society.

The Government of The Gambia (GoTG) will work with all relevant stakeholders to identify, understand the vulnerabilities and Cyber security posture of The Gambia's information infrastructure CIIs. The Government will also work with relevant stakeholders to establish measures that will address current and future cyber threats and risks to the national information infrastructure, and to drive improvements where necessary.

7.2.1 Strategic Goal (i): Identify and Manage the Critical Information Infrastructure of The Gambia

7.2.2 Actions

7.2.3 Establish a National CII Register

7.2.4 Develop a National CII Governance Framework which provides details on CII protection procedures and processes

7.2.5 Establish a National Risk Register and Regulations and/or Guidelines that promote continuous risk assessment and management across CIIs in The Gambia

7.2.6 Establish Mandatory Equipment Specifications, Mandatory Guidelines, Regulations, Security Requirements, Procedures relating to the management of risks by CIIs

7.2.7 Create a National Vulnerability Register and Framework for regular vulnerability monitoring and disclosure for CII

7.2.8 Undertake continuous monitoring and regular testing to detect errors, vulnerabilities, and intrusions in CII

7.2.9 Promote and enhance regional and international cooperation in the protection of the critical information infrastructure (CII)

7.2.10 Establish mandatory and minimum technology and security requirements for equipment of ISPs and end users like the banking sector

7.2.11 Develop a government programme to deploy and manage government ICT infrastructure

7.2.12 Develop a national programme to enhance internet infrastructure development and resilience

7.2.13 Develop National Contingency plans which identify emergency response asset priorities and standard operating procedures (SOPs)

7.2.14 Review and update the map of current emergency response assets

7.2.15 Ensure communication channels are deployed across emergency response functions, geographic areas of responsibility, public and private responders, and command authority

Strategic Goal 1: Building Robust Systems

This is targeting critical infrastructure owners and operators to procure, install or build robust and redundant systems to withstand attacks or mitigate vulnerabilities. This will include systems design and engineering and reliable back-up systems. It will embrace the adoption of reconstitution and rehabilitation measures to ensure immediate recovery. This will also incorporate the formulation, adoption and issuance of security standards that will serve as a guide to IT security administrators or managers.

7.2.2 Specific Objectives 1: Intrusion Detection

This initiative envisions monitoring of intrusions as a way to detect existence of an attack. This will be a function of the focal points or, Sectoral CSIRTs and monitoring points.

7.2.3 Specific Objectives 2: Operations Security (OPSEC)

This will be for government information security. It will focus on systems and procedures on the proper handling of classified and critical information. The implementation of an encryption system for the government institutions

7.2.4 Specific Objectives 2: Security Audit

This will require the periodic conduct of security audit to identify vulnerabilities, compliance of security standards and monitoring the appropriate implementation of security programs.

7.2.5 Specific Objectives 2: Consumer Protection

This will establish mechanisms to address consumer protection and technology products quality assurance including the following concerns:

- Product Quality assurance checks

- Consumer Education
- Remedy and redress in case of fraud
- Product information for choice
- Access to products
- Product evaluation and testing

7.3 PROGRAMME 4: RESPONSE CAPABILITY PROGRAM

7.3.1 Strategic Goal 1: Establishing Computer Security Response Units

7.3.2 Specific Objectives 1: Establish the National CSIRT

The national CSIRT for The Gambia is GM-CSIRT which is the national computer emergency response team. Besides recovery and reconstitution, the GM-CSIRT will be the national focal point for response to incidents and other cyber-related matters. Therefore for GM-CSIRT to be able to carry its functions, the following should be put in place.

7.3.2.1 Expedite the operationalization of a GM-CSIRT with clear processes, defined roles and responsibilities

7.3.2.2 Continuously develop the capacity of GM-CSIRT staff to address the fast-changing technical requirements, and develop abilities to actively obtain information in cyberspace, about current cyber risks and threats

7.3.2.3 Develop a national incident reporting, information sharing and coordination mechanisms to address reporting of incidents and coordination in incident response

7.3.2.4 Create and continuously update cyber security incident register, assess incidents, and suggest measures to resolve issues and mitigate threats and risks.

7.3.2.5 Strengthen GM-CSIRT capacity in terms of budget, technology and human resources with roles and responsibilities clearly defined.

7.3.2.6 Continuously monitor, analyze and assess cyber threats and potential risks and be able to provide a real time overview of state of cyber security across the nation

7.3.2.7 Develop a Cybersecurity Governance Framework for defining roles and responsibilities of all stakeholders as well as describe SOPs and code of conduct in responding to incidents

7.3.2.8 Establish a call centre/help line for reporting incidents or seeking assistance with incidents

7.3.2.9 Develop and implement cybersecurity incident simulation scenarios and programs that can be used during the national exercises/drills

7.3.2.10 Develop updates cybersecurity contingency plans, including roles of the military/security forces during cyber-attacks and emergencies

7.3.2.11 Develop a Cyber Defence Strategy that details approaches to addressing threats to national security in cyberspace

7.3.2.12 Establish a Central Defence Command and Control Centre for cybersecurity in The Gambia

7.3.2.13 Establish mechanisms for regional and international cooperation for incident response

7.3.2.14 Develop web portal to receive cyber complaints

7.3.3 Specific Objectives 2: Creation of Sectoral Focal Points/CSIRTs

In support of the GM-CSIRT, this program entails the establishment of sectoral computer emergency response teams or focal points across the country to enable faster and more localized response to cyber incidents. They can be any regional or local government offices, or private sector organizations that have the capability to undertake the initiative. These sectoral CSIRTS will serve as immediate points of contact for government agencies, local government units. It will coordinate its operation with the GM-CSIRT.

7.3.4 Specific Objectives 3: Establishing Cyber Crime Complaint Center

This initiative envisions providing a mechanism to receive and develop Internet-related criminal complaints and refer the same to the law enforcement agencies and the GM-CSIRT for investigation. A website will be developed and maintained as the primary complaint reporting point.

7.3.4.1 Action:

7.3.4.2 Develop a web portal to received complaints

7.4 PROGRAMME 5: ENHANCEMENT OF LAW ENFORCEMENT CAPABILITY

7.4.1 Strategic Goal 1: Establishing Police Cybercrime Response Unit

This program will improve and increase the current law enforcement capability. It envisions training and developing Forensics investigators and Incident Responders in every designated law enforcement offices. It will provide local and international trainings on Computer/digital forensics and investigation, incident response, preservation of evidence, data recovery/retrieval and analysis, digital intelligence and other relevant courses.

7.4.2 Specific Objectives 1: Establish National Forensics Laboratory

This initiative aims to establish a modern national forensic laboratory that will be called the National Computer Forensic Laboratory (NCFL), serving as a processing laboratory and center for computer crime evidence repository.
It will provide support to law enforcement operations in addition to conducting training on computer forensics and investigation.

7.4.3 Specific Objective 2: Enhance Cybercrime Detection

7.4.3.1 Actions:

7.4.3.2 Undertake a gap analysis to identify gaps in current ICT Security, legal and regulatory framework

7.4.3.3 Develop requisite instruments to address Gaps including issues relating to substantive, procedural, privacy and data protection

7.4.3.4 Develop and publish a cybersecurity policy and standards

7.4.3.5 Create a national programme to promote the adoption of cybersecurity standards across government agencies and CII

7.4.3.6 Establish the requisite framework to operationalize a digital forensics laboratory

7.4.3.7 Develop mandatory digital forensics and evidence handling courses for the judiciary, law enforcement and personnel from other related agencies involved in the detection and prosecution of cybercrime

7.4.3.8 Build and enhance capacity to detect cybercrime incidents

7.4.3.9 Train judiciary and the legal fraternity on how to interpret and enforce the policy, legal and regulatory frameworks on Cyber security in The Gambia

7.4.3.10 Identify needs, provide training and education to develop the capacities of the law enforcement agencies, judiciary and the legal

7.4.3.11 Fraternity on how to interpret and enforce the policy, legal & regulatory frameworks on cybersecurity in The Gambia

7.4.4 Specific Objectives 3: Build Capacity of Judges and Prosecutors

This will provide education and training for judges, prosecutors and lawyers to help them in the effective handling of cyber-crimes and in the administration of justice.

7.4.5 Actions

7.4.5.1 Develop mandatory digital forensics and evidence handling courses for the judiciary, law enforcement and personnel from other related agencies involved in the detection and prosecution of cybercrime

7.4.5.2 Train judiciary and the legal fraternity on how to interpret and enforce the policy, legal and regulatory frameworks on Cyber security in The Gambia

7.5 PROGRAMME 6: GOVERNMENT CYBER SECURITY EMHANCEMENT PROGRAM

7.5.1 **Strategic Goal 1**: To safeguard Government information systems and critical national infrastructures against cyber-attacks.

7.5.2 **Specific Objective2:** Establish Information Security Assurance mechanisms or Compliance

7.5.3 **Specific Objective 3:** Establish security levels for systems, applications and services

7.5.4 **Specific Objective 4:** Enhance Technical and procedural measures for implementing Cyber security for critical information infrastructures (CIIs).

7.5.5 **Actions:**

7.5.5.1 Establish mandatory and minimum technology and security requirements for CIIs

7.5.5.2 Develop national Programme to deploy and manage government ICT infrastructure

7.5.5.5 Develop a national programme to enhance internet infrastructure development and resilience

7.5.5.6 Develop national contingency plans which identify emergency response asset priorities and standard operating procedures (SOPs)

7.5.5.6 Review, develop or update the emergency response assets

7.5.5.7 Ensure communication channels are deployed across emergency response functions, geographic areas of responsibility, public and private responders, and command authority.

7.5.6 Specific Objective 5: Facilitate recruitment, develop and enhance cybersecurity technical capacity in The Gambia

7.5.7 Actions

7.5.7.1 Develop national and Career Progression Policy promoting continuous training and education for Incident Response and addressing issues relating to Cyber security

7.5.7.2 Identify staffing requirements for Government Agencies and CII operators and develop a national recruitment and retention strategy.

7.5.7.2 Develop and implement Cyber security training and capacity building training plans for Government personnel.

7.5.7.3 Revise the National Research Agenda to promote R&D in cybersecurity

7.5.7.4 Establish a National Centre of Excellence for cybersecurity training & research

7.5.7.5 Review and update primary, secondary and tertiary level education curriculum to include cybersecurity components

7.5.7.6 Promote cybersecurity competitions and Support R & D projects in universities and schools

7.5.7.7 Support national enterprises providing cybersecurity solutions, and undertaking R & D in cybersecurity

7.5.7.8 Collaborate with universities, tertiary and the private sector to create new study and internship programs on cyber security

7.5.7.9 Collaborate with the private sector and academia to support participation of government institutions, universities, private sector in regional and international research projects and exercises relating to cybersecurity

7.5.7.10 Create standards in cybersecurity training and education

7.5.7.11 Train IT personnel of various sectors of Government on how to detect incidents, report incidents, and collaborate with the GM-CSIRT and institutions from other sectors on cybersecurity

7.5.8 Specific objective 6: Establish secure and reliable environment for e-Government and e-commerce with National Public Key Infrastructure

7.5.9 Actions:

7.5.9.1 Create, and periodically update the general public and other sectors on how cyberspace is securely used to deliver e-government and e-commerce services in The Gambia, highlighting the various security features deployed to foster trust.

7.5.9.2 Encourage the use of Public Key Infrastructure (PKI) for transactions to/from Government Ministries, Departments and Agencies to enhance high cyber security levels and trust in delivering public services.

7.5.9.3 Appoint cyber security inspectors who will serve as focal points of contacts to support small and medium enterprises in addressing cyber security needs and method of mitigating cyber threats

7.6 CRISIS MANAGEMENT

7.6.1 PROGRAMME 7: BUSINESS CONTINUITY / RESILIENCY PROGRAM

This program will provide measures and mechanisms to effectively manage Crisis, mitigate losses/damages and allow critical infrastructures to recover and reconstitute immediately in order to arrest further disruption of the operation of critical infrastructure.

7.6.2 Strategic Goal 1: Establish Mechanism to Manage Crisis and Prevent Damage and Losses

7.6.2.1 Develop a national business continuity/disaster recovery / contingency plan with the cybersecurity component.

7.6.2.1 Designate cybersecurity exercise planning to GM-CSIRT in collaboration with Gambia National Disaster Management Agency (NDMA).

7.6.2.1 Involve key stakeholders and other experts, such as thank thanks, academic and civil society leaders in the planning process

7.6.2.2 Design, implement and test a cybersecurity needs assessment

7.6.2.3 Develop Framework to gauge the mitigation measures, protocols and techniques for crisis management.

7.6.2.4 Organize national cybersecurity exercises/drills

7.6.2.5 Identify metrics to evaluate the success of the exercises

7.6.2.6 Conduct periodic reviews of evolving threats to ensure that cyber defence policies continue to meet national security objectives

7.6.2.7 Enhance coordination regarding resilience of Internet infrastructure across public and private sectors

7.6.2.8 Establish a system to formally manage national infrastructure, with documented processes, roles and responsibilities, and redundancy.

7.6.2.9 Promote professional (private and public sector) and user understanding of the importance of anti-malware software and network firewalls.

7.6.3 Specific Objective 1: Cyber Defense

7.6.3.1 Develop and ensure that existing draft or National Security Strategy takes into consideration cyber defence component and identified threats to national security that might emerge from cyberspace.

