Kiribati National Cybersecurity Strategy 2020

Ensuring a secure, reliable and efficient cyberspace for a sustainable prosperity.

Information and Communication Minister's Foreword

The use of Information and Communication Technology (ICT) has truly transform almost every aspect of our lives. The geography of Kiribati, with our low-lying islands dispersed over a vast ocean present unique challenges in communication. ICT have the potential to to resolve a lot of our challenges, one example is the commissioned of the 3G mobile network on the Southernmost islands of the Gilbert group, including Tamana, Arorae, Nikunau, Tabiteuea South, Nonouti and Beru have since then enable these islands to connect to the internet and to the rest of Kiribati and the world. ICT has brought together our dispersed islands closer, with opportunities and possibilities, bringing services such as ATM banking, sending and receiving money to remote outer islands, access to online banking and efficient communication capability for businesses and government services on these islands.

The government recognised ICT as an enabler and a driver in our pursuit for social and economic development for a sustainable prosperity in this digital era. The government is fully aware of risks and threats involved in this interconnected and interdependence world of Information and Communication Technologies, however the potential of ICT by far outweighs these risks and threats. The government does not only recognise the importance of Cybersecurity but is equally aware about the challenges in protecting ICT. In order to fully realize the benefits of ICT we must prioritise security (Cybersecurity).

The increase in internet connectivity throughout communities in Kiribati have also brought risks, including spam and phishing activities by cybercriminals to lure ordinary citizens into sending personal details and even money for their gain. We have also seen based on surveys carried out by the International Telecommunication Union (ITU) and the Government that a lot of young children in Kiribati have been exposed to different Cybersecurity incidents. Disinformation and fake news are also becoming issues that not only threaten the wellbeing of our people but the very foundation of our communities in such that these fake news or disinformation can be widely sway the perception of the public on some very crucial information relating to health, government services and other essential information. These are some but not all of pressing issues that we must address to ensure the security and prosperity of our people on the internet and the cyberspace in general.

Enshrined on the government Manifesto and reiterated in the Government's Kiribati Vision for the next 20 year (KV20); we are prioritising national Internet Security as a pillar for a secure, peaceful and prosperous Kiribati.

This strategy reiterates our commitment in ensuring the security to our national

Information and Communication Minister's Foreword

internet ecosystem (cyberspace) and to fulfil our obligation to ensure the fundamental rights of all our fellow Kiribati citizens.

This strategy paves a way in securing our people and our national internet ecosystem (cyberspace) to help us realize the full potential of ICT in our pursuit for economic growth.

I would like to thank all those who have contributed to the development of this strategy, including ITU and relevant development partners who have lend a hand in formulating this strategy. It is my hope that we join efforts to embrace this strategy and work together to implement and achieve the goals laid out in this strategy for a secure cyberspace for all Kiribati citizens.

Te Mauri (Health), Te Raoi (Peace) ao Te Tabomoa (and Prosperity).

Hon Tekeeua Tarati MP
Minister of Information, Communication, Transport and Tourism Development

Strengthening Cyber Security for a Safer and Secure Kiribati

The Government of Kiribati recognizes the relevance of Information Communication Technology (ICT) for the Kiribati. As outlined in the National ICT Policy 2019 the government is committed to creating a robust and reliable ICT environment. This includes investments into ICT infrastructure and services. The National ICT Policy 2019 highlights that one component of this approach is Cybersecurity. This includes but is not limited to securing fundamental rights of the people of Kiribati, protecting the infrastructure and investigating attacks. This strategy builds upon existing policies and sets out the Goals, and Objectives for Kiribati in maximizing safety and security in relation to the use of ICT. It pays particular attention to the National ICT Policy 2019, in particular policy issue 14 that deals with future developments in ICT. It also reflect – among others - the aims of the Millennium Development Goals, draws upon the recommendations related to ICT arising from the Final Acts of the International Telecommunication Union (ITU) Plenipotentiary Conferences (Busan, 2014 and Dubai, 2018). The strategy has been developed by Ministry of Information, Communications, Transport and Tourism Development with technical assistance from the ITU. Discussions were initiated with national and international experts to ensure a broad participation including governmental, non-governmental and open stakeholder consultations. Prior to the process of drafting this strategy the situation in the country as well as expectations from the public and private sector were assessed through different instruments. The input generated was directly included in the drafting of this document.

