World Bank
West Africa Regional Communications and Infrastructure Program (WARCIP)

THE GAMBIA NATIONAL CYBERSECURITY STRATEGY

ACTION PLAN

28 June 2016

Draft V5

A study conducted by

Expertise France, Bird & Bird and Civipol Conseil
with the financial support of the WARCIP

ACRONYMS

CIIP	Critical Information Infrastructure Protection
CIRT	Computer Incident Response Team
CSIRT	Computer Security & Incident Response Team
GBOS	Gambia Bureau of Statistics
GNCSS	The Gambia National Cybersecurity Strategy
GRTS	Gambia Radio & Television Services
ICT	Information and Communication Technology
MOE	Ministry of Energy
MOHERST	Ministry of Higher Education, Research, Science and Technology
MOFA	Ministry of Foreign Affairs
MOI	Ministry of Interior
MOJ	Ministry of Justice
MOICI	Ministry of Information and Communication Infrastructure
NCI	National Critical Infrastructure
NCII	National Critical Information Infrastructure
NICI	National Information & Communication Infrastructure Policy & Plans
NICTA	National ICT Agency
NCCD	NICTA Cybersecurity Coordination Department
NCSC	National Cybersecurity Commission
NRS	National Records Services
PURA	Public Utilities Regulatory Authority
SOC	Security Operation Centre
UN	United Nations
WARCIP	West Africa Regional Communications Infrastructure Program

Action Plan

It is recommended to implement this Action Plan in 3 phases

- Phase 0: inception phase
- Phase 1: the first 8 months
- Phase 2: Months 8 to 16
- Phase 3: Months 16 to 24

Within each phase, tasks assigned as Priority 1 shall be initiated first.

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G0	**Preparation phase: elaborate and validate the final Action Plan and achieve the first priority actions**				
G0A1	Identify a small group of people (around 10-15 persons) with skills or interest in cybersecurity, selected preferably among the most active participants in the Cybersecurity Forum organised on 17th May 2016. This group shall provide key contributors from different ministries and private sector, who will participate in the NCCD, the GM-CSIRT or the NCSC.	MOICI		1	Phase 0
G0A2	Assign these individuals a role in the different strategic goals, leveraging their interests and skills. Initial activities (announcement of the Strategy, set-up of the NCSC, NCCD and GM-CSIRT, development of the first initiatives in development of education and training) shall contribute to establish these professionals as pioneers/early adopters/points of contacts for the upcoming activities.	MOICI		1	Phase 0
G0A3	Submit the final Action Plan and the way of implementing it in the planned timeframe to the NCSC for advice and to the NCCD for approval	MOICI		1	Phase 0
G0A4	Before implementing the Action Plan, set up reporting rules and indicators for assessing and monitoring its implementation by NCCD.	MOICI		1	Phase 0

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G0A5	Before implementing the Action Plan, set up a public communication plan to promote The Gambia National Cybersecurity Strategy (GNCSS) at national level and position The Gambia at international level.	MOICI		1	Phase 0
G1	**Strategic goal 1: Develop and enhance awareness, training and education**				
G11	**Sub Goal 1.1 Prepare the next generation of cybersecurity professionals**				
G11A	**Constitute the nucleus group on which the Goal 1 will be built**		MOICI NCSC	1	Phase 1
G11A1	Identify existing IT professionals with skills and/or interest in cybersecurity from public and private sectors	NCCD	MOICI, Ministries NCII, ICT companies …		
G11A2	Assign them a role in the building up of first academic curriculum and awareness tools on cybersecurity (developing content and teaching it)	NCCD	MOE, MOHERST		
G11B	**Improve the nucleus group skills and experience on cybersecurity and train future trainers**			1	Phase 1
G11B1	Set up an informal network for information and experience sharing	NCCD	Nucleus group		
G11B2	Study the numerous websites of CSIRTs and agencies around the world (in particular those who have developed content and initiatives in the field of capacity building) and identify the content that can be reused	Nucleus group			
G11B3	Enhance their skills and experience by getting cybersecurity training abroad or from abroad	NCCD			
G11C	**Setting up the first academic curriculum on cybersecurity aiming at educating**				
G11C1	Define the training goals of the first curriculum (having as soon as possible some advanced cybersecurity experts for GM-CSIRT and education, and less advanced but as numerous as possible IT experts with cybersecurity knowledge for ministries and NCII operators)	MOHERST	MOICI NCCD Nucleus group	1	Phases 1 to 3
G11C2	Recruit students with skills or interest in ICT or cybersecurity	MOHERST	NCCD, NCSC Nucleus group	1	Phases 1 to 3
G11D	**Attract young people to cybersecurity careers, including female**				