7.6.3.2 Develop a communication and coordination framework for cyber defence, build on existing security structures

7.6.3.3 Establish a central command and control of cyber defence capabilities in the Gambia national army (GNA) to host and manage cyber defense

7.6.3.4 Establish cyber operations units in different branches of government and armed forces as appropriate

7.6.3.5 Develop communication and coordination framework for cyber defence.

7.6.3.6 Periodically assess and determine cyber defence capability requirements, involving public and private sector stakeholders

7.6.3.7 Expand coordination in response to malicious attacks on military information systems and national critical infrastructure

7.6.3.8 Establish training programmes for employees and develop awareness campaigns

7.6.4 Specific Objectives 2: Communications Redundancy

7.6.4.1 Ensure that the redundancy efforts are appropriately communicated to relevant stakeholders

7.6.4.1 Establish a process, to identify gaps and overlaps in emergency response assets communications and authority links

7.6.4.2 Create outreach and education activities of redundant communications protocols including the roles and responsibilities of each organization in the emergency response plan.

7.7 PROGRAMME 8: REMEDIATION PROGRAM

This program focuses on the development of security remedies and solutions to cyber-attacks through private sector partnership. This will be a joint undertaking with private organizations like software companies, educational institutions, IT security companies and other relevant organizations

8. DIMENSION 3: INSTITUTIONAL GOVERNANCE FRAMEWORK

8.1 STRATEGY 3: ORGANIZATION AND MOBILIZATION FOR CYBER SECURITY

This strategy pertains to the organization and mobilization of human, financial, and relevant resources for the implementation of the National Cyber Security Program. Mobilization as used in this section is the enlistment and active participation of all stakeholders in support of all programs listed herein.

8.1.1 Strategic Goal 1: To build sound institutional governance structure for effective coordination of national cyber security initiatives. Cyber Security Advisory Board, focal points or sector CSIRTs should be established to coordinate all policy and convergence effort of the government. The same shall lead in the formulation and implementation of all national cyber security programs and other related programs**.** The following actions should be taken in this regard.

8.1.2 Specific Objective 1: Set-up Institutional Governance Framework for Cyber Security.

8.1.2.1 Establish National Cyber Security Advisory Board

8.1.2.2 Establish Focal Points

8.2 PROGRAMME 9: ESTABLISHING NATIONWIDE MONITORING POINTS

This program will establish Monitoring Points that will serve as listening posts for intrusions. They will be deployed at strategic points around the country. They will detect, gather and help analyze information with regard to intrusions. Envisioned as a public private sector partnership, it will support the program on threat assessment and detection.

9. DIMENSION 4: NATIONAL & INTERNATIONAL COOPERATION

9.1 PROGRAMME 10: ESTABLISHING PUBLIC AND PRIVATE PARTNERSHIP/COOPERATION

9.1.1 Specific Objectives 1: Public-Private Partnership Forum

This initiative is intended to establish mechanisms for a strong partnership public-private sector for cyber infrastructure protection. Cooperation, collaboration and coordination between the government and the private sector are vital components in the implementation of the National Cyber Security Plan. Public-private partnership will be in the form of:

9.1.1.1 Capacity-Building

9.1.1.2 Information-Sharing

9.1.1.3 Threat Assessment

9.1.1.4 Joint Management of Cyber Security Programs

9.1.1.5 Incident Reporting

9.1.1.6 Advocacy

9.1.2 Actions

9.1.2.1 Undertake the transition from IPV4 to IPV6 protocol and disseminate information on the benefits of the transition, especially IPV6 security features relating to confidentiality, authentication and data integrity.

9.1.3 Specific Objectives 2: National and International Partnership / Cooperation

This program initiative aims to forge partnerships with national, regional and international partners and organizations for sharing information and best practices, capacity building and law enforcement.

9.1.3.1 Facilitate informal cooperation mechanisms within the law enforcement and criminal justice system, and between law enforcement and third parties, both domestically and cross-border, in particular ISPs.

9.1.3.2 Allocate resources to support information sharing between the public and private sectors at the national level.

9.1.4 Specific Objective 3: Promote International Cooperation and Collaboration

9.1.5 Actions:

9.1.5.1 Strengthen collaboration with regional, international partners in combating cybercrime through conventions (Budapest),

9.1.5.2 Ensure ratification and accession to the AU Malabo Convention, ECOWAS OCWAR-C Regional strategy, among other African bilateral treaty agreements, especially through frameworks such as the 24/7 cybercrime Network, mutual legal assistance frameworks,

9.1.5.3 Develop a clear plan that outlines how to manage international collaboration across multiple areas such as law enforcement, incidence response, research and innovation in cyber security.

9.1.5.4 Subscribe to and participate in all relevant regional and international forums on cyber security.

10. DIMENSION 5: CYBER SECURITY CAPACITY BUILDING AND AWARENESS

10.1 PROGRAMME 11: ADVOCACY AND PUBLIC AWARENESS

This program initiative will focus on implementing a cyber-security advocacy program that will rally the general public to protect The Gambian cyberspace. This program will specifically focus on: **Computer Ethics, Computer Security and Incident Reporting.**

This program should be incorporated in the educational curricula of the Ministry of Basic and Secondary Education (MoBSE) and Ministry of Higher Education research science and Technology (MOHERST) and other tertiary institutions or training centers.

10.1.1 Strategic Goal 1: To build cyber security prevention and response capabilities and create cyber security awareness for Gambian citizens.

10.1.2 Specific objective1: Develop a National Cyber Security Awareness Program

10.1.4 **Specific Objective 2:** Enhance Cyber security awareness across the general public and national institutions

10.1.5 **Actions:**

10.1.5.1 : Speed up acceptance of the draft national cybersecurity strategy to fast track development and implementation of a national cybersecurity awareness-raising programme

10.1.5.2 GM-CSIRT to undertake a nationwide assessment to determine level of awareness of Cyber security across the nation in alliance with civil society organization such as ITAG or GCSA

10.1.5.2 Develop and implement a national roadmap for improving awareness of current cyber security trends and threats

10.1.5.3 Develop and disseminate National Cyber security best practices to engrain a Cyber security mindset in the public.

10.1.5.4 Undertake mandatory training of members of different organizations to enhance their understanding of cyber issues and how their organizations address these threats.

10.1.5.5 Create a single online portal linking to appropriate cybersecurity information and disseminate materials for various target groups.

10.1.5.6 Develop a dedicated awareness-raising programme for executive managers within the public and private sectors.

10.1.5.7 Integrate cybersecurity awareness-raising efforts into ICT literacy courses (for e.g.: using the computer and managing files, internet and email, concepts of IT) and initiatives at schools and universities.

10. 6 Specific Objective 3: Develop Cyber Security Education and Profession Training

10.6.1 Assign an institution Ministry for Basic & Secondary Education and the Ministry of Higher Education) to develop a national curriculum on cybersecurity related courses and requirements/standards.

10.6.2 MOICI should dedicate a national budget for coordinating cybersecurity education and research

10.6.3 Develop qualification programmes for cybersecurity educators and start building a cadre of existing and new professional educators.

10.6.4 Integrate specialized cybersecurity courses in all computer science degrees at universities and offer specialized cybersecurity courses in other professional bodies.

10.6.5 Ensure Cybersecurity Awareness introductory course in introduce in ALL University courses.

10.6.6 Design specific cybersecurity programmes at the Bachelor or Master levels and consider hosting annual cybersecurity competitions for students.

10.6.7 Introduce more technical/ICT related courses at high school level in order to initiate students early-on before they begin studies at university.

10.6.8 Cybersecurity courses taught at Gambian universities should include ICT/computer lab components to support practical hands-on experience.

10.6.9 Offer university scholarships or bursaries in order to make ICT education at postgraduate and doctoral level affordable.

10.6.10 Ensure higher education, private, public sector and stakeholders to develop an Industry Based Learning/Certification programme for students.

10.6.11 Identify training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT professionals.

10.6.12 Establish training for experts on various aspects of cybersecurity such as technical training in data systems, tools, models, and operation of these tools

10.6.13 Establish a knowledge exchange programme targeted at enhanced cooperation between training providers and academia

10.6.14 Create specific measures to help government and companies to retain skilled cybersecurity staff

10.6.15 Create a framework for cybersecurity Certification and accreditation for public and private sector professionals

10.6.16 Improve cybersecurity training conditions, including infrastructure (tools and equipment) in all region of The Gambia

10.7 Specific Objective 4: Promote collaboration and Information Sharing on Cyber security

10.7.1 Actions:

10.7.2 Create a national forum to enhance and promote information sharing and collaboration nationally on Cyber security in collaboration with NCCD.

10.7.3 Continuously update the citizens, the private sector and the public sector, on information related to cyber threats, vulnerabilities, incidents, activities across the nation to foster trust.

10.7.4 Promote measures to protect privacy and enable users to make informed decisions when and how they share their personal information online.

10.8 Specific Objective 5: Ensure online safety for vulnerable groups, especially children

10.8.1 Actions

10.8.2 Ensure a bill to legislate online safety of children of The Gambia is achieved

10.8.3 Develop and disseminate online safety guidelines and best practices to protect vulnerable groups in The Gambia, especially children, from cyber threats.

10.8.4 Deploy special awareness programmes to target and inform children and other vulnerable groups about safe and responsible use of the internet.

10.8.5 Promote, in collaboration with civil society, the secure use of internet based on indicators

10.8.6 Encourage ISPs to establish programmes that promote trust in their services

10.8.7 Establish Certification by third parties when introducing e-government services for citizens, implement security measures from the beginning and have them

10.8.8 Encourage the private sector, in particular telecommunication and ecommerce services to employ cybersecurity good (proactive) practices

10.9 Specific Objective 6: Deploy tools to ensure vulnerable groups such as children are safe online

10.9.1 Actions:

10.9.2 Promote the deployment of technical measures such as web filtering tools that prevent access to harmful content by children and other vulnerable groups.

10.9.3 Encourage ISPs and other services providers to make their clients, especially parents and guardians aware of how to leverage available tools, technologies to manage potential risks to vulnerable groups while accessing services online.

11. PROGRAMMEE 12: ESTABLISHING CORPORATE DISASTER AND RECOVERY PLAN

This program will require all CI's to have a Corporate Disaster and Recovery Plan that will define contingency measures in case of attacks or disasters. It will define systems and procedures for the immediate recovery and resumption of their normal operations. This plan will include the following:

11.1 Actions

11.1.1 Establish Redundancy and back-up systems

11.1.2 Conduct Rapid assessment of attack and extent of damages,

11.1.3 Determine vulnerabilities exploited and conduct of restoration procedures to avert or deter similar attacks previously experienced by the system

11.1.4 Adopt standard operating procedures (SOPs)

11.1.5 Coordinate with GM- CSIRT and law enforcement units

12. DIMENSION 6: LEGAL AND REGULATORY FRAMEWORK

12.1 STRATEGY 4: INSTITUTIONAL BUILD-UP

This strategy intends to institute reforms that are necessary to address the challenges of cyber threats. Regulatory and legislative changes will have to be undertaken to provide the necessary legal regime and policy environment.

12.2 Strategic Goal 1: To strengthen existing legal and regulatory framework to adequately address cyber-crime and facilitate the criminalization of acts related to cyber-crime

12.3 Specific Objectives 1: Passage of Cyber-crime Law

12.3.1 **Actions**

12.3.1.1 The Cyber Crime Bill 2019 should be enacted into law

12.3.1.2 The private sector to lobby for the passage of the bill if necessary

12.3.1.3 Ensure that a national child protection online legislation is successfully enacted and implemented in accordance with international and regional standards.

12.3.1.4 Ensure the development and implementation of specific provisions and procedures on the current and new consumer protection legal framework

12.3.1.5 Review and implement specific legal provision on e-commerce concerning cybercrime incidents, such as online fraud, spam, and phishing sites

12.3.1.6 Ratify and implement international, regional and national cybercrime instruments, including the Budapest and Malabo conventions.

12.4 Specific Objectives 2: Administration of justice

12.4.1 Actions

12.4.2 Create a special court to handle cybercrimes

12.4.3 Institutionalize relevant educational programs for lawyers and judge

12.4.4 Ensure resolution of issues and problems related to Evidence Law or more specifically, the admissibility of electronic evidence in computer crime prosecutions.

12.4.5 Ensure investment in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases

12.5 Specific Objectives 3: Establish Security Standard

12.5.1 Actions

12.5.2 Develop a program to identify, adapt and/or adopt international information risk management standards applicable to government agencies, personal and/or ICT infrastructure, solutions

12.5.3 Adopt and implement by all government agencies of relevant international and local standards such as ISO 27001/02 and those promulgated by the Standards Bureau under ISO 9001:2000 quality management systems requirements;

12.5.3 Adopting an Information Security Management System (ISMS) ISO27001/02 as a requirement in the Integrated Information Systems Plan of each government agency

12.5.4 Promote adoption of international IT and cybersecurity standards for procurement.

12.5.5 Promote the adoption of relevant standards in software development.

12.5.6 In partnership with academia and civil society, gather and assess evidence of software quality deficiencies and it impact on usability and performance

12.5.7 Promote adoption and implementation of international IT and cybersecurity standards among private sector companies

12.6 Specific Objectives 4: Building the Capacity of Law Enforcement

12.6.1 Actions

12.6.1.1 Institutionalize training of law enforcement agencies on computer Forensics, Investigation and Handling of digital evidence.

12.6.1.2 Build capacity of cyber security professionals.

12.6.1.3 Establish partnerships with foreign governments and international organizations.

12.6.1.4 Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources

12.6.1.4 Build a cadre of specialized prosecutors and judges on cybercrime and electronic evidence to investigate, prosecute and process cybercrime-related cases

12.6.1.5 Collect and analyze statistics and trends regularly on cybercrime investigations, prosecutions and convictions.

12.7 Specific Objectives 5: Knowledge Management (KM)

This initiative is the adoption of Knowledge Management as a means to provide knowledge to all stakeholders. Experiences, technological innovations and best practices on cyber security have to be acquired, re-created stored and disseminated to improve cyber security programs.

