THE NATIONAL CYBERSECURITY STRATEGY AND ACTION PLAN OF THE GAMBIA 2022-2026

REVISED EDITION

September 2022

Contents

LIST OF ABBREVIATIONS

ICT	Information Communications Technology
ICI	Information Communications Infrastructure
NICI	National Information Communications Infrastructure
NCI	National Critical Infrastructure
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	The Gambia Telecommunications Services Company
GM-CSIRT	The Gambia Computer Security Incident Response Team
CERT	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
NCSA	National Cybersecurity Authority
NCSC	National Cybersecurity Committee
NCCD	National Cybersecurity Coordination Department
GNCSS	Gambia 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
RNP	Regional Network Provider
MOD	Ministry of Defense
MOI	Ministry of the Interior
BCP	Business Continuity Plan PKI Public Key Infrastructure
NDP	National Development Plan

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 Cybersecurity 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 Cybersecurity 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 Cybersecurity 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 Cybersecurity policies and programs. The National Cybersecurity Strategy and Action Plan shall be the cornerstone of the country's Cybersecurity policy.

2. NATIONAL CYBERSECURITY STRATEGY

This national Cybersecurity 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 Cybersecurity 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 Cybersecurity and ways to improve or calibrate the Cybersecurity 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 Pillars of critical infrastructure protection including measures to respond to challenges of cyber threats were considered. To address Cybersecurity 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 Cybersecurity measures from strategic, tactical to operational aspects of Cybersecurity.

As a global challenge, Cybersecurity demands both domestic and international solutions. Given the shared nature of vulnerabilities, the national Cybersecurity strategy would require 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 collaboration of all stakeholders (i.e. government, private sector, civil society, citizens and international cooperation and collaboration. To this end, GoTG shall promote and strengthen collaboration with regional and international partners in confronting the Cybersecurity challenges.

2.1. Vision

Ensure full implementation of the key Cybersecurity Pillars, strategic objectives and priority policy actions to bring about a secure, trusted and resilient cyberspace for enhanced inclusive socio-economic development.

2.2. Mission

To create an enabling environment that ensures the protection of critical national infrastructure, Information systems and users with effective capabilities for accelerated responses to cyber risks and treats.

2.3. Strategic Goals

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

- Strengthened Legal and Regulatory Frameworks that promotes compliance with appropriate technical and security standards.
- A trained, educated, aware and informed Cybersecurity cultured society at all sectors and levels within the country, that promotes information sharing and collaboration on Cybersecurity.
- Established Institutional Framework that fosters cyber-security coordination and enhances the fight against all forms of

cybercrime.

- Existence of strong Cybersecurity capabilities, capacities and infrastructure for prevention, protection, detection, and response to Cybersecurity incidents and threats.
- Continued protection of Information Systems in particular critical information infrastructure and services that ensures the safety of vulnerable groups in cyberspace, especially those of children.
- Compliance with National and International Cybersecurity Standards, Treaties and Protocols.

3. STRATEGY

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

The 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 Cybersecurity 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 Cybersecurity 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
6. Establish a national cybersecurity governance framework

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

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 should be adopted.

4.1 Identify assets to determine level of protection gainst cyber threats
4.2 Conduct threat assessment for vulnerabilities, risk and potential impact
4.3 Develop and Implement Disaster Recovery Plan
4.4 Develop and implement early warning plan
4.5 Develop and Implement Security awareness
4.6 Define clear roles and responsibilities
4.7 Develop and implement a robust incident response capability
4.8 Ensure continuous monitoring and conduct periodic security audits.

4.3 GENERAL DIRECTION AND GOALS

The focus of this section general 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 Cybersecurity conscious society

4.4 GUIDING FRAMEWORK

4.4.1 Establishing a Secure Environment

4.4.1.1 **Identify assets and the associated threats:** Knowing the threats, what to protect, and determining ways to reduce risks.

4.4.1.2 **Evaluate Vulnerabilities:** Identify and remove potential weaknesses and enhance level of resilience.