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G11D1	Regularly speak to young generations in schools by highlighting ICT and cybersecurity jobs attractiveness, and by using serious game about cybersecurity (to be carried out simultaneously with young people awareness, Action G14)	NCCD	MOHERST, MOE NCSC, GM-CSIRT Women's Bureau	1	Phases 1 to 3
G12	Sub Goal **1.2 Enhance cybersecurity knowledge of ICT experts**				
G12A1	Introduce adequate cybersecurity lessons in ICT academic curricula (at least, cyber vulnerabilities, threats, risk management approach and solutions to mitigate the risks in ICT)…)	MOHERST	NCCD, GM-CSIRT	1	Phase 1
G12A2	Organise practical courses and workshops for ICT students in public and private ICT departments	MOHERST	NCCD, Ministries, NCII, ICT companies	2	Phases 1 to 3
G12A3	Upgrade cybersecurity skills of ICT professionals, notably those employed by NCII and ICT companies, by organizing theoretical and practical courses and workshops	NCCD	MOHERST Ministries, NCII, ICT companies	1	Phase 1 to 3
G13	**Sub Goal 1.3 Train and educate prosecutors and investigators on cybercrime**				
G13A	**Set up a specialised law enforcement team in charge of cybercrime**			1	Phase 1
G13A1	Identify existing prosecutors and investigators with skills or interest in cybercrime	MOJ		1	Phase 1
G13A2	Enhance their technical and procedural skills and experience by meeting with GM-CSIRT experts and getting cybercrime training abroad	MOJ	MOICI, GM-CSIRT INTERPOL	1	Phase 1&2
G13B	**Provide specific awareness sessions on fighting cybercrime to future prosecutors and investigators**				
G13B1	Incorporate courses on cybercrime, digital investigation and electronic evidence within the curriculum on law enforcement	MOJ	MOE, INTERPOL	2	Phase 2
G13B2	Include basic training on cybercrime and electronic evidence for police students	MOJ	MOE, INTERPOL	1	Phase 1
G13C	**Enlarge the law enforcement team as much as necessary and possible**	MOJ, MOI	NCCD	2	Phase 3
G14	**Sub Goal 1.4 Rising public awareness on cyber risks and solutions**				
G14A	**Set up a cybersecurity awareness strategy toward the various audiences**			1	Phases 1 to 3

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G14A1	Define and prioritize the various audiences (managers, ICT professionals, ICT users, school children, individuals …)	NCCD	MOICI, MOE GM-CSIRT NCSC		
G14A2	Define awareness sessions content and length for each audience (at least, cyber risks and computing hygiene for all, ways of taking into account cybersecurity requirements for managers)	NCCD	MOICI, MOE GM-CSIRT NCSC		
G14B	**Organise awareness actions**				
G14B1	Plan awareness sessions, events and media campaigns	NCCD	MOICI, Ministries GM-CSIRT NCSC, GRTS	1	Phase 1
G14B2	Consider the possibility of organizing an annual "cybersecurity Day" (or week, or month)	NCCD	MOICI, NCSC GM-CSIRT	2	Phase 3
G2	**Strategic goal 2: Establish and develop institutional governance and capabilities**				
G21	**Sub Goal 2.1 Setting up the National Cybersecurity Authority (NCCD)**				
G21A1	Set up the NCCD	MOICI		1	Phase 1
G21A1	Draw up the document specifying his role and responsibilities and disseminate it to the public administrations, NCIIs and NCSC members	MOICI		2	Phase 1
G22	**Sub Goal 2.2 Setting up the National Cybersecurity Committee (NCSC)**				
G22A1	Appoint the members of the Committee	NCCD	MOICI, Ministries …	1	Phase 1
G22A2	Draw up the document specifying its role and responsibilities and disseminate it to the public administrations, NCIIs and NCSC members	NCCD	MOICI, Ministries	1	Phase 1
G22A2	Draw up the internal operating rules	NCCD		2	Phase 1
G22A3	Regularly specify the working plan for the Committee and the agenda for the NCSC meetings	NCCD		1	Continuously
G23	**Sub Goal 2.3 Setting-up The Gambia Computer Security and Incident Response Team (GM-CSIRT)**				