12.7.1 Actions

12.7.1 Establish Knowledge Centers that can provide information resources to law enforcement units, CI operators, ICT security managers, government personnel and others;

12.7.2 Establish collaboration with relevant international KM organizations

13. PROGRAMME 12: BUILDING CYBER SECURITY INDUSTRY

13.1. Strategic Goal 1: To develop a stronger cyber security industry and to ensure a resilient cyber space.

13.1.1 Specific Objectives 1: Foster Innovation through Research and Development.

This will undertake research and development including, but not limited to, the following areas: Cryptography, Information Warfare, Intrusion Detection, Hacking, and Vulnerability Assessment.

13.2 Actions

13.2.1 Revise the National Research Agenda to promote R&D in Cyber security in The Gambia

13.2.2 Promote professional (private and public sector) and user understanding of the importance of deploying Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS

13.2.3 Encourage ISPs to establish policies for technical security control deployment as part of their services

13.2.4 Encourage the development and dissemination of cryptographic controls across all sectors for protection of data at rest and in transit, according to international standards and guidelines.

13.2.5 Encourage Web service providers to deploy state of art tools such as SSL and TLS to protect communications between servers and browsers as part of their standard packages

13.2.6 Raise public awareness of secure communication services, such as encrypted/signed emails.

13.2.2 Establish a National Centre of Excellence for Cyber security Training & Research

13.2.3 Review and update primary, secondary and tertiary level education curriculum to include cyber security elements

13.2.4 Support Cyber security competitions and R & D projects in Universities and Gambian Secondary Schools

13.2.5 Support national enterprises providing Cyber security solutions, and undertaking R & D in Cyber security

13.2.6 Collaborate with universities, colleges and the private sector to create new studies and internship programs on cyber security

13.2.7 Collaborate with the private sector and academia to support participation of government institutions, universities, private sector in regional and international research projects and exercises relating to Cyber security

13.2.8 Create standards in Cyber security training and education

13.2.9 Train ICT personnel of various Government ministries and institutions on how to detect incidents, report incidents, and collaborate with the GM-CSIRT and institutions from other sectors on Cyber security jointly undertaken with the private sector and relevant international organizations.

14. INSTITUTIONAL FRAMEWORK

14.1 Roles and Responsibilities

This section describes the roles and responsibilities of key actors involved in the implementation of the strategy:

14.2 Ministry of Information Communication & infrastructure (MOICI)

MOICI is the government entity or national Authority responsible for creating conducive legal and regulatory environment for the safe use of ICTs and confidence in cyberspace, by developing relevant policies, laws, and regulations that enable the smooth functioning of the ICT sector of The Gambia.

MOICI is primarily responsible for leading, planning and coordinating the implementation of the National Cyber security Strategy through collaboration with other stakeholders. MOICI will through GM-CSIRT, monitor the cyberspace to provide pro-active and reactive responses to cyber threats and risks.

GICTA will implement the National Cyber Strategy as well as keep oversight but report to MOICI. MOICI will through GICTA provide regulatory oversight of the ICT sector of The Gambia and ensures compliance to relevant cyber security-related frameworks within the ICT sector.

14.3 National Cyber Security Coordination Directorate (NCCD)

The NCCD is a Directorate under the National ICT Agency (GICTA). The NCCD advises and provide support role to the permanent secretary of MOICI. NCCD also monitors the application of the strategy and its successful implementation in coordination with NCSC.

14.4 National Cyber Security Commission (NCSC)

This body serves as the advisor to the national authority in charge of cyber security on all aspects of the cyber security strategy from its formulation, to its implementation and review (MOICI).

The NCSC ensures that the relevant public and private stakeholders are identified, mobilized and leveraged. It composition is multi-sectoral involving all major stakeholder including civil society.

14.5 Ministry of Justice (MoJ)

The Ministry of Justice (MoJ) will lead prosecution of cybercrime in consultation with relevant stakeholders such as MOI, MOICI, GM-CSIRT and GICTA. Under the GM-CSIRT, they will continuously monitor the cyberspace and help entities mitigate threats.

14.6 Ministry of Defense (MoD)

This Ministry will be responsible for setting the defense policy to guide the implementing agencies on matters of National Security. This includes the Gambia national Army and the State Intelligence Service (SIS) respectively to undertake their cyber related activities in line with the policy.

14.7 Ministry of the Interior & Gambia Police Force (GPF)

The Gambia Police Force (GPF) and other law enforcement agencies under the interior ministry will be responsible for the investigation and enforcement of cybercrimes in The Gambia. They will also play a vital role in collaborating with national and international stakeholders and partner law enforcement agencies in combating cybercrime.

14.8 The Gambia Computer Security Incident Response Team (GM-CSIRT)

The Gambia CSIRT serves as the governmental and national operational cyber security centre. It is also a resource centre for cyber security professionals. GM-CSIRT will continuously monitor The Gambia cyberspace to identify and address cyber threats and risks to the National Security.

It will also promote training and awareness and will work with other security agencies and private sector to safeguard and combat cybercrime/ cyber terrorism, maintain law and order during national incidents or emergencies.

14.9 Critical Information Infrastructure (CII) Owners and Operators

CII owners and/or operators in The Gambia will be responsible for protecting their infrastructure from cyber threats and vulnerabilities. To this end, they will ensure that various mitigation measures are implemented to protect the CII. They will also be responsible for ensuring that they comply with various cyber security-related frameworks in force in The Gambia.

14.10 Academia

Academia will play a key role in the national efforts in developing capacity and expertise in cyber security to address The Gambia's requirements for skilled and knowledgeable cyber security professionals both present and in the future. The University and the Industry will play a leading role in undertaking cyber security-related R&D.

14.11 Civil Society

The Civil Society of The Gambia will work with relevant stakeholders to promote effective engagement, promote transparency and accountability of the public and private sector institutions, and strengthen knowledge and awareness of cyber security related issues across The Gambia.

14.12 Private Sector

The Private Sector will be responsible for protecting the data, services and systems they own, provide and operate respectively, and as such will be responsible for ensuring their compliance with national laws, policies, standards, procedures and frameworks relating to Cyber security.

14.13 Citizens

The citizens will be expected to take appropriate steps in order to safeguard themselves in cyberspace against cyber threats and attacks. They will further be expected to utilize the information and messages available on the safe use of the cyberspace.

14.14 Cost of Implementation

Funding and Resources for the successful implementation of The Gambia's NCSS is dependent on adequate funds and resources. Considering that ICTs and Cyberspace spur socio-economic growth, the National Cyber security strategy implementation logical frameworks have funding sources for various measures proposed in the Strategic Action Plan.

14.15 Monitoring & Evaluation

To be able to monitor and evaluate the implementation of national Cyber security strategy, establishing a formal process is fundamental.

This sector is about monitoring the progress of implementation of the strategy and evaluating the outcome of the strategy. The Monitoring and Evaluation of NCSS will require a framework that:

14.15.1 Support attainment of the NCSS Vision and Strategic Goals

14.15.2 Enables accurate reporting on progress and identification of lessons learned and challenges encountered for informed decision making and effective planning.

This above actions will elaborate new measures as well as amend and tailor existing initiatives under the strategy. Monitoring and evaluation section details the proposed systematic approach to monitoring and evaluating progress as an integral part in the implementation the NCSS of The Gambia. The monitoring should be periodic in order to track progress of implementation of the NCSS.

The monitoring will, therefore, focus on periodic and objective assessment of progress towards the attainment of the set objectives. The key objectives of the monitoring and evaluation approach are:

14.15.3 Establish performance targets for various governmental institutions or relevant stakeholders responsible for implementing specific actions of the NCSS.

14.15.4 Develop performance plans to establish a shared understanding of the expected end results, the approach to achieving these end results and identify the resources necessary to ensure a successful implementation. The plans will be based on the KPIs, Performance targets and deadlines provided in the Implementation of Logical Framework.

14.15.5 Monitor and report performance and progress in achieving expected end results by identifying and promptly reporting observed or likely deviations.

14.15.6 Periodically evaluate institutional or individual performance against established performance targets.

14.15.7 An independent stakeholder should be commissioned to undertake the mid-term and long- term reviews of the strategy to determine the long-term impact and outcomes of the strategy if necessary effect remedial actions to keep implementation on track.

14.15.8 Ministry of Information & Communications Infrastructure (MOICI) and all relevant stakeholders will develop a comprehensive Monitoring and Evaluation Plan which will be based on the proposed approach.

14.15.9 The monitoring and evaluation plan will enable the assessment of the operational issues encountered during the implementation of the strategy, as well as the assessment of the long-term impact and outcomes of the strategy based on periodic reviews.

14.15.10 The Monitoring and Evaluation Plan will also provide mechanisms or tools for data collection and reporting, and further information on the roles and responsibilities of stakeholders, and frequency of reports.

APPENDIX (A) Monitoring and Evaluation Framework

Framework to Monitor and Evaluate Progress

Monitoring and Evaluation of the Strategic Goals		
Objective 1: Identify and protect Gambia's Critical Information Infrastructure		
Support & Implementing Agencies and their assigned responsibilities	**Supporting Agency**	**Responsibility**
	MOICI	
	GICTA	
Specific Objectives critical success factors	Commitment of stakeholders to identify and produce publish/Documented National CII register	
Implementing Risk factors	Delay or failure to identify and or document NCII	
Objective 2: Strengthen Cyber Intelligence Collection		
Support & Implementing Agencies and their assigned responsibilities	**Supporting Agency**	**Responsibility**
	State Intelligence Service(SIS), Gambia Arm Forces (GFA), Gambia Police Force	
	/NCCD,GM-CSIRT	
Specific Objectives critical success factors	Commitment of stakeholders to implement and strengthen cyber intelligence collection mechanism and methods	
Implementing Risk factors	Lack of resources, manpower, stakeholders commitment to implement and strengthen cyber intelligence collection	

Objective 3: Building Robust Systems

	Time Bound Measurable Target	
Supporting implementing Agencies and their assigned responsibilities	**Supporting Agency**	**Responsibility**
	Sector IT Units/ Operation Units	
	Units in MDAs	
Specific Objectives critical success factors	Commitment and support from stakeholders to implement intrusion detection systems, review, monitor vulnerabilities, assess threats and conduct periodic security Audits	
Implementing Risk factors	Lack of capacity, commitment and funding support from relevant sectors or agencies	

Objective4: Establish and strengthen Gambia Computer Security Response Units

	Time Bound Measurable Target	
Supporting implementing Agencies and their assigned responsibilities	**Supporting Agency**	**Responsibility**
	MOICI/GM-CSIRT/	
	GCITA/NCCD/	
Specific Objectives critical success factors	Commitment to fully operationalize GM-CSIRT, establish mandate, equipped and train the personnel.	
Implementing Risk factors	Delay in the implementation drive, lack of support, funding and or commitment from supporting Agency	

Objective 5: Enhance Police Cybercrime Response Unit

	Time Bound Measurable Target	
Supporting implementing Agencies and their assigned responsibilities	**Supporting Agency**	**Responsibility**
	Ministry of Interior	
	/Ministry of Justice/GPF	
	Commitment to facilitate creation of cybercrime	

Specific Objectives critical success factors	Response Unit within the Police Force; recruit, train and equip personnel for implementation	
Implementing Risk factors	Lack of commitment, resources, funding, and manpower from the supporting agency	
Objective 6: Facilitate Recruitment and Retention of Cyber Security Expertise in The Gambia		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agency	**Responsibility**
	MOICI	
	GICTA/NCCD	
Specific Objectives critical success factors	Commitment and involvement of all stakeholders in the development of national career progression policy, training and education in cyber security incident response	
Implementing Risk factors	Delay in implementation, lack of manpower, funding and support.	
Objective 7: Establish Secure and Reliable environment for e-Government and e-Commerce with National Public Key Infrastructure		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agencies	**Responsibility**
	MOICI/ GICTA/	
	NCCD/IFMIS/Gambia Chamber of Commerce	
Specific Objectives critical success factors	Commitment of creating a secure and reliable e-government and e-Commerce systems. Raise awareness of e- services and security features by stakeholders	
Implementing Risk factors	Lack of support, funding and opportunities	
Objective 8: Strengthen Mechanism to Manage Crisis, Prevent Damage and Losses		
Supporting implementing Agencies and	**Time Bound Measurable Target**	
	Supporting Agency	**Responsibility**

their assigned responsibilities	GM-CSIRT /NDMA GICTA /NCCD/NCSC	
Specific Objectives critical success factors	Commitment to develop a implement National Disaster Recovery and Business Continuity Plan	
Implementing Risk factors	Delay in implementation, lack of manpower, funding and support from stakeholder members	
Objective 9: Cyber Defense		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agencies	**Responsibility**
	Ministry of Defense(MoD) GAF/SIS/ MOICI	
Specific Objectives critical success factors	Commitment to include cyber defense component in the National security strategy, implement coordination framework, establish cybersecurity operational command and control units in the GAF and SIS	
Implementing Risk factors	Failure to include Cyber defense Component, Lack of support, funding and necessary resources	
Objective 10: Communication Redundancy		

Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agency	**Responsibility**
	GICTA	
	/NCCD Private stakeholders	
Specific Objectives critical success factors	Commitment to established appropriate communication channel are involving all stakeholders	
Implementing Risk factors	Delay in implementation, funding and support from stakeholder members	
Objective 11 : Institutional Governance Framework for Cyber Security		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agencies	**Responsibility**
	MOICI/GM- CSIRT	
	NCCD/NCSC	
Specific Objectives critical success factors	Commitment to implement NCCD establishment and NCSC including the creation of sector CSIRTs/IT Operations Units by stakeholder members	
Implementing Risk factors	Lack of support, funding and manpower	
Objective 12: Public & Private and International Partnership Cooperation		
	Time Bound Measurable Target	

Supporting implementing Agencies and their assigned responsibilities	**Supporting Agencies**	**Responsibility**
	MOICI/GICTA PUBLIC – PRIVATE OPERATORS	
	NCCD/NCSC	
Specific Objectives critical success factors	Stakeholders commitment to establish and promote strong public–private partnership, regional including International Cooperation	
Implementing Risk factors	Lack of support, framework for public and private sector partnership, relevant cooperation agreements and funding.	
Objective 13: Develop a National Cyber Security Awareness Program		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agency	**Responsibility**
	MOICI/NCCD	
	GM-CSIRT	
Specific Objectives critical success factors	Commitment to build and strengthen cybersecurity prevention and response, awareness and education programs	
Implementing Risk factors	Delay in implementation, lack of manpower, funding and support from stakeholder members	
Objective 14 : Enhance Cyber Security Awareness across Civil society and national Institutions		

Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agencies	**Responsibility**
	MOICI/GM- CSIRT	
	NCCD/NCSC	
Specific Objectives critical success factors	Commitment to strengthen cybersecurity awareness in both public, private institutions and civil society	
Implementing Risk factors	Lack of support, funding and involvement of concern stakeholders	
Objective 15: Develop Cyber Security Education and Professional Training		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agencies	**Responsibility**
	MOICI/ GM- CSIRT NCCD MoBSE/MOHERST	
Specific Objectives critical success factors	Commitment to develop and roll out Cyber Security curriculum including awareness into Basic, Secondary, Tertiary and University Educational system	
Implementing Risk factors	Lack of support, funding and necessary resources	
Objective 16: Promote collaboration and Information sharing on Cyber security		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agency	**Responsibility**
	MOICI	
	NCCD/ NCSC/ GM- CSIRT	

Specific Objectives critical success factors	Commitment to create a national forum to promote information sharing and collaboration by NCCD/NSCS including stakeholder members	
Implementing Risk factors	Delay in implementation, lack of manpower, funding and support from stakeholder members	
Objective 17 : Ensure online safety for vulnerable groups, especially children		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agencies	**Responsibility**
	MOICI/ GISTA NCCD/ GM- CSIRT	
	PRIVATE OPERATORS	
Specific Objectives critical success factors	Commitment to establish preventive mechanism to promote online safety for vulnerable groups and children and to enhance technical capacity by supporting Agencies	
Implementing Risk factors	Delay in implementation, lack of manpower, funding and resources	
Objective 18 : Deploy Tools to Ensure Vulnerable Groups such as Children are Safe Online		

	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	MOICI/ GISTA NCCD/ GM-CSIRT	
	PRIVATE OPERATORS	
Specific Objectives critical success factors	Commitment to implement safety tools to secure children or vulnerable groups online.	
Implementing Risk factors	Lack of support, funding and required resources	
Objective 19: Passage of Cyber-crime and other Laws		
	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	MOICI& Ministry of Justice	
	NCCD	
Specific Objectives critical success factors	Commitment by state holder to enacted cybercrime bill 2019 and to pass a child online protection bill in the national assembly. In addition, ratification of international protocols such as the Budapest, Malabo conventions should be pursued.	
Implementing Risk factors	Lack of resources, support and funding	
Objective 20: Administration of Justice		

Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agency	**Responsibility**
	Ministry of Justice/	
	MOICI	
Specific Objectives critical success factors	Commitment to review, establish special court on cybercrime, strengthen capacity of personnel of the judiciary and other law enforcement by stakeholders.	
Implementing Risk factors	Delay in implementation, lack of manpower, funding and support	
Objective 21 : Establish Security Standard		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agencies	**Responsibility**
	MOICI/GICTA GM- CSIRT	
	NCCD	
Specific Objectives critical success factors	Commitment to establish and implement a unified information security assurance policy mechanism to government agencies based on international standards (ISO-IEC27001, ISO/IEC20000, ISO-22301, ISO 9000 and ISO-14000 by stakeholders	

Implementing Risk factors	Lack of resources, support and funding.

Objective 22: Building the Capacity of Law Enforcement

	Time Bound Measurable Target	
	Supporting Agency	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	MOICI/NCC	
	GPF/GM-CSIRT	
Specific Objectives critical success factors	Commitment to develop a training programme and enhance the technical capacity of Law enforcement by stakeholders. Commitment to establish and institutionalize cybersecurity training in public and civil society by stakeholder members	
Implementing Risk factors	Delay in implementation, lack of manpower, funding and support from stakeholder members	

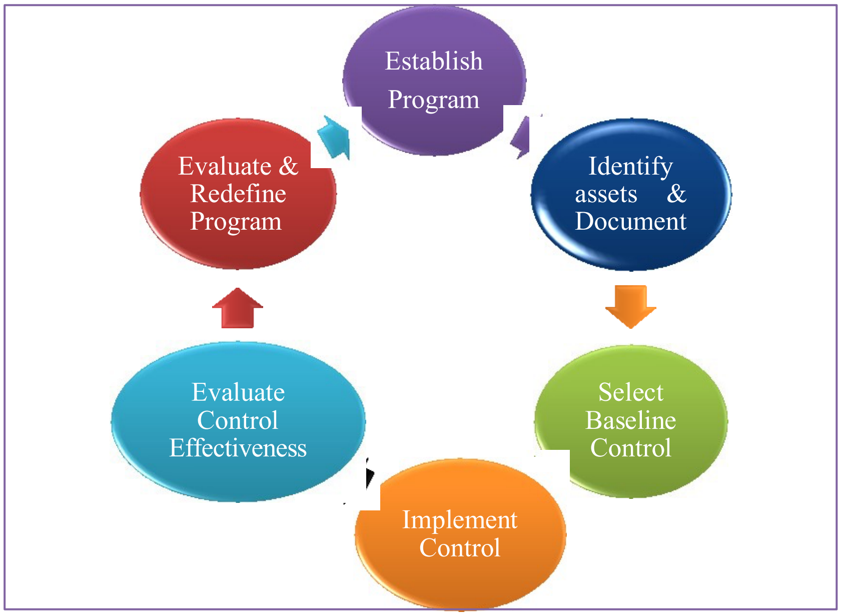
Objective 23 : Knowledge Management (KM)

	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	MOICI/GM- CSIRT/ NCCD/ RELEVANT SECTORS	
	NCCD	
Specific Objectives critical success factors	Commitment to establish knowledge management centers and strengthen collaboration between stakeholders	
Implementing Risk factors	Lack of resource, support and funding	

Objective 24: Foster Innovation through Research and Development		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	Supporting Agencies	**Responsibility**
	MOICI/GM- CSIRT	
	NCCD/MOHERST UNIVERSITY/PRIVATE SECTOR	
Specific Objectives critical success factors	Commitment to establish and promote Cyber Security research and development (R &D) in the Gambia.	
Implementing Risk factors	Lack of support, funding and international cooperation	

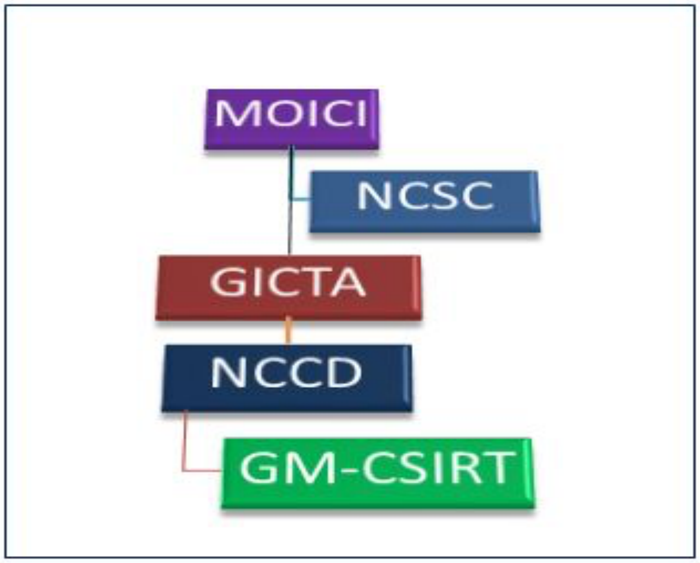
APPENDIX (B) Cyber Security Program Risk Assessment Flow

CYBER SECURITY PROGRAM RISK ASSESSMENT FRAMEWORK


Establish Program
Identify assets & Document
Select Baseline Control
Implement Control
Evaluate Control Effectiveness
Evaluate & Redefine Program

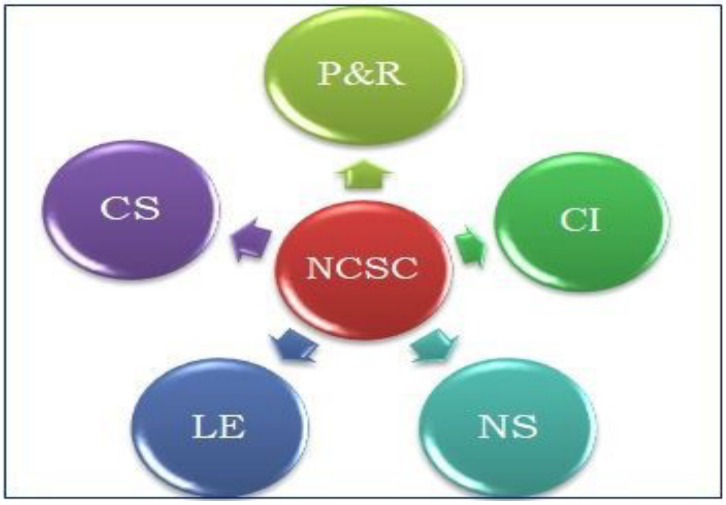
APPENDIX (C) Cyber Security Governance Organogram

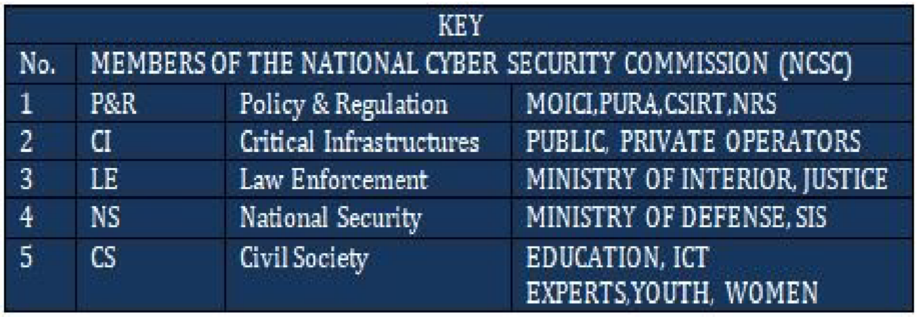
THE GAMBIA CYBER-GOVERNANCE/COORDINATION OGANOGRAM



Appendix (D) National Cyber security Commission Committees

NATIONAL CYBER SECURITY COMMISSION COMMITTEES





KEY			
No.	MEMBERS OF THE NATIONAL CYBER SECURITY COMMISSION (NCSC)		
1	P&R	Policy & Regulation	MOICI,PURA,CSIRT,NRS
2	CI	Critical Infrastructures	PUBLIC, PRIVATE OPERATORS
3	LE	Law Enforcement	MINISTRY OF INTERIOR, JUSTICE
4	NS	National Security	MINISTRY OF DEFENSE, SIS
5	CS	Civil Society	EDUCATION, ICT EXPERTS,YOUTH, WOMEN

APPENDIX (E) LOGICAL FLOW OF ACTION PLAN

THE GAMBIA NATIONAL CYBERSECURITY STRATEGY ACTION PLAN 2020-2024

DIMENSION 1: NATIONAL RISK ASSESSMENT

STRATEGY 1: UNDERSTANDING RISK

P.1 - PROGRAMME: NATIONAL THREAT ASSESSMENT

Strategic Goal 1: To identify and Manage Critical Information Infrastructure of The Gambia

1.1 Specific Objective: 1 Identify, classify, assess risk and protect Gambia's Critical Information Infrastructure

Code	Strategies/Action	Deliverables/Outputs	Lead Implementing Institution/Support	Timeline	Budget	Performance Indicators	Funding Sources
1.1.1	Establish a National CII register	Develop National CII register Document Comprehensive inventory of CII classify CII based on risk level and criticality	MOICI/GICTA	3rd Quarter 2020	$30,000	Publish/Documented National CII Register	MOICI/GICTA

1.1.2	Develop a national CII Governance Framework providing details on CII protection procedures and processes	National CII governance framework	MOICI/GICTA	3rd Quarter 2020	$27,500	Publish/Documented national CII governance framework with details on CII protection procedure and processes	MOICI/GICTA
1.1.3	Establish a national Risk register and regulations and/or guidelines that promote continuous risk assessment and management across CIIs in The Gambia	Risk assessment and management guidelines for CIIs national Risk Register	MOICI/ GICTA	September 2021 To January 2022	$35,000	Frequency of Risk assessment exercises Frequency of updates to national Risk Register	MOICI/ GICTA MOICI/GICTA
1.1.4	Develop standards and guidelines for Audit and protection of CNII	Develop standards/Guidelines for CNII	MOICI/ GICTA Standard Bureau	February – June 2021	$24,000	An approved standards or CII	MOICI/ GICTA Standard Bureau
DIMENSION 2: BUILDING CYBER SECURITY CAPABILITIES							
STRATEGY 2: CONTROLING RISK							
P.2 PROGRAMME: PREVENTIVE CAPABILITY PROGRAM							
Strategic Goal 1: Establishing Measures to Prevent Cyber Attacks							