4.4.1.3 **Defeat and attacks**. Provide resources and implement appropriate effective countermeasures

4.4.1.4 **Reduce losses and damages.** Implement contingency plans and other risk mitigation measures to reduce impact

4.4.1.5 **Implement a resiliency program.** Implement program to ensure continuity of businesses

4.4.1.6 **Institute effective law enforcement programs.** Enhance professional capacity and capabilities of law enforcement, judiciary and periodic review of the policy.

5. STRATEGIC OBJECTIVES AND PROGRAMS

Based on the above, five (5) strategies and twelve (12) programmes have been formulated critical to information infrastructures protection and services of The Gambia.

1. Cybersecurity Policy and Strategy: To enable and facilitate the formulation and implementation of appropriate policies, strategies and programs for a secure, resilient and development oriented digital ecosystem within a period of two years.
2. Cybersecurity Culture and Society: To inculcate cyber-hygiene best practices and security culture in order to ensure safety and confidence in the cyberspace.
3. Cybersecurity Education, Training and Skills: To develop cybersecurity capacity building programmes for ensuring the availability, quality, and uptake of educational and trainings for stakeholders by 2023
4. Legal and Regulatory Framework: To formulate and strengthen cybersecurity legal and regulatory frameworks with enforcement mechanisms for enhanced resilience in the cyberspace.
5. Standards, Organization, and Technologies: To develop and adopt best standards and practices to mitigate cybersecurity risks.

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.

5.1. 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.

6. PILLAR 1: CRITICAL NATIONAL INFRASTRUCTURE

6.1. 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 Cybersecurity 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.

6.2. STRATEGIC OBJECTIVE 5: To develop and adopt best standards and practices to mitigate cybersecurity risks.

The most important strategy in the national critical cyber infrastructures protecting is to understand the nature of threats to Gambia's cyberspace, assess vulnerabilities, the likelihood and the degree of impact should an incident occur. This strategy would involve continuing periodic 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 Cybersecurity, and Institutional and Policy Build-Up. Every strategy has corresponding programs to be undertaken.

6.3. PROGRAMME 1: NATIONAL THREAT ASSESSMENT

6.3.1.Strategic Goal 1: To Conduct National Assessment

This initiative consist two primary specific objectives:

6.3.1.1. National cyber mapping

6.3.1.2. National Risk assessment

6.3.2.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.

6.3.2.1. ACTIONS

6.3.2.1.1. 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 cybersecurity. This will include accounting of physical facilities, hardware, software and people.

6.3.3.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 Actions.

ACTIONS

6.3.3.1. National Threat Assessment

A national threat assessment initiative will be implemented to priority basis and conduct periodic assessment. This process will be essential for understanding the nature of cyber threats and how they can be addressed effectively from operational and strategic perspectives. In addition, a cyber-

intelligence program will be created for knowledge acquisition.

6.3.3.2. 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:

6.3.3.2.1. 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.

6.3.3.2.2. 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.

6.3.4. 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. PILLAR 2: BUILDING CYBERSECURITY CAPABILITIES

7.1. STRATEGIC OBJECTIVE 1: To enable and facilitate the formulation and implementation of appropriate policies, strategies and programs for a secure, resilient and development oriented digital ecosystem within a period of two years.

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 PILLAR 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

7.2.1. Strategic Goal 1: Establishing Measures to Prevent Attacks

7.2.2. Specific Objective 1: GM-CSIRT to Strengthen Cyber Intelligence Collection & Sharing

Cyber intelligence involves the acquisition and utilization of 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 Collection program will be focus on intelligence collection on sources of cyber threats and sharing among relevant stakeholders. GM-CSIRT will collect cyber intelligence and incident reports and share them with law enforcement, military units and international partners especially on the interdiction of cyber-criminals.

To be able to effectively implement cyber intelligence sharing and coordination, the following should be implemented.

7.2.2.1. Setting up a Cyber Special Operations Unit.

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

7.2.2.3. GM-CSIRT to develop and manage cyber-Intelligence Database

7.2.2.4. Ministry of Defense, SIS in collaboration with GM-CSIRT to develop and implement sectoral cyber-intelligence training program

7.2.2.5. GM-CSIRT to promote and receive incident reports 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 provide updates on 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.