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G23A	**Create the CSIRT and CSIRT services**				
G23A1	Appoint the initial CSIRT team (partially achieved by action G11A)	NCCD	MOICI	1	Phase 1
G23A2	Specify the initial services to be provided by the CSIRT and project those to be progressively implemented in phase 2 and 3	NCCD	CSIRT	1	Phase 1
G23A3	Set up CSIRT infrastructure and equipment	CSIRT	MOICI NCCD	1	Phase 1
G23A4	Draft internal procedures and security policies	CSIRT		1	Phase 1
G23A5	Draft rules for reporting incident to national authorities and make them validated by NCCD	CSIRT	NCCD, NCSC	1	Phase 1
G23A6	Build if possible a GM-CSIRT website for easily sharing information on alerts, warning and announcements with the constituency and the public	CSIRT		2	Phase 2 & 3
G23A7	Set up a cyber threat monitoring system	CSIRT		2	Phase 2 & 3
G23B	**Create the CSIRT constituency and the rules of relationship**				
G23B1	Draft the GM-CSIRT constituency policy (consider PPP for sharing expenses and people with private operators)	MOICI	CSIRT	1	Phase 1
G23B2	Establish the initial constituency and extend it gradually	MOICI	CSIRT, Ministries NCSC, NCII	1	Phases 1 to 3
G23B3	Set up external procedures for interactions between the CSIRT and the constituency	CSIRT		1	Phase 1
G23B4	Establish liaison with point of contact (PoC) designated by each constituency members	CSIRT	Constituency	1	Phases 1 to 3
G23B5	Regularly bring PoCs together for assessing difficulties and progresses made	CSIRT	Constituency	2	Permanent
G23B6	Regularly test procedures and perform progressive training	CSIRT	Constituency	2	Permanent
G24	**Sub Goal 2.4 Setting-up governmental capability on cyber crisis management**				
G24A1	Plan a contingency organisation to be quickly set up in case of disruption of major critical services in Gambia (as a result of a cybersecurity incident or any other kind of incident)	Relevant Ministries		2	Phase 2
G24A2	Draft contingency plans to minimise the impact of the disruption by ensuring minimal services during the incident, then restore the normal capability, for various scenarios of impacted services	Relevant Ministries		2	Phase 2
G24A3	Regularly test organization and plans and train teams, especially on cyber incident scenarios where the capability must work closely with the GM-CSIRT.	Relevant Ministries		2	Phase 3
G25	**Sub Goal 2.5 Setting-up capability on judicial treatment against cybercrime**				