Links to other government policies

This strategy directly builds upon Kiribati's National ICT policy 2019 and directly links the security components to the ambitious goals defined by the National ICT policy 2019. The government in this regards underlines, that the government and the private sector in Kiribati have a finite budget. While Kiribati faces similar security challenges as other nations it will not be able to develop extensive institutional capacities. The strategy is therefore based on the principle of strengthening existing structures instead of creating new ones

Multistakeholder partnership in combating cyber threats

The Government builds upon the existing structures as well as the support of the private sector to share the responsibility of fulfilling the goals of this strategy. This includes the ICT Infrastructure provider that play a key role in connecting the people of Kiribati and businesses and are in a unique position to protect them and support the work of law enforcement in preventing and investigating crime.

Cyber threats in an increasingly connected Kiribati

The use of ICT and the increasing connectivity opens the door for offenders. The government, especially through the work of law enforcement, is aware that while citizens, businesses and the government have taken measures to enhance Cybersecurity attacks take place. They range from illegal content accessed and shared online to attacks against computer systems. With the increasing bandwidth following the completion of currently ongoing Submarine Cable project, new types of attacks will be possible that have previously not been possible. One example is the abuse of computer systems in Kiribati for large scale botnet attacks.

International cooperation in addressing cyberthreats and attacks

The government believes, that the fast-changing risk landscape requires constant monitoring and observations. Especially with regard to the fact that those developments take place in an increasingly international environment that requires close cooperation with other nations the government is committed to further improving it's knowledge about Cyber threats. In order to respond to trends and new developments the government in general and the specialized institutions require up-to-date information about attacks in the country. Kiribati will address the challenges by developing and reporting mechanism. In this regard the government is committed to support a bi-directional exchange.

To realise the potential of ICT, Cybersecurity should be a priority

While the government is of the firm believe that the potential of ICT by far outweighs the risks it does not only recognize the importance of Cybersecurity but is equally aware about the challenges of protecting ICT. The government especially notices that neither in developing nor highly developed countries, the government and law enforcement are single-handed capable of protecting businesses and citizens from Cyber threats.

Universal Access Plan

The goal of the Universal Access Plan is to ensure availability, affordability and accessibility to information and communication technologies (ICT) throughout Kiribati. There are provisions under the Communications Act 2012 for Universal Access Plan. The plan will facilitate connecting all Kiribati islands to the Internet. Including funding of Universal Access project under the advise of the Universal Access Advisory Commitee.

Objectives & Goals

The pursuit of Economic growth through ICT

The National Cybersecurity strategy is consistent with the aims and strategies of the Kiribati National ICT policy 2019 and the Development Plan – namely, the pursuit of economic growth and the development of the full potential of ICT. It shall take into account relevant national, regional and global best practices in building confidence and security in ICT by cultivating strong linkages with the applicable UN GA resolutions as well as the ITU recommendations.

Proper protection for all Kiribati citizens against cyber threats

The government aims to protect the people, businesses and government agencies and provide the necessary secure framework to achieve the aims developed and defined in the National ICT Policy. The government is aware that the measures defined by the ICT Policy, will have a major impact on the connectivity within the country. In addition the government is aware that with the increase in bandwidth new services will be available and that some of them will go along with security concerns. As a consequence the government gives priority to a timely implementation of this strategy to ensure that Cybersecurity measures are implemented in parallel to the increase in services and connectivity. Policy measures shall include appropriate legislation and regulations. The legislation will especially focus improving the fight against criminal abuse of ICT and Cybercrime. Regulations will especially focus on technical minimum standards in relation to Cybersecurity.

Guiding Principles

- Safe and secure environment for all citizens.
- Protection of fundemantal rights.
- Balanced approach in line with international and regional best practices.