7.3. 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 engage relevant stakeholders to identify, understand the vulnerabilities and Cybersecurity posture of The Gambia's critical information infrastructure CIIs. The Government will also establish measures to cater for both current and potential cyber threats and risks to critical national information infrastructure, It will also drive improvements where necessary.

7.3.1. Strategic Goal 1: Identify and Manage the Critical Information Infrastructure of The Gambia

7.3.2. Actions

7.3.2.1. Develop a Security classification plan including inventory and documentation of CII Register.

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

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

7.3.2.4. Establish mandatory and voluntary Equipment Specifications, Guidelines, and Procedures relating to the management of risks by CIIs.

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

7.3.2.6. Undertake continuous monitoring and reporting of CII incidents, regular testing to detect errors, vulnerabilities, and intrusions in CII.

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

7.3.2.8. Establish mandatory and minimum standards and security requirements for equipment of ISPs and end users like the banking sector.

7.3.2.9. Develop a government programme to deploy and manage government ICT infrastructure.

7.3.2.10. Develop a national programme to enhance internet infrastructure development and resilience.

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

7.3.2.12. Review and update the map of current emergency response assets.

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

7.4. Strategic Goal 2: 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, 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.

7.4.1.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 sectoral units or monitoring points.

7.4.2.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

7.4.3.Specific Objectives 3: 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.

7.4.4.Specific Objectives 4: Consumer Protection

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

7.4.4.1. Product Quality assurance checks
7.4.4.2. Consumer Education
7.4.4.3. Remedy and redress in case of fraud
7.4.4.4. Product information for choice
7.4.4.5. Access to products
7.4.4.6. Product evaluation and testing

7.5. PROGRAMME 4: RESPONSE CAPABILITY PROGRAM

7.5.1. Strategic Goal 1: Establishing Computer Security Response Units

7.5.2. 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.

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

7.5.2.2. 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

7.5.2.3. Develop a national incident reporting, information sharing and coordination mechanisms targeting critical information owners to address reporting of incidents and coordination in incident response.

7.5.2.4. Create and periodically update Cybersecurity incident register, assess incidents, and provide opportunity for incident resolution request to resolve issues and mitigate risks.

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

7.5.2.6. Periodically assess and analyze cyber threats and potential risks and be able to provide a real time overview of state of Cybersecurity across the nation

7.5.2.7. Develop a Cybersecurity Governance Framework for defining roles and responsibilities of national stakeholders as well as describe Standard Operating Procedure and code of conduct in responding to incidents.

7.5.2.8. Set-up an automated incident response system for reporting

incidents or seeking assistance with incidents.

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

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

7.5.2.11. Develop a Cyber Defense Strategy that details approaches to addressing threats to national security in cyberspace.

7.5.2.12. Establish a general Defense Command and Control Centre for Cybersecurity. The Centre should have liaison with GM-CSIRT incident reporting as well as sharing of intelligence.

7.5.2.13. Establish mechanisms for regional and international cooperation for incident response.

7.5.2.14. Develop web portal to receive cyber complaints.

7.5.3. Specific Objectives 2: Creation of Sectoral Focal Points/CSIRTSs

These sectoral Units will support as well as collaborate with the operators and actors within their sectors. This will entail establishing sectoral computer security and incident response teams or focal points across the country to enable faster and more localized response to cyber incidents. They can be located in any regional or local government offices, or private sector organizations that have the capability to undertake the initiative. These sector CSIRTS will serve as immediate points of contact for government agencies, local government units.

7.5.4.Specific Objectives 3: Establishing Cybercrime 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 such a police Cybercrime Response Unit for investigation at same time maintain a close collaboration with GM-CSIRT for better understanding of the

crime scene. A website will be developed and maintained as the primary complaint reporting point

7.5.4.1.Action:

7.5.4.1.1. Develop a web portal to received complaints.

7.6. PROGRAMME 5: ENHANCEMENT OF LAW ENFORCEMENT CAPABILITY

7.6.1. 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.