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G25A1	Set up a small cybercrime unit within the Gambia police force (achieved by actions G13)	MOI		1	Phase 1
G25A2	Equip cybercrime investigators with appropriate equipment for forensics	MOI		1	Phase 1 to 3
G25A3	Concentrate cybercrime complaints within the police cybercrime unit	MOI	MOJ	1	Permanent
G25A4	Organise collaboration of GM-CSIRT with the police cybercrime unit, especially its support for technical investigations with due regard to confidentiality of investigations and preservation of digital evidence	NCCD	MOI, MOJ GM-CSIRT	2	Phase 2
G25B1	Have at least two experienced prosecutors for cybercrime affairs (achieved by actions G13)	MOJ		2	
G25C1	Monitor cybercrime trends and share relevant information with NCCD and NCSC	MOJ	MOI, MOICI NCSC, GBOS, NRS	3	Phase 3
G3	**Strategic goal 3: Ensuring the protection of information systems, in particular those underlying important services**				
G31	**Sub Goal 3.1 Identification of The Gambia National Critical Information Infrastructure (NCII)**				
G31A1	Based on risk scenarios, identify the public and private services and infrastructure whose disruption or destruction would have a debilitating impact on citizens' health and welfare, economy, public institutions and national security	Ministries	MOICI, NCCD	1	Phase 1
G31A2	Identify NCI operators	Relevant Ministries / Office of the President		1	Phase 1
G31B1	Identify and designate National Critical Information Infrastructure (NCII) by carrying out a cyber-risk assessment on NCIs' ICT systems and identifying those which are critical	Ministries NCCD	MOICI, CSIRT	1	Phase 1
G31C1	Revisit the list of NCI and NCII on a regular basis	Ministries NCCD	MOICI, CSIRT	2	Permanent
G32	**Sub Goal 3.2 Ensuring protection and resilience of NCII**				
G32A	Define minimal security rules to be implemented by each operator of NCII:	NCCD	Ministries, NCII GM-CSIRT	1	Phase 1
G32A1	Designation of the operator cybersecurity authority				

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G32A2	Setting up an operator SOC capability responsible for implanting software security patches and administrating security control (firewall, antivirus, attack detection tools …)				
G32A3	Carrying a cyber risk analysis and accordingly upgrading security controls				
G32A4	Coming into force of a cybersecurity policy setting rules and behaviour to be respected by ICT professionals and users, including computing hygiene rules				
G32A5	Performing regularly cybersecurity audits				
G32A6	Reporting of ICT incidents to the GM-CSIRT				
G32A7	Developing business continuity plans				
G32B	Notify each operator of NCII with the minimal security rules it has to implement	NCCD	MOICI Ministries	1	Phase 1 or 2
G32C	Apply the minimal security rules as defined	NCII	GM-CSIRT	1	Phases 2 to 3
G32D	Test the continuity plans on a regular basis	NCCD	NCII, CSIRT Ministries	2	Permanent
G33	**Sub Goal 3.3 Foster the adoption of cybersecurity standards and good practices within government and private sector**				
G33A	**Foster the adoption of cybersecurity policies**				
G33A1	Implement a cybersecurity policy in every public administration and regulated private company (Telecom operators, banks, water supplier…), specifying the basic computer hygiene rules employees (ICT professionals and others) have to comply with	MOICI	GM-CSIRT PURA, CBG …	1	Phase 2
G33A2	Engage all other bodies (private operators, association …) to do likewise	MOICI	GM-CSIRT	2	Phase 2
G33B	Ensure compliance of private operators with the international cybersecurity rules and good practices applicable in regulated sectors (especially Telecom operators and banks)	Regulators			
G33C	**Integrate adequate cybersecurity requirements in every ICT4D plan**	MOICI	Ministries	2	Phase 2
G33C1	Define minimal security standards for ICT4D plans of the Gambia	MOICI	Ministries		
G33C2	Identify regular training needs	MOICI	Ministries		
G33C3	Ensure compliance to the standards	GM-CSIRT	NCCD, Ministries	2	Permanent
G34	**Sub Goal 3.4 Foster the development of a cybersecurity ecosystem**				
G34A	Foster demand for cybersecurity solutions and services (achieved by actions G32 and G33)	NCCD	GM-CSIRT	2	Permanent