Mechanisms for implementing these principles

This Strategy has the following specific objectives arranged in three groups for timing purposes:

Short term goal (2020)

- Gap analysis to existing legislations on cybersecurity and cybercrime.
- Child Online Protection Working Group (COPWG) to be established.
- Kiribati Cybersecurity Working Group (KCSWG) to be established.
- Situational Analysis for capacity building in cyber security & capacity building.

Medium term goal (2020-2021)

- Creation of CERTKiribati.
- Development of National Cybersecurity Guidelines.
- Development of National Incident Reporting, handling and referral guideline.
- Comprehensive cybercrime legislation established.
- Established National Contingency Plan.
- International cooperation on cyber security (cyber crime).
- Critical Infrastructure protection Plan.
- Cyber Security Capacity building.

Long term goals (2020-2023)

- Development of Outer Island Strategy on Cyber Security.
- Cyber Security Introduction to education curriculum.

Establishment of a Computer Emergency Response Team (CERT) Kiribati

As pointed out, Kiribati is mindful about limited resources and determined to maximize the use of existing organizational structures.

Creation of CERT Kiribati

An independent National CERT of Kiribati (CERTKiribati) will be created. It shall be supervised and monitored by the Ministry of Information, Communications, Transport and Tourism Development. CERTKiribati will be responsible for providing services related to Cybersecurity to the government, government institutions, law enforcement, businesses and the people. It should focus on promoting Cybersecurity; awareness raising; upon request supporting institutions and businesses in prevention, detection and response to Cyber attacks; maintain 24/7 points of contact; carrying out digital forensic investigations; receiving and distributing reports about incidents and auditing and providing special support to critical infrastructure provider.

Information processed by CERT Kiribati as a baseline for cybersecurity initiatives

KiribatiCERT will carry out a coordinated survey and assessment, to analyse how far citizens, businesses and government are affected by Cybersecurity incidents and Cybercrime. KiribatiCERT will identify local contact points on the Outer Islands that can facilitate the collection of input about recent developments as well as spreading information to the communities.

Public Private Partnership for better cooperation and sustainable services

Within this process public private partnership approaches shall be taken into consideration. KiribatiCERT will, upon request, provide the government, government institutions, law enforcement, businesses and the people with information about Cybersecurity. It should maintain resources to handle request, promote the adoption of global best practices in Cybersecurity and compliance, provide training material and practical information as well as refer to publicly available tools. It should in addition provide on the ground advisory support to critical infrastructure provider and law enforcement agencies. Wherever possible KiribatiCERT shall cooperate with regional and international organizations as well as institutions and initiatives present in the country that already provide services, material and information on a non-commercial level and evaluate the possibility of building upon existing instead of developing new material.

Development of National Cybersecurity Guidelines

The stakeholder consultations carried out during the process of developing this strategy revealed that people and businesses are seeking guidance how they can enhance Cybersecurity. Providing them as well the different government institutions with National Cybersecurity Guidelines responds to this demand. The government believes, that the unique situation of Kiribati shall be reflected when making available information and guidelines.

Establishing a Kiribati Cybersecurity Working Group (KCSWG)

The Kiribati Cybersecurity Working Group (KCSWG) will be formed. During the stakeholder consultations various existing government and non-government institutions were identified that are currently active in the field of Cybersecurity in order to create a diverse group. The KCSWG shall have the following structure:
The KCSWG will be chaired by CERTKiribati with members from the both government private and academia institutions.
These members should have a strong Information & Communication Technology (ICT) technical background, including technical knowledge on information security/cybersecurity. Members from legal institutions should be well versed with legal aspects and existing legislations relating Information Communication Technologies. The KCSWG should have at least one and no more than two representatives from these institutions, unless otherwise justified under certain circumstances.