7.6.2.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.

7.6.3.Specific Objective 2: Enhance Cybercrime Detection

7.6.3.1.Actions

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

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

7.6.3.1.1.3. Develop and publish Information Security Policies and

Standards.

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

7.6.3.1.1.5. Establish the requisite framework to operationalize a digital forensics laboratory.

7.6.3.1.1.6. 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.

7.6.3.1.1.7. Build and enhance capacity to detect cybercrime incidents.

7.6.3.1.1.8. Train judiciary and the legal fraternity on how to interpret and enforce the policy, legal and regulatory frameworks on Cybersecurity in The Gambia.

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

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

7.6.4.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.

7.6.5.Actions

7.6.5.1. 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.

7.6.5.2. Train judiciary and the legal fraternity on how to interpret and enforce the policy, legal and regulatory frameworks on Cybersecurity in The Gambia.

7.7. PROGRAMME 6: GOVERNMENT CYBERSECURITY EMHANCEMENT PROGRAM

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

7.7.2. Specific Objective2: Establish Information Security Assurance mechanisms or Compliance

7.7.3. Specific Objective 3: Establish security levels for systems, applications and services

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

7.7.5. Actions:

7.7.5.1. Establish mandatory and minimum technology and security requirements for CIIs.

7.7.5.2. Develop national Programme to deploy and manage government ICT infrastructure.

7.7.5.3. Develop a national programme to enhance internet infrastructure development and resilience.

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

7.7.5.5. Review, develop or update the emergency response assets.

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

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

7.7.7. Actions

7.7.7.1. Develop national cybersecurity training curriculum to enhance professional competence in Incident Response

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

7.7.7.3. Develop and implement Cybersecurity training and capacity building of Government personnel.

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

7.7.7.5. Establish a National Centre of Excellence for cybersecurity training & research.

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

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

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

7.7.7.9. Collaborate with universities, tertiary and the private sector to provide education and internship programs on Cybersecurity.

7.7.7.10. Collaborate with the private sector and academia to support participation of government institutions, universities, private sector in regional and international research projects and conferences on cybersecurity.

7.7.7.11. Create standards in cybersecurity training and education.

7.7.7.12. Train IT personnel of various sectors of Government on cyber incident detection, reporting in collaboration with GM-CSIRT and other institutions on cybersecurity

7.7.8. Specific objective 6: Establish Secure and Reliable Environment for e-Government and e-commerce with National Public Key Infrastructure

7.7.9. Actions:

7.7.9.1. 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.

7.7.9.2. Encourage the use of Public Key Infrastructure (PKI) such as digital certificates for ensuring secure transactions between Government and other institutions.

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

7.8. CRISIS MANAGEMENT - PROGRAMME 7: BUSINESS CONTINUITY / RESILIENCY PROGRAM

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

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

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

7.8.1.2. Designate cybersecurity exercise planning to GM-CSIRT in collaboration with Gambia National Disaster Management Agency (NDMA). GM-CSIRT to have cybersecurity liaison and reporting mechanism with Gambia National Disaster Management Agency (NDMA).

7.8.1.3. Design, implement and test a cybersecurity needs assessment.

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

7.8.1.5. Organize national cybersecurity exercises/drills.

7.8.1.6. Identify metrics to evaluate the success of the exercises.

7.8.1.7. Conduct periodic reviews of evolving threats to ensure that cyber defense policies continue to meet national security objectives.

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

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

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

7.8.2. Specific Objective 1: Cyber Defense

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

7.8.2.2. Develop a communication and coordination framework for cyber defense, build on existing security structures.

7.8.2.3. Establish a central command and control of cyber defense capabilities in the Gambia national army (GNA) to host and manage cyber defense with liaison and reporting mechanism between GM-CSIRT and GNA and Set-up liaison and reporting mechanism between GM-CSIRT and SIS cyber Intelligence Collection unit.