2.1 - Specific Objective 1: Strengthen Cyber Intelligence Collection

Code.	Strategies/Action	Deliverables/Outputs	Lead Implementing Institution/Support	Time Frame	Budget	Performance Indicators	Funding Sources
2.1.1	Set up a Cyber Security Special Operations Unit.	Make sure special Cyber Security operations unit is establishment in the security services	GPF/ GAF/SIS	July 2021 To December 2021	$42,000	Enough manpower f\ully resourced and professionalism	GAF/SIS/GPF/ MoD
2.1.2	Develop monthly National Intelligence Estimates (NIE) targeting strategic and operational intelligence on cybercrimes	Produce Monthly Intelligence Estimate	GAF/SIS/GPF/ Ministry of Defence	Continuous	$18,000	Quality intelligence collection and methods	GAF/SIS/GPF/ MoD
2.1.3	Develop and manage cyber-criminal Database	Implement and commission a cyber-criminal database system	SIS to lead implementation of a centralised system	January 2022 To September 2022	$10,000	Regular updates , information sharing and inter-service cooperation	MoD/SIS
2.1.4	Ministry of Defence and SIS to develop and implement inter-service cyber-intelligence training program	Deliver appropriate training program for the specialised Cyber Security Operations Unit	GAF/SIS/GPF/ Ministry of Defence (Refresher and continuous professional trainings)	January 2022 To December 2022	$15,000	Regular training of personnel, program scoping and international partnership	MoD/SIS
2.1.5	Develop information assurance policies and standards	Approved policies and standard operating procedures (SOP)	GAF/SIS/GPF/ Ministry of Defence	January 2023 To March 2023	$14,000	Sop developed, implemented and audited	GAF/SIS/GPF/ Ministry of Defence

P.3 PROGRAMME 3 PROTECTIVE CAPABILITY PROGRAM

Strategic Goal 1: Building Robust Systems

Code.	Strategies/Action	Deliverables/Outputs	Lead Implementing Institution/Support	Time Frame	Budget	Performance Indicators	Funding Sources
2.2.1	Procure Host and Network based Intrusion Detection System and monitor to detect intrusion	Implement cutting-edge intrusion detection system	Sector CSIRT/IT Units in MDAs	January 2023 To June 2023	$9,000 Enterprise version	Ability to monitor cyber-attacks and potential intrusion real-time	Sector CSIRT/IT Ops Units in MDAs
2.2.2	Operations Security (OPSEC) – Review systems vulnerability, procedures, handling of classified and critical information.	Conduct Periodic review of systems threats and vulnerabilities	Sector CSIRT/IT Units in MDAs	Periodically	$5,000 annually	Conduct information security Auditing and compliance	Sector CSIRTT/IT Units in MDAs
2.2.3	Conduct periodic Security Audit to identify vulnerabilities and ensure compliance with security programs and standards	Security audit reports indicating system errors, vulnerabilities	GM-CSIRT/NCCD	Periodically	$7000 annually	Number and frequency of security audits and tests; Effectiveness of security audits and tests Effectiveness of intrusion detection tests/systems	GM-CSIRT/NCCD

2.2.4	Consumer Protection – Establish mechanism to address consumer protection, technology and product quality assurance.	Produce framework on technology product quality standards	GM-CIRT/NAQAA	Periodically	$6,500	Implementation of the standards and consumer protection quality Audit	GM-CIRT/NAQAA

P.4 PROGRAMME: RESPONSE CAPABILITY PROGRAM

3. Strategic Goal 1: Establishing Computer Security Response Units

Code.	Strategies/Action	Deliverables/Outputs	Lead Implementing Institution/Support	Time Frame	Budget	Performance Indicators	Funding Sources
2.3.1	Expedite the operationalization of a GM-CSIRT with clear processes, defined roles and responsibilities	Establish and operationalize GM-CSIRT	MOICI/ GICTA/NCCD	September 2020 To August 2021	$23,600	Extent of operationalization of GM-CSIRT Effectiveness of GM-CSIRT	MOICI/ GICTA/NCCD
2.3..2	Continuously develop the capacity of GM-CSIRT staff to address the fast-changing technical requirements, and develop	GM-CSIRT Training Program	MOICI/ GICTA/NCCD	March 2021 To August 2021	$27,800	Number and frequency of GM-CSIRT training sessions Number of	MOICI/ GICTA/NCCD

	abilities to actively obtain information in cyberspace, about current cyber risks and threats					incidents/attacks/threats/risks	
2.3.3	Develop a national incident reporting, information sharing and coordination mechanisms to address reporting of incidents and coordination in incident response	National incident reporting and information sharing framework	MOICI/ GM-CSIRT/GICTA	December 2020 To March 2021	$18,300	Effectiveness and adaptability of the incident reporting and information sharing awareness raising framework	MOICI/ GICTA/NCCD
2.3.4	Create and continuously update cyber security incident register, assess incidents, and suggest measures to resolve issues and mitigate threats and risks	Real time cyber security incident registers; Measures to mitigate threats, risks and resolve incidents	MOICI/ GICTA	Continuous	$16,500	Extent of update of incident registers; Extent of implementation of mitigation measures	MOICI/ GICTA
2.3.5	Strengthen GM-CSIRT capacity in terms of budget, technology and human resources with roles and responsibilities clearly defined	Capacitize GM-CSIRT in terms of budget, technology and manpower	MOICI/ GICTA/GM-CSIRT	January 2021 To February 2021	$9,000	Level of awareness of minimum and mandatory log requirement	MOICI/ GICTA

2.3.6	Continuously monitor, analyse and assess cyber threats and potential risks and be able to provide a real time overview of state of cyber security across the nation	Real time overview of the state of cybersecurity	MOICI/ GICTA/GM-CSIRT	Continuous	$12,500	Frequency of updates to overview of the state of cybersecurity	MOICI/ GICTA
2.3..7	Develop a Cybersecurity Governance Framework for defining roles and responsibilities of all stakeholders as well as describe SOPs and code of conduct in responding to incidents	Cybersecurity Governance Framework that roles and responsibilities of all stakeholders as well as describe SOPs and code of conduct in responding to incidents	MOICI/ GICTA/NCSC	January 2021 To June 2021	$20,200	Extent of effective response to incidents nationwide	MOICI/NCSC
2.3.8	Establish a call centre/help line for reporting incidents or seeking assistance with incidents	National Cyber Security Call Centre/Help Line	MOICI/ GICTA/ GM-CSIRT/NCCD	June 2021 To August 2021	$19,400	Number of calls to help line or call centre Extent of incidents addressed through call line	MOICI/ GICTA
2.3.9	Develop and implement cybersecurity incident simulation scenarios and programs that can be used during the national exercises/drills	Cybersecurity incident simulation scenarios and programs	MOICI/ GICTA/ GM-CSIRT	July 2021 To August 2021	$15,300	Usage of cybersecurity incident simulation scenarios and programs during national exercises	MOICI/ GICTA/NCCD

2.3.10	Develop update cybersecurity contingency plans, including roles of the military/security agencies during cyber-attacks and emergencies	Annual review of Sector specific contingency plans	MOICI/ GICTA/NCCD	Annually	$14,200	Level of awareness of Sector specific contingency plans	MOICI/ GICTA
2.3.11	Develop a Cyber Defence Strategy that details approaches to addressing threats to national security in cyberspace	National Cyber Defence Strategy	MOICI/ GICTA/NCSC	March 2021 To June 2021	$17,500	Extent of implementation of Cyber Defence Strategy	MOICI/GICTA
2.3.12	Establish a Central Defence Command and Control Centre for cybersecurity in The Gambia	A Central Defence Command and Control Centre for cybersecurity	Ministry of Defence/SIS	September 2021 To December 2021	$17,800	Extent of operationalization of a Central Defence Command and Control Centre for cybersecurity	MoD/SIS
2.3.13	Establish mechanisms for regional and international cooperation for incident response.	Signed Memorandum of understanding with partners	GM-CSIRT/NCSC	January 2022 To March 2022	$10,000	Number of Signed MoUs and extent of engagement with partners	GM-CSIRT/NCSC
2.3.14	Develop web portal to receive cyber complaints.	Commissioned Web portal to received cyber complaints	GM-CSIRT/GPF	September 2022 To December 2022	$12,000	Extent of awareness and inflow of complaints	GM-CSIRT/GPF

P.5 - PROGRAMME: ENHANCEMENT OF LAW ENFORCEMENT CAPABILITY							
Strategic Goal 1: Establishing Police Cybercrime Response Unit							
Code.	**Strategies/Action**	**Deliverables/Outputs**	**Lead implementing Institution/support**	**Time Frame**	**Budget**	**Performance Indicators**	**Funding Sources**
2.4.1	Undertake a gap analysis to identify gaps in current ICT Security, legal and regulatory framework Develop requisite instruments to address Gaps including issues relating to substantive, procedural, privacy and data protection.	An analysis of gaps in current ICT security legal and regulatory framework s Review instruments to address gaps including issues relating to substantive and procedural, privacy and data protection	MOICI/ Ministry of Justice	August 2021 To January 2022	$63,800	Enacted amendments to existing legislations or policies Enactment of new policies/legislations	MOICI/MOJ
2.4.2 2.4.3	Develop and publish a cybersecurity policy and standards To include general and sector-specific cybersecurity controls to be recognized as a national standard	A Cybersecurity Framework (CSF) consisting of general and sector-specific policies and controls	MOICI	January 2021 To April 2021	$17,700	Extent of adoption/implementation of a Cybersecurity Framework (CSF)	MOICI

	Create a national programme to promote the adoption of cyber standards across government institutions and CII in The Gambia	Deployment of national cyber standards across the nation	MOICI/GICTA	August 2021 To July 2022	55,250	Extent of adoption/implement-tation of cyber standards across the nation	MOICI/GICTA
2.4.4	Establish the requisite framework to operationalize a digital forensics laboratory	Operational digital forensics laboratory Plans and budgets to establish Digital forensics laboratory	Gambia Police Force Ministry of Justice	January 2022 To October 2022	$44,800	Extent of operationalization of Digital Forensics Lab	GPF/MOJ
2.4.5	Develop mandatory digital forensics and evidence handling courses for the judiciary, law enforcement and personnel from other related agencies involved in the detection and prosecution of cybercrime	Training programme on digital forensics and evidence handling procedures	Ministry of the Interior/ Gambia Police Force Ministry of Justice	Continuously (Annually)	$32,900 (Annually)	Number and frequency of mandatory courses and qualifications delivered to or acquired on cybercrime by judiciary and security personnel nationwide Number of successful prosecutions of cybercrimes	MOI/GPF GPF/MOJ

2.4.6	Build and enhance capacity to detect cybercrime incidents	Training Programme and Budget on cybercrime incident detection	Gambia Police Force Ministry of Justice	January 2022 To December 2024	$32,100 (Annually)	Number and frequency of mandatory courses and qualifications delivered to or acquired on cybercrime by judiciary and security personnel nationwide Extent of detection of cybercrimes	GPF/MOJ
2.4.7	Identify needs, provide training and education to develop the capacities of the law enforcement agencies, judiciary and the legal fraternity on how to interpret and enforce the policy, legal & regulatory frameworks on cybersecurity in The Gambia	Training programme for law enforcement agencies and judiciary on how to interpret and enforce the policy, legal & regulatory frameworks on cybersecurity in The Gambia Strong law enforcement and judiciary capable of enforcing the policy, legal & regulatory frameworks on cybersecurity	Ministry of Justice/Ministry of the Interior	Continuously	$35,000	Number of capacity building programmes conducted. Capacity of Law Enforcement and Judiciary in enforcing the policy, legal & regulatory frameworks on cybersecurity in The Gambia	MOJ/GPF

P.6 - PROGRAMME: GOVERNMENT CYBER SECURITY ENHANCEMENT PROGRAM

2.5 Strategic Goal 1: To safeguard Government Information Systems and Critical National Infrastructures against Cyber-Attacks

Code.	Strategies/Action	Deliverables/Outputs	Lead implementing Institution/support	Time Frame	Budget	Performance Indicators	Funding Sources
2.5.1	Establish mandatory and minimum technology and security requirements for equipment of ISPs and end users like the Banking sector	Mandatory and minimum technology and security requirements for equipment of ISPs and end user	GM-CSIRT CIIs, ISPs and other end users	September 2021 To January 2022	$17,950	Extent of identification of equipment that do not meet the minimum technology or security requirements	GM-CSIRT
2.5.2	Strengthen measures to improve security of government networks and IT systems	Develop and enforce security standards for the protection of government IT systems as well as online presence (websites, portals and databases)	GICTA/NCCD/ GM-CSIRT	January 2022 To January 2023	$22,000	Develop or improve relevant standards for protection of government IT Systems, online presence and procurement of IT products	GICTA