Roles and Responsibilities of KCSWG

KCSWG is tasked with the development of a set of specific Cybersecurity and Cyber-Safety guidelines. It should go beyond policy statements and focus on concrete measures that will guide people, businesses and government institutions. It should address the following issues: Responsibility within the government and private sector, definition of processes, technical specifications and risk assessment and emergency plans. The responsibility section should clearly point out the roles and responsibilities of different institutions. This may include technical as well as management responsibilities. The government underlines that maintaining a sufficient crisis and incident management is a key component of any Cyber defence strategy. Taking into account the potential devastating impact of cyber attacks, clear rules and procedures are required that define under which circumstances certain people and institutions need to take action. The processes shall define Cybersecurity related requirements with

Development of National Cybersecurity Guidelines

regard to relevant government processes. It may range from mandatory training procedures for new staff to concrete security procedures for trans-border travel. In order to provide solution-oriented guidance, processes should be described as precisely as necessary. Processes should especially include prevention, preparedness, detection, response and recovery. Defining clear, government as well as industry-wide technical specifications for Cybersecurity, such as minimum requirements with regard to the encryption of classified documents, should overcome conflicts caused by differing standards. The risk assessment and emergency plans should provide guidance with regard to the most likely threats scenarios. KCSWG will be responsible for the coordination and prioritization of information collection activities with a focus on building and strengthening a local knowledge sharing community. It will furthermore identify minimum requirements and qualifications for information security professionals that will serve as basis for the development of a related curriculum.

Protecting Children Online

The Child Online Protection Survey and stakeholder consultations carried out during the process of developing this strategy revealed that children in Kiribati are already at risk with regard to online threats. Protecting children has a high priority for the government.

Establishing a Child Online Protection Working Group (COPWG)

A Child Online Protection Working Group (COPWG) will be formed with the following structure:

1. KiribatiCERT (Chair).
2. Ministry of Women, Youth, Sport and Social Affairs (Social Affairs: Child Protection Officer).
3. Ministry of Education (Representative).
4. The United Nation Children's Fund (UNICEF: Child Protection Officer).
5. Communication Commission of Kiribati (Representative)
6. Kiribati Police Service (Representative)
7. Invited institutions who have direct engagement on child protection.

Roles and Responsibilities of COPWG

COPWG is tasked to identify areas of child online protection (such as technical protection measures, curriculums for school and information material for parents and guardians) that need to be integrated in Kiribati. Existing material made available by international organizations such as UNICEF and ITU shall be taken into consideration. One focus should be on evaluating different technical measures that services providers must introduce to protect children online and parameters that shall be included in a report submitted to guardians upon request. Based upon the evaluation COPWG in cooperation with KiribatiCERT will develop guidelines for technical child online protection measures. This shall include recommendations for measures how to prevent an abuse of the service.

Child Online Protection

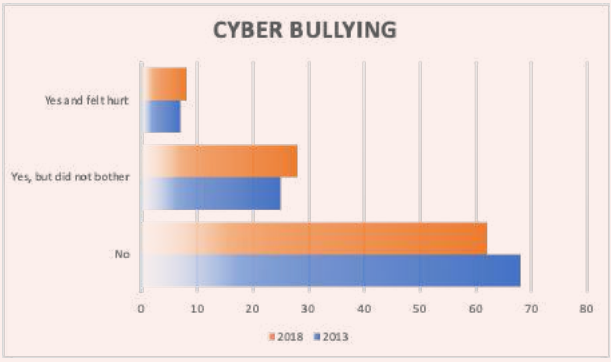
Measures implemented by GSM and Internet Access Provider

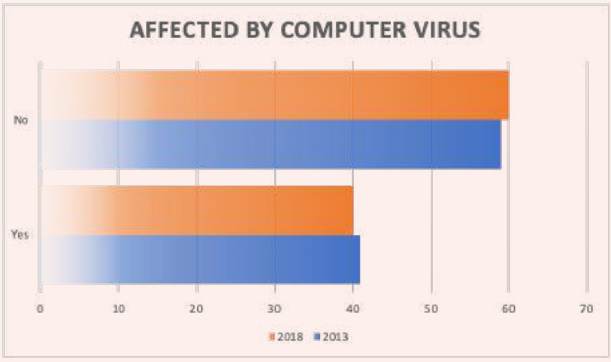
Based upon the guidelines developed by COPWG commercial provider of Internet access in Kiribati shall be obliged to provide – upon request of the user - a restricted Internet access that includes available technical measures aiming to block content that is not appropriate for children. Furthermore, the provider shall be obliged to provide – upon request of the user – a special reporting for parents or guardians that highlights the services used and other parameters defined by the COPWG. Based upon the guidelines developed by COPWG each commercial provider of GSM mobile communication services in Kiribati shall be obliged to provide – upon request - a SIM card with restricted access to services that may not be appropriate for children. The provider may not charge any additional fees for such service.