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

7.8.2.5. Develop communication and coordination framework for cyber defense.

7.8.2.6. Periodically assess and determine cyber defense capability requirements, involving public and private sector stakeholders.

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

7.8.2.8. Establish training programmes for employees and develop awareness campaigns

7.8.3. Specific Objectives 2: Communications Redundancy

7.8.3.1. Ensure that the redundancy efforts are appropriately communicated to relevant stakeholders.

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

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

7.9. 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. PILLAR 3: INSTITUTIONAL FRAMEWORK FOR CYBERSECURITY GOVERNANCE & ENHANCEMENT

8.1. STRATEGIC OBJECTIVE 2: To inculcate cyber-hygiene best practices and security culture in order to ensure safety and confidence in the cyberspace.

This Strategy pertains to the organization and mobilization of human, financial, and relevant resources for the implementation of the National Cybersecurity 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 Cybersecurity initiatives. Cybersecurity Advisory Board, focal points or sector CERTs 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 Cybersecurity 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 Cybersecurity.

8.1.2.1 Establish National Cybersecurity Advisory Board/Committee

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.

9.0. PILLAR 4: NATIONAL & INTERNATIONAL COOPERATION

9.1. STRATEGIC OBJECTIVE 4: To formulate and strengthen cybersecurity legal and regulatory frameworks with enforcement mechanisms for enhanced resilience in the cyberspace.

9.2. PROGRAMME 10: ESTABLISHING PUBLIC AND PRIVATE PARTNERSHIP/COOPERATION

9.2.1.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 Cybersecurity Plan. Public-private partnership will be in the form of:

9.2.1.1. Capacity-Building
9.2.1.2. Information-Sharing
9.2.1.3. Threat Assessment
9.2.1.4. Joint Management of Cybersecurity Programs
9.2.1.5. Incident Reporting
9.2.1.6. Advocacy

9.2.2. 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.

9.2.3.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.

9.2.3.1. 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.

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

9.2.4.Specific Objective 3: Promote International Cooperation and Collaboration

9.2.5.Actions:

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

9.2.5.2. 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,

9.2.5.3. Develop a clear plan that outlines how to manage international collaboration across multiple areas such as law enforcement,

incidence response, research and innovation in Cybersecurity.

9.2.5.4. Subscribe to and participate in all relevant regional and international forums on Cybersecurity.

10. PILLAR 5: CYBERSECURITY CAPACITY BUILDING AND AWARENESS

10.1. STRATEGIC OBJECTIVE 5: To develop cybersecurity capacity building programmes for ensuring the availability, quality, and uptake of educational and trainings for stakeholders by 2023

10.2. 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 will involve incident reporting and public awareness program. 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.

10.2.1. **Strategic Goal 1:** To build Cybersecurity prevention and response capabilities and create Cybersecurity awareness for Gambian citizens.

10.2.2. Specific objective1: Develop a National Cybersecurity Awareness Program

10.2.3. Specific Objective 2: Enhance Cybersecurity awareness across the general public and national institutions

10.2.4. Actions:

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

10.2.4.2. GM-CSIRT to contribute in nationwide assessment to determine

level of awareness of Cybersecurity in collaboration with civil society organization such as Information Technology Association of The Gambia (ITAG) and GCSA.

10.2.4.3. Develop and implement a national roadmap for improving awareness of current Cybersecurity trends and threats.

10.2.4.4. Develop and disseminate National Cybersecurity best practices to engrain a Cybersecurity mindset in the public.

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

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

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

10.2.4.8. 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. 3. Specific Objective 3: Develop Cybersecurity Education and Profession Training

10.3.1. 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.

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

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

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

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

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

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

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

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

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

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

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

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

10.3.14. Advice government and companies on measures to implement to retain skilled cybersecurity staff.

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

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

10.4. Specific Objective 4: Promote collaboration and Information Sharing on Cybersecurity

10.4.1.Actions:

10.4.1.1. Create a national forum to enhance and promote information sharing and collaboration nationally on Cybersecurity in collaboration with NCCD.

10.4.1.2. 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.