2.5.3	Develop a government programme to deploy and manage government ICT infrastructure	National programme to deploy and manage government ICT infrastructure	MOICI/GICTA	January 2022 Onwards	$17,500	Extent of implementation of national programme to enhance internet infrastructure	MOICI/GICTA
2.5.4	Develop a national programme to enhance internet infrastructure development and resilience	National programme to enhance internet infrastructure development and resilience	MOICI/GICTA/GSC	January 2022 Onwards	$17,500	Extent of implementation of national programme to enhance internet infrastructure development and resilience	MOICI
2.5.5	Develop National Contingency plans which identify emergency response asset priorities and standard operating procedures (SOPs)	National contingency plan	GICTA/ GM-CSIRT	January 2021 To June 2021	$18,400	Adoption of national contingency plan including the emergency response asset priorities and standard operating procedures (SOPs)	MOICI/GM-CSIRT
2.5.6	Review and update the map of current emergency response assets	Emergency response asset map	GICTA/ GM-CSIRT	Annually	$17,000	Completion of emergency response asset map	GM-CSIRT

2.5.7	Ensure communication channels are deployed across emergency response functions, geographic areas of responsibility, public and private responders, and command authority	Emergency Communication Network	MOICI/ GICTA	Continuously	$20,150	Extent of deployment of Emergency Communication Network	MOICI/ GICTA
2.5.8	**Specific Objective:1 Facilitate Recruitment and Retention of Cyber Security Expertise in The Gambia**						
2.5.8.1	Develop National and Career Progression Policy promoting continuous training and education for Incident response and addressing issues relating to cybersecurity	Training and education for incident response and addressing countermeasures for GM-CSIRT and security personnel Career progression strategy that promotes continuous professional education	Personnel Management Office (PMO) GICTA	September 2022 To January 2023	$21,500	Strategy Extent of national policy promoting continuous training and education	PMO /GICTA
2.5.8.2	Identify the staffing requirements for Government agencies and Critical Infrastructure operators and develop a national recruitment and retention	Set of staffing requirements for Government agencies and Critical Infrastructure operators Cybersecurity staffing recruitment and retention	Personnel management Office (PMO) GICTA	September 2022 To January 2023	$21,200	Extent of cybersecurity staffing recruitment and retention	PMO /GICTA

	strategy	strategy					
2.5.8.3	Develop and implement cybersecurity training and capacity building plans for Government personnel	National cybersecurity training and capacity building training plans for Government Personnel	Personnel management Office (PMO) GICTA/Labour	December 2022 Onwards	$37,500	Frequency of courses/ qualifications delivered / acquired	PMO /GICTA
2.5.9	**Specific objective 2 : Establish secure and reliable environment for e-Government and e-Commerce with National Public Key Infrastructure**						
2.5.9.1	Create, and periodically update the general public and other sectors on how cyberspace is securely used to deliver e-government and e-commerce services in The Gambia, highlighting the various security features deployed to foster trust.	Implement and raise awareness on National Public Key Infrastructure	GICTA/NCCD/GM-CSIRT	January 2023 To September 2023	$30,000	Frequency of updates and the involvement of general public	GICTA/NCCD/GM-CSIRT
2.5.9.2	Encourage the use of Public Key Infrastructure (PKI) for transactions to/from Government Ministries, Departments and Agencies to enhance high cyber security levels and trust in delivering	A national PKI that is recognised worldwide	GICTA/NCCD/GM-CSIRT	January 2023 To September 2023	$40,000	Establish primary and secondary sites and CSIRTificate Authority of national PKI	GICTA/NCCD/GM-CSIRT

	public services.						
2.5.9.3	Appoint cyber security inspectors who will serve as focal points of contacts to support small and medium enterprises in addressing cyber security needs and method of mitigating cyber threats	Appoint inspectors or focal points to extend cybersecurity support to small and medium enterprises	NCCD/GM-CSIRT	June 2022 To December 2022	$18,000 (Annually)	Enhanced protection for small and medium enterprises	NCCD/GM-CSIRT

P.7 - PROGRAMME: BUSINESS CONTINUITY / RESILIENCY PROGRAM

2.6 Strategic Goal 1: Establish Mechanism to Manage Crisis, Prevent Damage and Losses

Code.	Strategies/Action	Deliverables/Outputs	Lead implementing Institution/support	Time Frame	Budget	Performance Indicators	Funding Sources
2.6.1	Develop a national business continuity / disaster recovery / contingency plan with a cybersecurity component	Produce a national business continuity / disaster recovery / contingency plan	GICTA/NCCD	January 2023 To June	$25,000	Publish disaster recovery and continuity Plan and extent of implementation of the Plan	GICTA/NCCD
2.6.2	Designate cybersecurity exercise planning to GM-CSIRT in collaboration with Gambia National Disaster Management Agency (NDMA).	GM-CSIRT and NDMA to carry out cybersecurity exercise planning	GM-CSIRT/NDMA	September 2023 To December 2023	$38,000	Published schedule plan for national cybersecurity drills	GM-CSIRT/NDMA

2.6.3	Develop Framework to gauge the mitigation measures, protocols and techniques for crisis management.	Framework developed to evaluate mitigation measures	GICTA/NCCD	Continuous	$10,000	Publish framework to evaluate mitigation measures and techniques	GICTA/NCCD
2.6.4	Organize national cybersecurity exercises/drills Identify metrics to evaluate the success of the exercises	Lessons/Results of cyber drill exercise Frequent cyber drills	NCCD/GM-CSIRT/NDMA	continuous	$15,000	Number and quality of national drills	NCCD/GM-CSIRT/NDMA
2.6.5	Conduct periodic reviews of evolving threats to ensure that cyber defence policies continue to meet national security objectives	Review cyber threats periodically to meet national security objectives	GM-CSIRT/NCCD	Periodically	$12,000 (Annually)	Number of review and periodic system audit	GM-CSIRT/NCCD
2.6.6	Enhance coordination regarding resilience of Internet infrastructure across public and private sectors	Provide assurance on Internet Infrastructure Coordination and resilience	GICTA/NCCD	continuous	$20,000	Extent of Implementations of the coordination effort	GICTA/NCCD

2.6.7	Establish a system to formally manage national infrastructure, with documented processes, roles and responsibilities, and redundancy.	System establish to manage infrastructure	GICTA/NCCD	January 2021 To September 2021	$27,000	Evaluate systems performance periodically	GICTA/NCCD
2.6.8	Promote professional (private and public sector) and user understanding of the importance of anti-malware software and network firewalls	Awareness on the importance of antimalware software and network firewalls	GM-CSIRT/NCCD/ NCSC	Periodically	$10,000	Extent of awareness on anti-malware applications and network firewalls	GM-CSIRT/NCCD/ NCSC
2.6.9	Develop and test crisis management measures during cyber drills	National crisis management measures for Gambia's regular cyber drills	MOICI/ GICTA/GM-CSIRT	Annually	$15,400	Level of awareness of National crisis Management measures for The Gambia	MOICI/GICTA

2.6.10	Evaluate cyber drills to develop options on how to improve crisis management measures	Lessons/Results of cyber drill exercise Regular cyber drills	MOICI/ GICTA /GM-CSIRT	Annually	$13,100	Frequency of cyber drill exercises Number of revisions of contingency plans	MOICI/GICTA

2.6. 11 Specific Objective 1: Cyber Defence

Code.	Strategies/Action	Deliverables/Outputs	Lead implementing Institution/support	Time Frame	Budget	Performance Indicators	Funding Sources
2.6.11.1	Develop and ensure that existing draft or National Security Strategy takes into consideration cyber defence component and identified threats to national security that might emerge from cyberspace	National Security Strategy with Cyber defense component	Ministry of Defense/MOICI	Jan 2021 To April 2021	$8,000	Extent of inclusion of Cybersecurity Component in the Final Gambia National Security Strategy	MoD/MOICI

2.6.11.2	Develop a communication and coordination framework for cyber defence, build on existing security structures	Communication and Coordination Framework	Ministry of Defense/MOICI	September 2022 To December 2022	$10,000	Publish Communication and Coordination framework	MoD/MOICI
2.6.11.3	Establish a central command and control of cyber defence capabilities in the Gambia national army (GAF) to host and manage cyber defence	Command and Control centre hosted by GAF	Ministry of Defense/GAF	January 2022 December 2022	$45,000	Extent of operations of the Command and control Centre	MoD/GAF
2.6.11.4	Establish cyber operations units in different branches of government and armed forces as appropriate	Cyber Operations Units in Government Agencies	NCSC/NCCD/GM-CSIRT	January 2021 To December 2024	$12,000	Periodic Review of cyber security operation in all government sectors	NCSC/NCCD/ GM-CSIRT
2.6.11.5	Periodically assess and determine cyber defence capability requirements, involving public and private sector stakeholders	Periodic Cyber defense assessment involving public and private sector	Ministry of Defense/GAF	Periodically	$5000	Extent of involvement of public and private sector	MoD/GAF

2.6.11.6	Expand coordination in response to malicious attacks on military information systems and national critical infrastructure	Mechanism to response to attacks on military information systems and national critical infrastructure	GM-CSIRT/Ministry of Defense	Periodically	$7000	Mechanism in place and number of successful response preparedness	GM-CSIRT/MoD
2.6.11.7	Establish training programmes for employees and develop awareness campaigns	Training programmes for employees	GM-CSIRT/Ministry of Defense	September 2022 December 2022	$28,000	Scope of programme and quality of delivery	GM-CSIRT/MoD
2.6.12	**Specific Objectives 3: Communications Redundancy**						
2.6.12.1	Ensure that the redundancy efforts are appropriately communicated to relevant stakeholders	Communication channel to inform relevant stakeholder on issue of redundancy	GICTA/NCCD	continuous	$4000	Effectiveness of the channel of communication	GICTA/NCCD
2.6.12.3	Create outreach education activities of redundant communications protocols including the roles and responsibilities of each organization in the	promote awareness and education on redundant communication protocols	GICTA/NCCD	Annually	$30,000	Extent of outreach	GICTA/NCCD

	emergency response plan						
DIMENSION 3: INSTITUTIONAL GOVERNANCE FRAMEWORK							
STRATEGY 3: ORGANIZATION AND MOBILIZATION FOR CYBER SECURITY							
3. Strategic Goal 1: To build sound Institutional Governance Structure for effective Coordination of National Cyber Security Initiatives							
P.8 - PROGRAMME: ESTABLISHING NATIONWIDE MONITORING POINTS							
3.1	**Specific Objective 1: Set-up Institutional Governance Framework for Cyber Security**						
Code.	**Strategies/Action**	**Deliverables/Outputs**	**Lead implementing Institution/support**	**Time Frame**	**Budget**	**Performance Indicators**	**Funding Sources**
3.1.1	Establish National Cyber Security Advisory Board	Establish an advisory committees/commission	MOICI/PURA/MOJ	January 2021 To September 2021	$36,000	Extent of multi-sectoral involvement in the implementation	MOICI/PURA/MOJ

3.1.2	Establish Focal Points/IT units	Sectoral focal points or IT Units identified to work with GM CSIRT	MOCI/GICTA NCCD/GM-CSIRT	September 2020 To December 2020	$22,000	Extent of collaboration with GM-CSIRT	MOCI/GICTA
DIMENSION 4: NATIONAL & INTERNATIONAL COOPERATION							
STRATEGY 4 : INSTITUTIONAL AND POLICY BUILD-UP							
4. Strategic Goal 1: To establish mechanisms for a strong partnership public-private sector and to forge partnerships with national, regional and international partners and organizations.							
P.9 - PROGRAMME: ESTABLISHING PUBLIC AND PRIVATE PARTNERSHIP/COOPERATION							

4.1	**Specific Objectives 1: Public-Private Partnership Forum**						
Code.	**Strategies/Action**	**Deliverables/ Outputs**	**Lead implementing Institution/support**	**Time Frame**	**Budget**	**Performance Indicators**	**Funding Sources**
4.1.1	Strengthen collaboration with regional, international partners in combating cybercrime through treaties, conventions and bilateral agreements, especially through frameworks such as the 24/7 cybercrime Network, mutual legal assistance frameworks, etc.	Signatures of relevant international treaty agreements on cybercrime MOUs between countries and international partners Participation in international forums on cybercrime	MOICI PURA	Continuously	$17,800 (Annually)	Effectiveness and efficiency in international collaboration Extent of collaboration and information sharing internationally	MOICI PURA

4.1.2	Subscribe to and participate in all relevant regional and international forums on cybersecurity	Improved regional and international collaboration on cybersecurity Participation in relevant regional and international fora on cybersecurity	MOICI PURA GCSIRT	January 2021 Onwards	$22,500 (Annually)	Effectiveness and efficiency in international collaboration Extent of participation in regional and international for a on cybersecurity	MOICI PURA
4.1.3	From IPV4 to IPV6 protocol, disseminate information on the benefits of the transition, especially IPV6 security features relating to confidentiality, authentication and data integrity	Utilize IPV6 security features relating to confidentiality, authentication and data integrity	GM-CSIRT	February 2023 To January 2024	$42,850	Extent of awareness of the security features of the Transition	GM-CSIRT
4.1.4	Facilitate informal cooperation mechanisms within law enforcement and criminal justice system, and third parties, both domestically and cross-border, in particular ISPs	Set-up informal or cooperation mechanism between law enforcement and criminal justice	MOJ/MOI /GPF	Continuous	$25,000	Extent of Inter-agency cooperation and collaboration	MOJ/MOI /GPF

4.1.5	Allocate resources to support information sharing between the public and private sectors at the national level	Ensure resources are available to support information sharing	MOJ/GPF	Periodically	$23,000	Ability of public – private sector to share information at national level	MOJ/G