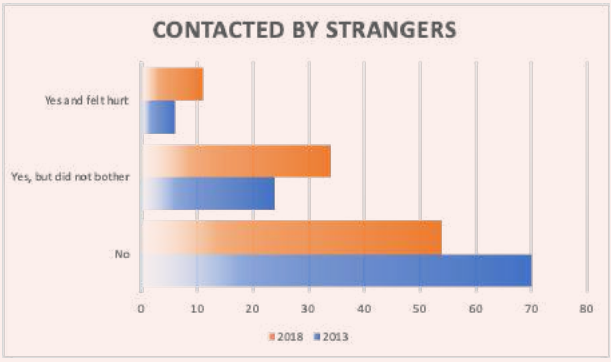
Child Online Proctetion Helpline

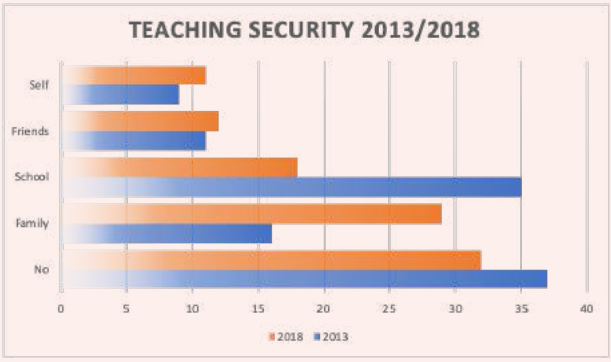
The Child Online Protection Surveys carried out in 2013 and 2018 reveals that a significant percentage of children have already been victim of cyber threats. In order to provide those victims with professional help and prevent further harm a helpline shall be created. The helpline shall be available through a toll-free number and through chat at least 4 hours a day.

Child Online Proctetion Assessment Survey (ITU/MICTTD) 2013/2018









Strengthening legislation on Cybersecurity and Cybercrime

Legislative gap analysis on cybersecurity and cybercrime

The Ministry of Information, Communications, Transport and Tourism Development (MICTTD) together with the Kiribati Police Service (KPS) and the Office of the Attorney General (OAG) will carry out an assessment of existing legislation addressing Cybersecurity and Cybercrime. This shall include the following areas of law: privacy and data protection, national security, e-commerce, freedom of information, admissibility of electronic evidence, liability of Service Providers (SPs), Children Online Protection and International Co-operation. The review shall include the identification of existing provisions that could be utilized in relation to Cybersecurity, a comparison with international best practices, a gap analysis, suggestions for amendments and the related drafting instructions. If considered useful the assistance of international organizations active in this field to carry out the assessment and comparative analysis shall be requested. The results of the assessment and analysis, complimented by recommendations for amendments/improvements shall be submitted to parliament after endorsement from Cabinet. Priority should be given to the topic Cybercrime. An analysis shall include the following topics: definitions, substantive criminal law, procedural law and investigation instruments of law enforcement, criminal liability of Service Providers and international cooperation.

Legislation that supports international cooperation in combating cybecrime

The government recognizes the truly international dimension of cyber attacks. To ensure that Kiribati's legal framework and practice is fully in line with international best practices in relation to international cooperation Office of the Attorney General (OAG) and the Ministry of Foreign Affairs and Immigration (MFAI) will analyse the capacities of Kiribati to efficiently submit requests for mutual legal assistance as well as timely respond to requests submitted to authorities in the country. A report about the findings and recommendation for improvements shall be submitted to parliament after endorsement from Cabinet. KiribatiCERT will make recommendations with regard to a potential access to international or regional agreements, current processes of developing binding standards where Kiribati should participate, as well as 24/7 networks (such as the Interpol Network). With regard to the evaluation of an access to existing instruments the relevance for Kiribati, the reflection of legal standards and cultural specifies as well as the usefulness in cooperation with other countries shall be taken into consideration. KiribatiCERT will seek membership of Regional and Global CERTs as required.