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

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

10.5.1.Actions

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

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

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

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

10.5.1.5. Encourage ISPs to establish programmes that promote trust in their services.

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

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

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

10.6.1.Actions:

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

10.6.1.2. 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' operators' to have a Corporate Disaster and Recovery Plan that will define contingency measures in case of attacks or disasters. It the same vein, it should also include provision of disaster relief to those affected. The Plan will define systems and procedures for the immediate recovery and resumption of their normal operations. This should entail 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. PILLAR 6: LEGAL AND REGULATORY FRAMEWORK

12.1. STRATEGIC OBJECTIVE: To formulate and strengthen cybersecurity legal and regulatory frameworks with enforcement mechanisms for enhanced resilience in the cyberspace.

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

12.4.1.1. Create a special court to handle cybercrimes.
12.4.1.2. Institutionalize relevant educational programs for lawyers and judge.
12.4.1.3. Ensure resolution of issues and problems related to Evidence Law or more specifically, the admissibility of electronic evidence in computer crime prosecutions.
12.4.1.4. 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

12.5.1.1. Develop a program to identify, adapt and/or adopt international information risk management standards applicable to government agencies, personal and/or ICT infrastructure, solutions.
12.5.1.2. Adopt and implement relevant international and local standards such as ISO 27001/02, ISO 9001:2000 quality management systems requirements and those promulgated by the National Standards Bureau;
12.5.1.3. Adopting an Information Security Management System (ISMS) ISO27001/02 as a requirement in the Integrated Information Systems Plan of each government agency.
12.5.1.4. Promote adoption of international IT and cybersecurity standards for procurement.
12.5.1.5. Promote the adoption of relevant standards in software development.
12.5.1.6. In partnership with academia and civil society, gather and assess evidence of software quality deficiencies and it impact on usability and performance. 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 Cybersecurity 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 Cybersecurity have to be acquired, re-created stored and disseminated to improve Cybersecurity programs.

12.7.1.Actions

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

12.7.1.2. Establish collaboration with relevant international KM organizations.

13. PROGRAMME 12: BUILDING CYBERSECURITY INDUSTRY

13.1. Strategic Goal 1: To develop a stronger Cybersecurity 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.

13.1.1.Actions

13.1.1.1. Revise the National Research Agenda to promote R&D in Cybersecurity in The Gambia.

13.1.1.2. 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).

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

13.1.1.4. 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.

13.1.1.5. 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.

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

13.1.1.7. Establish a National Centre of Excellence for Cybersecurity Training & Research.

13.1.1.8. Review and update primary, secondary and tertiary level education curriculum to include Cybersecurity elements

13.1.1.9. Support Cybersecurity competitions and R & D projects in Universities and Gambian Secondary Schools.

13.1.1.10. Support national enterprises providing Cybersecurity solutions, and undertaking R & D in Cybersecurity.

13.1.1.11. Collaborate with universities, colleges and the private sector to create new studies and internship programs on Cybersecurity.

13.1.1.12. 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.

13.1.1.13. Create standards in Cybersecurity training and education.

13.1.1.14. 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 Cybersecurity 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 Cybersecurity 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 Cybersecurity-related frameworks within the ICT sector.

14.3. National Cybersecurity 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 Cybersecurity Commission (NCSC)

This body serves as the advisor to the national authority in charge of Cybersecurity on all aspects of the Cybersecurity 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 Ministry of Interior (MOI) 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 with other 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 Cybersecurity Centre. It is also a resource Centre for Cybersecurity 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 Cybersecurity-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 Cybersecurity to address The Gambia's requirements for skilled and knowledgeable Cybersecurity professionals both present and in the future. The University and the Industry will play a leading role in undertaking Cybersecurity-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 Cybersecurity 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 Cybersecurity.