4.1.6	**Specific Objective 2: Promote International Cooperation and Collaboration**						
4.1.6.1	Strengthen collaboration with regional, international partners in combating cybercrime through conventions (Budapest)	Enhance collaboration Regional and International collaboration programmes and information sharing mechanism MOUs with International partners on the monitoring, analysis and management of cross border CII	MOICI/ GICTA	December 2020 To February 2021 (3) Months from adoption of Policy)	$31,000 (Initial) $21,000 (Annually)	Extent of International cooperation in the protection of CII	MOICI/ GICTA
4.1.6.2	Ensure ratification and accession to the AU Malabo Convention, ECOWAS OCWAR-C Regional strategy, among other African bilateral treaty agreements, especially through frameworks such as the 24/7 cybercrime Network, mutual legal assistance frameworks,	Making sure Gambia ratifies and domesticate the international protocols mentioned	MOICI/ MOJ/PURA/ GICTA	January 2021 To June 2021	continuous	Domesticate ratified protocols	MOICI/ MOJ/PURA/ GICTA

4.1.6.3	Develop a clear plan that outlines how to manage international collaboration across multiple areas such as law enforcement, incidence response, research and innovation in cyber security	Develop multi-sectoral and international Collaboration plan	MOICI/ NCCD NCSC/GM-CSIRT	Continuous	$5000	Produce Collaboration Plan	MOICI/ NCCD NCSC/GM-CSIRT
4.1.6.4	Subscribe to and participate in all relevant regional and international forums on cyber security.	Participate in international cyber security forums	NCCD NCSC/GM-CSIRT	Continuous	$25,000	Scope of participation in international forums	NCCD NCSC/GM-CSIRT

DIMENSION 5: CYBER SECURITY CAPACITY BUILDING, AWARENESS AND EDUCATION

STRATEGY 4 : INSTITUTIONAL AND POLICY BUILD-UP

Strategic Goal 1: To Build Cyber Security Prevention and Response Capabilities and create Awareness for Gambian Citizens

P.10 - PROGRAMME: BUILDING AWARENESS, EDUCATION AND TRAINING

5.1 **Specific Objectives 1: Develop a National Cyber Security Awareness Program**

Code.	Strategies/Action	Deliverables/Outputs	Lead implementing Institution/support	Time Frame	Budget	Performance Indicators	Funding Sources
5.1.1	Speed up acceptance of the draft national cybersecurity strategy to fast track development and implementation of a national cybersecurity awareness-raising programme	Secure approval of the draft national cybersecurity strategy to expedite awareness raising	MOICI/ NCCD/NCSC GM-CSIRT	September 2020 To December 2020	-	Final approval and implementation of awareness programme	MOICI/ NCCD/NCSC GM-CSIRT

5.1.2	GM-CSIRT to undertake a nationwide assessment to determine level of awareness of Cyber security across the nation in alliance with civil society organization such as ITAG or GCSA	Conduct National awareness assessment	GM-CSIRT/ Civil society/ Gambia Cyber Security Alliance/ITAG	February 2021 To September 2021	$24,000	Extent of assessment of national levels of cybersecurity awareness	GM-CSIRT/ Civil society/ Gambia Cyber Security Alliance/ITAG
5.1.4	**Specific Objective 2: Enhance Cyber Security Awareness across General Public and National Institutions**						
5.1.4.2	Develop and implement a national roadmap for improving awareness of current cyber security trends and threats	National roadmap for improving awareness of current cyber security trends Up to date and functional website with information current cyber security threats, risks, vulnerabilities, etc.; Awareness campaigns to raise awareness of cybersecurity trends and threats	MOICI GM-CSIRT	April 2021 To September 2021	$16,500	Level of awareness Number/frequency of cybersecurity campaigns Effectiveness of campaigns Number of revisions to website	MOICI GM-CSIRT/NCCD
5.1.4.3	Improve national awareness on cybersecurity/internet safety across all segment of Gambian	Conduct baseline public opinion survey to determine awareness level and attitude of Gambians on	NCCD/NCSC	January 2021 To		Develop and implement a comprehensive plan for cybersecurity	NCCD/NCSC

	society through targeted awareness campaign/advocacy	cybersecurity		February 2022		awareness campaign for different segments of Gambia society: all stakeholders	
5.1.4.4	Develop and disseminate national cybersecurity best practices to engrain a cybersecurity mind-set in the public	National cybersecurity best practices	GICTA/ GM-CSIRT	April 2021 Onwards	$16,500	Extent of dissemination of cybersecurity best practice	GM-CSIRT
5.1.4.5	Undertake mandatory training Members of different organizations to enhance their understanding of cyber issues and how their organizations address these threats	Mandatory training of Members of different organizations	PURA CII GM-CSIRT	April 2021 To September 2021	$23,500	Extent of knowledge of cybersecurity and how organizations address them	GICTA/ GM-CSIRT

5.1.4.6	**Specific Objective 3: Develop Cyber Security Education and Profession Training**							
5.1.4.6.1	Assign Ministry for Basic & Secondary Education and the Ministry of Higher Education) to develop a national curriculum on cybersecurity related courses and requirements/standards.	Develop National Cyber security curriculum	MOCI/ MOHERST/ NAQAA/ MoBSE	January 2021 To June 2021	$35,000	Scope and implementation of the national cyber Security Curriculum	MOCI/ MOHERST/ NAQAA MoBSE
5.1.4.6.2	Dedicate national budget for coordinating cybersecurity education and research	Allocate national Budget for Cyber Security coordination across the country	MOICI NCCD/NCSC	Annually	$33,000	Availability of Funding	MOICI NCCD/NCSC
5.1.4.6.3	Develop qualification programmes for cybersecurity educators and start building a cadre of existing and new professional educators	Develop capacity building programme for cybersecurity instructors in Basic and Higher education systems	MOCI/ MOHERST/ MoBSE	September 2022 To December 2022	$18,000	Implementation and scope of training programme	MOCI/ MOHERST/ MoBSE
5.1.4.6.4	Integrate specialized cybersecurity courses in all computer science degrees at	Universities Computer Science, information systems and	MOICI/MOHERST Universities	January 2021 To	$18,000	Cybersecurity incorporated in all	MOICI/MOHERST UTG

	universities and offer specialized cybersecurity courses in other professional bodies.	telecommunication degrees to integrate cybersecurity courses		June 2021		university ICT degree courses	
5.1.4.6.5	Introduction of Cybersecurity Awareness course in ALL University courses	General Introductory Cybersecurity awareness course should be introduce in all university schools	MOHERST/ Universities	January 2021 To June 2021	$10,000	Implement Cybersecurity awareness course in all schools	MOHERST/ Universities
5.1.4.6.6	Design specific cybersecurity programmes at the Bachelor or Master levels and consider hosting annual cybersecurity competitions for students	Cybersecurity Programme be develop at Bachelor and Masters level including hosting annual cybersecurity competitions for students	MOHERST/NAQAAUniversities/Civil society	September 2021 To December 2021	$15,000	Develop and Implement programme at bachelor and Master levels	MOHERST/ NAQAA Universities/Civil society
5.1.4.6.7	Introduce more technical/ICT related courses at high school level in order to initiate students early-on before they begin studies at university	Technical/ICT related courses introduce in Gambia high school and tertiary institutions	MoBSE/ Tertiary Institutions	September 2021 To December 2021	$30,000	Develop and Implement Technical/ICT related courses in Gambia high school and tertiary institutions	MoBSE/ Tertiary Institutions
5.1.4.6.8	Cybersecurity courses taught at Gambian universities should include ICT/computer lab components to support practical	ICT/computer Lab /Hand-on component should be included in cyber security education in Gambian universities	MOHERST/ NAQAA, Universities	September 2021 To December 2021	$35,000	Extent of hand-on practical sessions	MOHERST/ NAQAA, Universities

	hands-on experience.						
5.1.4.6.9	University scholarships or bursaries to make ICT education at postgraduate and doctoral level affordable.	Provide scholarship/bursaries for ICT education at Postgraduate and doctoral level	MOHERST/Universities/ Partners	Continuous	$10,000	Availability of scholarship and bursaries	MOHERST/Universities/Partners
5.1.4.6.10	Ensure higher education, private, public sector and stakeholders to develop an Industry Based Learning/certification programme for students	Industry base certification Programme developed for student	MOHERST/Industry	September 2023 To February 2024	$37,000	Scope of Certification and quality delivery	MOHERST/Industry
5.1.4.6.12	Develop training for experts on various aspects of cybersecurity such as technical training in data systems, tools, models, and operation of these tools	Expert cyber security Training programme established	MOHERST/ GM-CSIRT/ Universities	June 2024 To December 2024	$26,000	Implementation and Quality of training	MOHERST/ GM-CSIRT/ Universities
5.1.4.6.16	**Specific Objective 4: Promote Collaboration and Information Sharing on Cyber Security**						
5.1.4.6.16	Undertake a nationwide assessment to determine level of awareness of cybersecurity across the nation	Assessment of national levels of cyber security	MOICI/GM-CSIRT/NCCD	Continuous	$26,000	Extent of assessment of national levels of cybersecurity awareness	MOICI/GM-CSIRT/NCCD

5.1.4.6.17	Continuously update the citizens, the private sector and the public sector, on information related to cyber threats, vulnerabilities, incidents, activities across the nation to foster trust.	Online platform which provides national cybersecurity related information	MOICI/GICTA NCCD	Continuous	$7000	Frequency of updates of online platform	MOICI/GICTA NCCD
5.1.4.6.18	Create a national forum to enhance and promote information sharing and collaboration nationally on cyber security	Collaboration	MOICI/GICTA NCCD	Continuous	$15,000	Extent of collaboration	MOICI/GICTA NCCD
5.1.4.6.19	**Specific Objective 5: Ensure online Safety for Vulnerable Groups, especially Children**						
5.1.4.6.19.1	Develop and disseminate online safety guidelines and best practices to protect vulnerable groups in The Gambia, especially children, from cyber threats	Guidelines and best practices to protect children and other vulnerable groups from cyber threats	MOICI GM-CSIRT/PURA	Continuously	$21,500	Frequency of publication, review and update of best practices and guidelines Frequency of dissemination of best practices and guidelines	MOICI GM-CSIRT/

5.1.4.6.19.2	Create and implement mechanism for child online protection	Establishment of a section under NCCD to handle matters relating to child online Abuse and exploitation	NCCD/GM-CSIRT MOBSE	September 2021 To September 2023	$55,000	Develop school based awareness programmes on cyber safety for primary and secondary schools	NCCD/GM-CSIRT
5.1.4.6.19.3	Deploy special awareness programmes to target and inform children and other vulnerable groups about safe and responsible use of the internet	Awareness programme for children and other vulnerable groups	GM-CSIRT/GICTA	Continuously	$41,500	special online safety awareness programme for children and other vulnerable groups Number of children and members of other vulnerable groups with skills on how to use the internet safely	GM-CSIRT/GICTA
5.1.4.6.19.4	Promote, in collaboration with civil society, the secure use of internet based on indicators	Wide deployment of technical measures to prevent access to harmful content by children and other vulnerable groups	Private Operators; ISPs	Within 3 month of adoption of national strategy and continuously after	$10,000	Extent of deployment of technical controls like parental control or authentication services	Private Operators; ISPs

5.1.4.6.19.5	Encourage ISPs to establish programmes that promote trust in their services	Knowledge and awareness of tools/ technologies that can be deployed by ISPs and other service providers to keep children and vulnerable groups safe online	GICTA/NCCD Operators/ISPs	June 2021 To December 2021	$25,000	Extent of dissemination of information on tools/technologies that can be deployed by ISPs	GICTA/NCCD Operators/ISPs
5.1.4.6.20	**Specific Objective 6: Deploy Tools to ensure Vulnerable Groups such as Children are safe Online**						
5.1.4.6.20.1	Promote the deployment of technical measures or web filtering tools that prevent access to harmful content by children and other vulnerable groups	Wide deployment of technical measures to prevent access to harmful content by children and other vulnerable groups	Operators; ISPs GSC/SIXP	Continuously	$190,000	Extent of deployment of technical controls or measures like parental control or authentication services Extent of usage of technical controls or measures like parental control or authentication service	PURA SIXP
	Encourage ISPs and other services providers to make their clients, especially parents	Knowledge and awareness of tools/technologies that can be deployed by ISPs and other service	PURA/ Operators; SIXP	Continuously	$60,000	Extent of dissemination of information on tools/technologies that can be	PURA/ SIXP

5.1.4.6.20.2	and guardians aware of how to leverage available Tools/technologies to manage potential risks to vulnerable groups while accessing services online	providers to keep children and other vulnerable groups safe online				deployed by ISPs and other service providers Extent of usage of technical controls or measures like parental control or authentication services Strategic	
P.11	**PROGRAMMEE: ESTABLISHING CORPORATE DISASTER AND RECOVERY PLAN**						
5.1.4.6.21	**Strategic Goal 1: All CI's to have a Corporate Disaster and Recovery Plan that will define contingency measures in case of attacks or disasters**						
Code.	**Strategies/Action**	**Deliverables/Outputs**	**Lead implementing Institution/support**	**Time Frame**	**Budget**	**Performance Indicators**	**Funding Sources**
5.1.4.6.21.1	Establish Redundancy and back-up systems	Corporate disaster recovery Plan to define contingency measures in the event of attacks or disaster	All information systems CI owners	Continuous	$34,000	Extent of implementation of the plan	All information systems CI owners