Cybersecurity capacity enhancement and a coordinated incident response

Cybersecurity capacity building with CERTKiribati

CERTKiribati shall provide a list of capacity building programs related to Cybersecurity that Kiribati could benefit from. To avoid an overlapping CERTKiribati shall develop a roadmap that lists the different capacity activities that the country require, identify potential programs and make suggestions which programs cover which activity.

Education and awareness for children about cybersecurity

Child Online Protection Surveys carried out with the support of the International Telecommunication Union (ITU) in 2013 and 2018 revealed that students wish for more Cybersecurity training in schools. The The Ministry of Education (MOE) and the Ministry of Women, Youth, Sport and Social Affairs (MWYSSA) will in cooperation with CERTKiribati and other authorities in Kiribati develop a curriculum to ensure that all students at primary school and high school receive at least once a year an updated training on Cybersecurity that includes information about latest trends. Training materials, background information for teachers and sample presentations shall be developed. In addition schools should receive a questionnaire to enable them to assess the use of ICT service by students as well child specific Cybersecurity risks. The anonymous assessment shall be carried out on anannual basis and the results shall be submitted to CERTKiribati and included in their annual report.

National Incident Reporting

Citizens, businesses and governments shall be encouraged to report cyber incidents. The provider of critical national infrastructure shall be obliged to submit such reports. To support the idea of information sharing, CERTKiribati shall develop routines to detect recent trends in relation to Cybersecurity incidents, create an emergency level system, summarizing incidents in a reporting format and providing background information, developing a network to communicate such reports through the relevant communication channels (e.g. press releases, information submitted to cooperation partners in rural areas) and submitting this information. This shall include the publication of relevant, non-confidential information on a regular basis on a publicly accessible website. Once a year, CERTKiribati shall submit a summary report on their work and especially notifications received. It should provide the government with regular briefings and provide additional information on request. CERTKiribati shall ensure that the information submitted to the different stakeholders reflect their needs with regard to details (e.g. executive summary for the minister, detailed information for system administrators on technical aspects of an attack) and that information are not distributed to recipients that are not affected.

Coordinated Incident response and Critical Infrastructure protection

Referral to Law Enforcement

CERTKiribati shall forward report about incidents that have a potentially criminal background to the responsible law enforcement agencies. Law enforcement should create a single point of contact and ensure that the secure infrastructure provided by CERTKiribati is utilized. The government will form an appropriate institutional structure within the law enforcement agency to handle cases of criminal nature reported by CERTKiribati.

Critical infrastructure protection

The government is aware that critical infrastructure (such as the airport) is increasingly depending on ICT. For the purpose of this strategy critical infrastructure shall be defined as the essential services that underpin Kiribati's society and serve as a backbone of the economy, security and health. The sectors included in the Critical Infrastructures are but not limited to Healthcare and Public Health Sector, Energy Provider Sector, Water and Wastewater Sector, Transportation Sector, Information and Communication Technology Sector, Food and Agriculture Sector, Financial Service Sector, Government Facility Sector, Emergency Service Sector, Law Enforcement and Judiciary and Tourism Sector. Significant parts of the today information infrastructure can be considered as critical information infrastructure as a failure or limited operation would cause tremendous impact on the vast majority of citizens. And concerns related to possible attacks against critical infrastructure are not limited to information infrastructure – various critical infrastructure providers that do not focus on information infrastructure, such as electricity and transportation provider intensively use ICT. Tremendous impact does therefore not only refer to direct damage but also indirect damages. With this strategy the government lays the foundation to increase the ability of a networks and information systems operated or utilized by critical infrastructure provider to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system.