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 Cybersecurity 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 Cybersecurity 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		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	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		
Supporting implementing Agencies and their assigned responsibilities	**Time Bound Measurable Target**	
	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		
Supporting implementing Agencies and their assigned	**Time Bound Measurable Target**	
	Supporting Agency	**Responsibility**
	Ministry of Interior	

responsibilities	/Ministry of Justice/GPF/Ministry of Interior	
	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 Cybersecurity Expertise in The Gambia

	Time Bound Measurable Target	
	Supporting Agency	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	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 Cybersecurity 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

	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	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

	Time Bound Measurable Target	
Supporting implementing Agencies and	**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

	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	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

	Time Bound Measurable Target	
	Supporting Agency	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	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 Cybersecurity

	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	MOICI/GM- CSIRT NCCD/NCSC	

<table>
<tr><td>Specific Objectives critical success factors</td><td colspan="2">Commitment to implement NCCD establishment and NCSC including the creation of sector CSIRTs/IT Operations Units by stakeholder members</td></tr>
<tr><td>Implementing Risk factors</td><td colspan="2">Lack of support, funding and manpower</td></tr>
<tr><td colspan="3">Objective 12: Public & Private and International Partnership Cooperation</td></tr>
<tr><td></td><td colspan="2">Time Bound Measurable Target</td></tr>
<tr><td rowspan="3">Supporting implementing Agencies and their assigned responsibilities</td><td>Supporting Agencies</td><td>Responsibility</td></tr>
<tr><td>MOICI/GICTA

PUBLIC – PRIVATE OPERATORS</td><td rowspan="2"></td></tr>
<tr><td>NCCD/NCSC</td></tr>
<tr><td>Specific Objectives critical success factors</td><td colspan="2">Stakeholders commitment to establish and promote strong public–private partnership, regional including International Cooperation</td></tr>
<tr><td>Implementing Risk factors</td><td colspan="2">Lack of support, framework for public and private sector partnership, relevant cooperation agreements and funding.</td></tr>
<tr><td colspan="3">Objective 13: Develop a National Cybersecurity Awareness Program</td></tr>
<tr><td rowspan="4">Supporting implementing Agencies and their assigned responsibilities</td><td colspan="2">Time Bound Measurable Target</td></tr>
<tr><td>Supporting Agency</td><td>Responsibility</td></tr>
<tr><td>MOICI/NCCD</td><td rowspan="2"></td></tr>
<tr><td>GM-CSIRT</td></tr>
</table>

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 Cybersecurity Awareness across Civil society and national Institutions

	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	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 Cybersecurity Education and Professional Training

	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	MOICI/ GM-CSIRT NCCD MoBSE/MOHERST	
Specific Objectives critical success factors	Commitment to develop and roll out Cybersecurity curriculum including awareness into Basic, Secondary, Tertiary and University Educational system	

<table>
<tr><td>Implementing Risk factors</td><td colspan="2">Lack of support, funding and necessary resources</td></tr>
<tr><td colspan="3">Objective 16: Promote collaboration and Information sharing on Cybersecurity</td></tr>
<tr><td rowspan="3"></td><td colspan="2">Time Bound Measurable Target</td></tr>
<tr><td>Supporting Agency</td><td>Responsibility</td></tr>
<tr><td>MOICI

NCCD/
NCSC/
GM-
CSIRT</td><td></td></tr>
<tr><td>Supporting implementing Agencies and their assigned responsibilities</td><td colspan="2"></td></tr>
<tr><td>Specific Objectives critical success factors</td><td colspan="2">Commitment to create a national forum to promote information sharing and collaboration by NCCD/NSCS including stakeholder members</td></tr>
<tr><td>Implementing Risk factors</td><td colspan="2">Delay in implementation, lack of manpower, funding and support from stakeholder members</td></tr>
<tr><td colspan="3">Objective 17 : Ensure online safety for vulnerable groups, especially children</td></tr>
<tr><td rowspan="3"></td><td colspan="2">Time Bound Measurable Target</td></tr>
<tr><td>Supporting Agencies</td><td>Responsibility</td></tr>
<tr><td>MOICI/
GISTA
NCCD/ GM-
CSIRT

PRIVATE OPERATORS</td><td></td></tr>
<tr><td>Supporting implementing Agencies and their assigned responsibilities</td><td colspan="2"></td></tr>
</table>