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G34B	Foster the supply by Gambia-based companies of secured ICT systems and cybersecurity solutions and services	NCCD	MOICI	2	Permanent
G34B1	Identify and implement methods to foster creation of cybersecurity companies, start-ups and initiatives	NCCD	MOICI		
G4	**Strategic goal 4: Development of legislative and regulatory framework**				
G41	**Sub Goal 4.1 Establishing appropriate institutional framework**				
G41A1	Provide legal basis to the NCCD, specifying his role and responsibilities	MOICI		2	Phase 1
G41A2	Provide legal basis to the NCSC, specifying his role and responsibilities	MOICI		2	Phase 1
G41A3	Provide legal basis to the GM-CSIRT, specifying his role and responsibilities	MOICI		2	Phase 1
G42	**Sub Goal 4.2 Ensuring security of networks and information systems**				
G42A1	Establish the list of the critical sectors and the NCI and NCII designation process, and provide NCCD authority to enforce cybersecurity rules to be implemented by NCII operators	MOICI	Ministries	2	Phase 1
G42A2	Establish the list of NCI and NCII operators and notify them	MOICI	Ministries	2	Phases 1 and 2
G42A3	Define the minimal cybersecurity rules to be implemented by NCII operators and notify them	MOICI	Ministries		
G43	**Sub Goal 4.3 Development of a substantive and procedural law on cybercrime**				
G43A1	Review existing legislation in order to clearly define all criminal offences related to ICT, and define effective, proportionate and dissuasive penalties	MOJ	NCCD	2	Phase 2
G43A2	Establish rules of procedures enabling judicial authorities to conduct specific investigations of proceedings for cybercrime	MOJ	NCCD	2	Phase 2
G5	**Strategic goal 5: Development of national and international cooperation**				
G51	**Sub Goal 5.1 Promoting active information sharing between public and private entities in The Gambia**				

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G51A1	Identify gradually the stakeholders within the Gambia	NCCD	MOICI, NCSC Ministries, NCII Academia ICT companies …	1	Phases 1 to 3
G51A2	Make the relevant stakeholders meet together to foster information sharing and national cooperation in the fields of cybersecurity and cybercrime, at strategic level under the auspices of NCSC and at technical level under the auspices of GM-CISRT (for cybersecurity) or MOI/MOJ (for cybercrime), starting with CNII points of contact.	NCCD GM-CSIRT MOI MOJ	MOICI, NCSC Ministries, NCII Academia ICT companies …	2	Phases 1 to 3
G51A3	Organize the cooperation between GM-CSIRT and law enforcement bodies	NCCD	MOICI, MOI, MOJ GM-CSIRT	1	Phases 2
G51A4	Encourage cybercrime victims and if need be GM-CSIRT to lodge complaints to law enforcement bodies	NCCD	MOI, MOJ GM-CSIRT	2	Phases 2 to 3
G52	**Sub Goal 5.2 Promoting active international cooperation on cybersecurity**				
G52A1	Establish liaison with regional CERTs and IMPACT for sharing experience, skills and operational information on cybersecurity	GM-CSIRT	NCCD, MOFA	2	Phase 2
G52A2	Consider the possibility to become a member of FIRST	GM-CSIRT	NCCD	2	Phase 3
G52A3	Identify and participate in regional and transregional forums on cybersecurity	GM-CSIRT	NCCD, MOICI MOFA	2	Permanent from phase 2
G52A4	Identify and participate in regional and transregional training on cybersecurity	GM-CSIRT	NCCD, MOICI MOFA	2	Permanent from phase 2
G53	**Sub Goal 5.3 Promoting active international cooperation against cybercrime**				
G53A1	Establish liaison with regional law enforcement agencies for sharing understanding, experience, skills and judicial information on cybercrime	MOJ MOI	MOFA, INTERPOL	1	Phase 2
G53A2	Identify and participate in regional and transregional forums and training on cybercrime	MOJ MOI	MOFA, INTERPOL	2	Permanent from phase 2
G53A3	Consider the ratification of the African Union Convention on Cyber Security and Personal Data Protection	MOFA	MOJ	2	Phase 3
G53A4	Consider the ratification of the ECOWAS Convention on Extradition	MOFA	MOJ	2	Phase 3

Action Code	Action	Lead	Stakeholders	Priority	Timeline
G53A5	Identify other legal instruments to both request and assist other countries related to cybercrime matters, e.g. bilateral agreements, international legal frameworks, Mutual Legal Assistance Treaties	MOJ MOI	MOFA, INTERPOL	2	Phase 3