Critical Infrastructure Assessment

The government is committed to strengthen the protection of critical infrastructure against Cyber attacks. This shall include the owner of critical infrastructure as well as operator of services using critical infrastructure. To ensure that the implementation of any mandatory standards is based upon the needs as well as capacities of the affected operators of critical infrastructure the government will carry out a needs and risk assessment, focusing on critical infrastructure provider, including small medium enterprises as well as large enterprises and public and private

Paving a Path to a Safer Cyber Space for all

Strengthening existing organizational structures

While the government is committed to protect businesses and the people in Kiribati from threats related to Cybersecurity it emphasizes the importance of self-protection and underlines the responsibility of the individual. The government will support the self-protection by providing knowledge through CERTKiribati.

Risk and vulnerability assessment for an effective cybersecurity strategy

Government institutions and business are encouraged to undertake an individual risk assessment, develop and implement a Cybersecurity strategy that addresses the main risks, designate a member of senior management as Chief Information Security Officer, responsible for Cybersecurity efforts and initiatives, maintain state-of-the art Cybersecurity technology that reflects it's risk landscape, implement risk assessment and risk management processes, have business continuity management and crisis management plans in place and carry out regular exercises. Further requirements apply to the provider of critical infrastructure. CERTKiribati shall support this process and develop a standard risk assessment framework for businesses in Kiribati. Businesses in Kiribati are encouraged to utilize this framework. CERTKiribati shall in addition evaluate the need to implement an evaluation/certification program for Cybersecurity services, products and systems. CERTKiribati shall develop andimplement technical and organizational protection measures as well as emergency plans to protect essential government services (such a eGovernment)

Cybersecurity In Education Curriculum

CERTKiribati will make recommendations and work in collaboration with the Ministry of Education for introduction of cybersecurity into the national education curriculum. The cybersecurity subject should include basic definitions of cybersecurity related terminologies and should gathered to allow and develop students' knowledge on ICT and cyber security.

Outer island strategy

The government is committed to further increasing connectivity on the Outer Islands with several milestones already achieved. Cybersecurity is as much of a threat for people, business and the government in the Outer Islands as it is elsewhere. The government will therefore ensure that Cybersecurity measures implemented by this strategy are rolled out in Outer Islands as well. Where necessary infrastructure is missing additional distribution channels and strategies will be developed.

Critical Infrastructure Protection

operators. The government will promote a nation wide as well as regional debate, involving all relevant public and private stakeholders, to define priorities for the long term resilience and stability of critical infrastructure against cyber attacks. The assessment shall be carried out by CERTKiribati and submit a report including recommendations to parliament after endorsement from Cabinet.

National Critical Infrastructure Protection Policy

After receiving the results of the assessment the government will decide if further action, especially the development of a National Critical Infrastructure Protection Policy is required.

Identification of Critical Infrastructure

Taking into account the importance of critical infrastructure and the cyber threats the following immediate measures shall be implemented by CERTKiribati: CERTKiribati together with KSWG will identify infrastructure provider in Kiribati that shall be considered critical based on the definition provided above. The identified infrastructure provider shall be identified that they are considered critical. CERTKiribati with the assistance of KCSWG should develop technical Cybersecurity guidelines for operator of critical infrastructure. CERTKiribati should in addition maintain an incident management system as well as the necessary technical and human resources to support critical infrastructure provider in dealing with cyber incidents. The purpose of the support is not to substitute the required resources on the side of the critical infrastructure provider but to provider addition support.

Cybersecurity Minimum Standards

The provider of critical infrastructure are required to take technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems. To coordinate the activities the provider of critical infrastructure shall appoint a member of senior management as Chief Information Security Officer and ensure that it earmarks a specific budget for implementing Cybersecurity measures. Further more the provider of critical infrastructure is obliged to carry out a risk and exposure self assessment at least once a year and document this process.

Critical Infrastructure Protection and National Contingency Plan

Incident Reporting

Identified critical infrastructure provider shall colloborate and report any ICT related incident to CERTKiribati providing basic information about the circumstance of the attack, the expected impact and affected services within 72 hours after detecting the incident.

National Contingency Plan

CERTKiribati shall develop a national contingency plan and organise regular exercises for large scale network security incident response and disaster recovery. Those exercises shall include latest trends and developments to allow critical infrastructure providers to prepare for attacks and cover technical components as well as risk management.