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

	Time Bound Measurable Target	
	Supporting Agency	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	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

	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**

Supporting implementing Agencies and their assigned responsibilities	MOICI/GICT A 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	
	MOI/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)

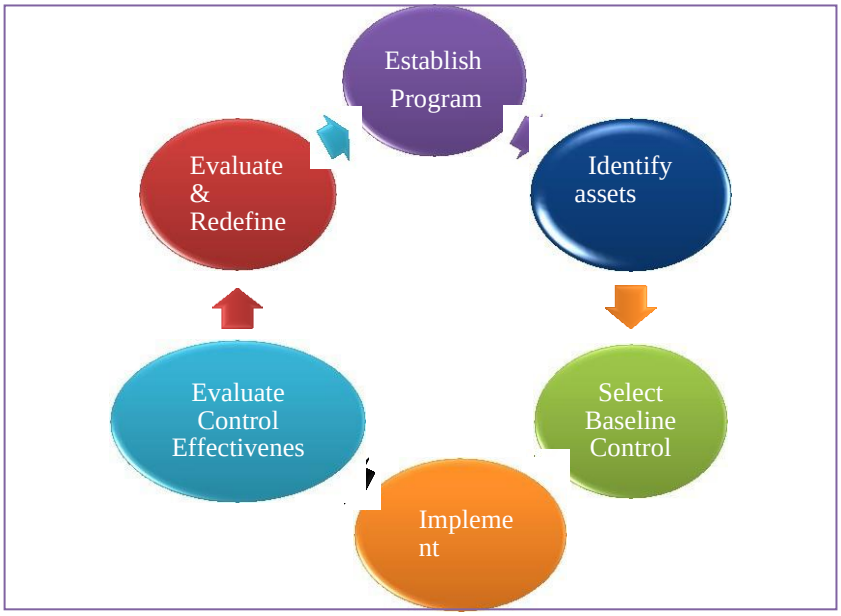
	Time Bound Measurable Target	
	Supporting Agencies	**Responsibility**
Supporting implementing Agencies and their assigned responsibilities	MOICI/GM- CSIRT/ NCCD/ RELEVANT SECTORS	
	NCCD	
Specific Objectives critical success factors	Commitment to establish knowledge management centers and strengthen collaboration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

Objective 24: Foster Innovation through Research and Development

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

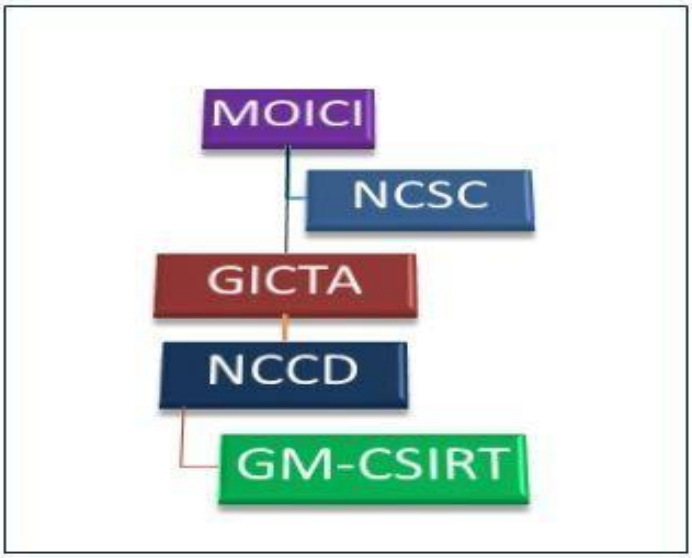
APPENDIX (B) Cybersecurity Program Risk Assessment Flow

CYBERSECURITY PROGRAM RISK ASSESSMENT FRAMEWORK



APPENDIX (C) Cybersecurity Governance Organogram

THE GAMBIA CYBER-GOVERNANCE/COORDINATION OGANOGRAM



Appendix (D) National Cybersecurity Commission Committees

NATIONAL CYBERSECURITY 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)

APPENDIX (E) LOGICAL FLOW OF ACTION PLAN