5.1.4.6.21.2.	Determine vulnerabilities exploited and conduct restoration procedures to avert or deter similar attacks previously experienced by the system	Conduct restoration to prevent stop future attacks	NCCD/GM-CSIRT /All CI owners	Continuous	-	Implement restoration process on the systems	NCCD/GM-CSIRT /All CI owners
5.1.4.6.21.3	Adopt standard operating procedures (SOPs)	Develop standard operating procedure manual	All CI Owners/sector IT Units	January 2021 To June 2021	$10,000	Develop standard operating procedure manual	All CI Owners/sector IT Units
DIMENSION 6: LEGAL AND REGULATORY FRAMEWORK							
STRATEGY 4 : INSTITUTIONAL AND POLICY BUILD-UP							
6. Strategic Goal 1: Strengthen existing legal and regulatory framework to adequately address cyber-crime and facilitate the criminalization of acts related to cyber-crime							
6.1 Specific Objectives 1: Passage of Cyber-crime Law							

Code.	Strategies/Action	Deliverables/Outputs	Lead implementing Institution/support	Time Frame	Budget	Performance Indicators	Funding Sources
6.1.1	Enact The Cyber Crime Bill 2019 and secure approval of the national policy/Strategy on cyber security	Cybercrime Act, National Cybersecurity policy and strategy Establish a cybersecurity Coordination Directora (NCCD) UNDER GICTA	MOICI/MOJ	June 2021 To September 2021	-	Create a Cybersecurity enforcement Unit to facilitate enforcement of the cybercrime legislation, 2019 once enacted	MOICI/MOJ
6.1.3	Ensure that a national child protection online legislation is enacted and implemented in accordance with international and regional standards	Legislation on online child protection	MOICI/MOJ	September 2020 To February 2021	$18,600	Legislation enacted and implemented	MOICI/MOJ
6.1.5	Review and implement specific legal provision on e-commerce concerning cybercrime incidents, such as online fraud, spam, and phishing	Implement specific legal provision on e-commerce and incidents of cyber crime	MOICI/MOJ	January 2022 To September 2022	$15,000	Number of reviews and implementation	MOICI/MOJ

	sites						
6.1.6	Ratify and implement international, regional and national cybercrime instruments, including the Budapest and Malabo conventions.	Ratify and domesticate international protocols	MOICI/MOJ	March 2022 To September 2022	-	Implement approved international instrument	MOICI/MOJ
6.1.7	**Specific Objectives 2: Administration of Justice**						
6.1.7.1	Create a special court to handle cybercrimes	established Special court on cybercrime	MOJ/GPF	September 2022 To December 2022	$ 15,000	Implement special court	MOJ/MOICI
6.1.7.2	Build capacity of the judiciary and law enforcement for cybercrime investigation, prosecution and adjudication	Establish baseline number of trained officers in the judiciary and law enforcement with skills in investigation/prosecution and adjudication of cybercrime cases. Increase the number of skilled personnel by 50%	MOJ/GPF	September 2022 To December 2022	$ 25,000	Get inputs from stakeholders, secure funding/partnership for training. Develop and implement training plan. Monitoring and Evaluation progress	MOJ/GPF
	Institutionalize relevant educational programs for lawyers and judge	Develop a mandatory educational programme for lawyers and judge	MOJ/MOICI	January 2023 September 2023	$ 10,000	Scope of programs And implementation	MOJ/MOICI

6.1.7.3	Ensure resolution of issues and problems related to Evidence Law or more specifically, the admissibility of electronic evidence in computer crime prosecutions.	Review resolution and evidence law related to admissibility in computer crime prosecution	MOJ/MOICI	September 2021 To December 2021	$9,000	Extend of reviews and implementation	MOJ/MOICI
6.1.8	**Specific Objectives 3: Establish Security Standard**						
6.1.8.1	Develop and publish a cybersecurity information assurance policy and standards consisting of general and sector specific cybersecurity controls that would be recognized as a national standards	Publish a cybersecurity policy and standards	MOICI/NCCD/ GM-CSIRT/Standards Bureau	January 2021 To December 2021	$7,500	Scope of publication	MOICI/NCCD/ GM-CSIRT/Standards Bureau
	Create a national programme to promote the adaptation of uniform cyber standards across government institutions and CII in The Gambia	National program to promote adaptation of uniform cyber standards	GM-CSIRT/NCCD	April 2022 September 2022	$26,000	Implementation of programme	GM-CSIRT/NCCD

6.1.8.2	Adopt and implement by all government agencies of relevant international and local standards such as ISO 27001/02 and those promulgated by the Standards Bureau under ISO 9001:2000 quality management systems requirements;	Government agencies to adopt and implement local and international standards	GICTA/NCCD/ GM-CSIRT	September 2021 To December	-	Extent of adoption of local and international standards	GICTA/NCCD/ GM-CSIRT
6.1.8.4	Promote adoption of international IT and cybersecurity standards for procurement	Adopt international IT and cybersecurity standards	GICTA/NCCD/ GM-CSIRT	January 2022 To June 2022	-	Implement international IT and cyber security	GICTA/NCCD/ GM-CSIRT
6.1.8.5	Promote the adoption of relevant standards in software development	Promote adoption of relevant software standards	GICTA/NCCD/ GM-CSIR GICTA/NCCD/ GM-CSIRT	continuous	$5000	Implement and cyber security	GICTA/NCCD/ GM-CSIRT
6.1.8.6	In partnership with academia and civil society, gather and assess evidence of software quality deficiencies and it impact on usability and performance	Partner with academia and civil society to gather and access evidence of software quality	MOICI/Standards Bureau/	Continuous	$8,0000	Extent of collaboration	MOICI/Standards Bureau/

6.1.9	**Specific Objectives 4: Building the Capacity of Law Enforcement**						
6.1.9.1	Establish the requisite framework to operationalize a digital forensics laboratory	Operational digital forensics laboratory Plans and budgets to establish Digital forensics laboratory	Gambia Police Force Ministry of Justice	January 2022 To October 2022	$44,800	Extent of operationalization of Digital Forensics Lab	GPF/MOJ
6.1.9.2	Develop mandatory digital forensics and evidence handling courses for the judiciary, law enforcement and personnel from other related agencies involved in the detection and prosecution of cybercrime	Training programme on digital forensics and evidence handling procedures	Gambia Police Force Ministry of Justice	Continuously (Annually)	$32,900 (Annually)	Number and frequency of mandatory courses and qualifications delivered to or acquired on cybercrime by judiciary and security personnel nationwide Number of successful prosecutions of cybercrimes	GPF/MOJ
6.1.9.3	Build and enhance capacity to detect cybercrime incidents	Training Programme and Budget on cybercrime incident detection	Gambia Police Force Ministry of Justice	January 2022 To December 2024	$32,100 (Annually)	Number and frequency of mandatory courses and qualifications delivered to or acquired on	GPF/MOJ

						cybercrime by judiciary and security personnel nationwide Extent of detection of cybercrimes	
6.1.10	**Specific Objective 1: Enhance Cybercrime Detection**						
6.1.10.1	Develop and continuously update an information sharing, governance and collaboration framework for the fight against cybercrime Ensure direct and timely collaboration between judiciary, law enforcement and personnel from other related agencies, service providers, CII entities, GM-CSIRT and other government institutions on issues	Governance Framework for fight against cybercrime	Gambia Police Force Other Security Agencies Judiciary and Ministry of Justice . GM-CSIRT/PURA	December 2020 Onwards Continuously	$19,200 (Annually)	Extent of collaboration across all relevant stakeholders in the fight against cybercrime and ensuring Cybersecurity	GPF/MOJ GM-CSIRT/PURA

	concerning cybercrime and cybersecurity						
6.1.11	**Specific Objectives 5: Knowledge Management (KM)**						
6.1.11.1	Establish Knowledge Centres that can provide information resources to law enforcement units, CI operators, ICT security managers, government personnel and others;	Create knowledge centres and across the regions in the country	NCCD/GM-CSIRT	September – December 2021	$20,000	Develop operational procedure for implementation of the program	NCCD/GM-CSIRT
6.1.11.2	Establish collaboration with relevant international KM organizations	Establish link and collaborate with international partners	NCCD/GM-CSIRT	January – September 2022	$8000 (Annually)	Establish link and secure funding	NCCD/GM-CSIRT

<table>
<tr><td><b>P.12</b></td><td colspan="7"><b>PROGRAMME 12: BUILDING CYBER SECURITY INDUSTRY</b></td></tr>
<tr><td>\
6.1.12</td><td colspan="7"><b>Strategic Goal 1: To develop a stronger cyber security industry and to ensure a resilient cyber space</b></td></tr>
<tr><td>6.1.12.1</td><td colspan="7"><b>Specific Objectives 1: Foster Innovation through Research and Development</b></td></tr>
<tr><th>Code.</th><th>Strategies/Action</th><th>Deliverables/Outputs</th><th>Lead implementing Institution/support</th><th>Time Frame</th><th>Budget</th><th>Performance Indicators</th><th>Funding Sources</th></tr>
<tr><td>6.1.12.1</td><td>Build a national framework for promoting cybersecurity research, innovation and local content development</td><td>Establish a cyber security centre of Excellence in the university
Build a team of experts with capacity to carry out research, development and training in specialize areas of cybersecurity</td><td>MOICI/MOHERST UNIVERSITY</td><td>February 2022-February 2023</td><td>$ 43,000</td><td>University to collaborate and industry to support setting up of cybersecurity centre of Excellence</td><td>MOICI/MOHERST UNIVERSITY</td></tr>
<tr><td>6.1.12.3</td><td>Encourage ISPs to establish policies for technical security control deployment as part of their services</td><td>ISPs to develop and implement policies for technical security controls in their service provision</td><td>Private Telecoms Operators (SIXP)</td><td>September – December 2022</td><td>$9,000</td><td>Develop and implement policies</td><td>Private telecoms Operators (SIXP</td></tr>
<tr><td>6.1.12.4</td><td>Encourage the development and dissemination of cryptographic controls across all</td><td>Develop and disseminate awareness on cryptographic controls across all sectors</td><td>GICTA/NCCD/ GM-CSIRT</td><td>January – December 2024</td><td>$15,000</td><td>Develop and disseminate awareness on cryptographic</td><td>GICTA/NCCD/ GM-CSIRT</td></tr>
</table>

	sectors for protection of data at rest and in transit, according to international standards and guidelines.					controls	
6.1.13	**Continuously Develop and Enhance Cybersecurity Technical Capacity in The Gambia** **Budget: $267,900**						
6.1.13.1	Revise the National Research Agenda to promote R&D in cybersecurity	Revised National Research Agenda which includes the cybersecurity aspects	Ministry of Higher Education, Science and Technology (MoHERST) MOICI	Continuously	$14,450	Extent of implementation of Revised National Research Agenda which includes the cybersecurity	Ministry of Higher Education, Science and Technology (MoHERST)
6.1.13.2	Establish a National Centre of Excellence for cybersecurity training & research	National Operational Centre of Excellence for cybersecurity training & research	MOICI (MoHERST) Academia (University) Private Sector	September 2021 To August 2022	$70,500	Extent of operationalization of National Centre of Excellence	MOICI MOHERST
6.1.13.3	Review and update primary, secondary and tertiary level education curriculum to include	Revised education curriculum to include cybersecurity awareness	Ministry of Higher Education, Science and Technology (MoHERST) &	September 2021 To August 2022	$48,000	Extent of implementation of revised curriculum	MOICI MOHERST MOBSE

	cybersecurity components		Ministry of Basic & Sec Education (MOBSE) Academia				
6.1.13.4	Promote cybersecurity competitions and Support R & D projects in universities and schools	Funding and incentive programmes for universities engaged in cybersecurity R & D competitions in schools on cybersecurity	Academia; Ministry of Higher Education, Science and Technology (MoHERST) Private sector	Annually/Continuously	$33,500	Number of universities participating in funding and incentive programme	MOICI MOHERST
6.1.13.5	Support national enterprises providing cybersecurity solutions, and undertaking R & D in cybersecurity	Funding and incentive programmes for Enterprises engaged in cybersecurity R & D	Academia; Ministry of Higher Education, Science and Technology (MoHEST	Annually/Continuously	$32,700	Number of Enterprises participating in funding and incentive programme	Academia MoHEST
6.1.13.6	Collaborate with universities, tertiary and the private sector to create new study and internship programs on cyber security	Internship programs on cybersecurity	Academia Ministry of Higher Education, Science and Technology (MoHERST), UTG/Private Sector	September 2021 To August 2022	$15,000	Number of new tertiary level study and internship programs on Cyber security created;	Private sector
	Collaborate with the private sector and	Partnerships to support participation of	Academia		$10,750	Extent of participation in	

6.1.13.7	academia to support participation of government institutions, universities, private sector in regional and international research projects and exercises relating to cybersecurity	government institutions, universities, private sector in regional and international research projects and exercises relating to cybersecurity	Ministry of Higher Education, Science and Technology (MoHERST)	Continuously		national and international research projects and activities concerning cyber security; Number of partnerships created in national and international research projects and activities concerning cyber security;	MOICI/GICTA
6.1.13.8	Create standards in cybersecurity training and education	Standards for cybersecurity training and education	Ministry of Higher Education, Science and Technology (MoHEST/NAQAA)	September 2021 To August 2022	$14,200	Certificate Levels of competence of the trained individuals	MoHEST/NAQAA)
6.1.13.9	Train IT personnel of various sectors of Government on how to detect incidents, report incidents, and collaborate with the GM-CSIRT and institutions from other sectors on cybersecurity	Training programme for IT personnel of various Government ministries and institutions	Personnel management Office (PMO)/GICTA	Continuously	$28,800	Number and frequency of courses/ qualifications delivered / acquired	(PMO)/GICTA